

---

---

## Informatiebeveiliging, cybersecurity en bescherming van de privacy – Beheersmaatregelen voor informatiebeveiliging

*Information security, cybersecurity and privacy protection —  
Information security controls*

*Sécurité de l'information, cybersécurité et protection de la vie  
privée — Mesures de sécurité de l'information*

Dit document mag slechts op een stand-alone PC worden geïnstalleerd. Gebruik op een netwerk is alleen toegestaan als een aanvullende licentieovereenkomst voor netwerkgebruik met NEN is afgesloten.  
This document may only be used on a stand-alone PC. Use in a network is only permitted when a supplementary license agreement for use in a network with NEN has been concluded.



Referentienummer  
ISO/IEC 27002:2022 (nl)

© ISO/IEC 2022

Dit document bevat de vertaling in het Nederlands van de internationale norm ISO/IEC 27002:2022.

Normcommissie 381027 'Informatiebeveiliging, Cyber security en Privacy'



**THIS PUBLICATION IS COPYRIGHT PROTECTED**

**DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD**

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of Stichting Koninklijk Nederlands Normalisatie Instituut.

Stichting Koninklijk Nederlands Normalisatie Instituut shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to Stichting Reprerecht.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van Stichting Koninklijk Nederlands Normalisatie Instituut niets uit deze uitgave worden veeelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Stichting Koninklijk Nederlands Normalisatie Instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor veeelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan Stichting Reprerecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. Stichting Koninklijk Nederlands Normalisatie Instituut and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by Stichting Koninklijk Nederlands Normalisatie Instituut.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Stichting Koninklijk Nederlands Normalisatie Instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door Stichting Koninklijk Nederlands Normalisatie Instituut gepubliceerde uitgaven.



© 2022 Stichting Koninklijk Nederlands Normalisatie Instituut  
www.nen.nl

# Inhoud

<b>Voorwoord .....</b>	<b>6</b>
<b>Inleiding.....</b>	<b>8</b>
<b>1      Onderwerp en toepassingsgebied.....</b>	<b>11</b>
<b>2      Normatieve verwijzingen .....</b>	<b>11</b>
<b>3      Termen, definities en afgekorte termen .....</b>	<b>11</b>
3.1      Termen en definities .....	11
3.2      Afgekorte termen .....	17
<b>4      Structuur van dit document.....</b>	<b>19</b>
4.1      Hoofdstukken .....	19
4.2      Thema's en attributen .....	19
4.3      Indeling beheersmaatregel .....	21
<b>5      Organisatorische beheersmaatregelen .....</b>	<b>21</b>
5.1      Beleidsregels voor informatiebeveiliging .....	21
5.2      Rollen en verantwoordelijkheden bij informatiebeveiliging .....	24
5.3      Functiescheiding .....	25
5.4      Managementverantwoordelijkheden .....	26
5.5      Contact met overheidsinstanties .....	27
5.6      Contact met speciale belangengroepen .....	28
5.7      Informatie en analyses over dreigingen .....	29
5.8      Informatiebeveiliging in projectmanagement .....	31
5.9      Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen .....	33
5.10      Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen .....	35
5.11      Retourneren van bedrijfsmiddelen .....	36
5.12      Classificeren van informatie .....	37
5.13      Labelen van informatie .....	39
5.14      Overdragen van informatie .....	41
5.15      Toegangsbeveiliging .....	44
5.16      Identiteitsbeheer .....	46
5.17      Beheren van authenticatie-informatie .....	47
5.18      Toegangsrechten .....	50
5.19      Informatiebeveiliging in leveranciersrelaties .....	52
5.20      Adresseren van informatiebeveiliging in leveranciersovereenkomsten.....	54
5.21      Beheren van informatiebeveiliging in de ICT-keten.....	57
5.22      Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten .....	59
5.23      Informatiebeveiliging voor het gebruik van clouddiensten .....	61
5.24      Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten.....	64
5.25      Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen .....	66
5.26      Reageren op informatiebeveiligingsincidenten .....	67
5.27      Leren van informatiebeveiligingsincidenten.....	68
5.28      Verzamelen van bewijsmateriaal .....	69
5.29      Informatiebeveiliging tijdens een verstoring.....	70
5.30      ICT-gereedheid voor bedrijfscontinuïteit.....	71
5.31      Wettelijke, statutaire, regelgevende en contractuele eisen.....	72
5.32      Intellectuele-eigendomsrechten .....	74
5.33      Beschermen van registraties.....	76
5.34      Privacy en bescherming van persoonsgegevens.....	78
5.35      Onafhankelijke beoordeling van informatiebeveiliging.....	79
5.36      Naleving van beleid, regels en normen voor informatiebeveiliging .....	80
5.37      Gedocumenteerde bedieningsprocedures.....	81

<b>6</b>	<b>Mensgerichte beheersmaatregelen .....</b>	<b>83</b>
6.1	Screening.....	83
6.2	Arbeidsovereenkomst.....	84
6.3	Bewustwording van, opleiding en training in informatiebeveiliging.....	86
6.4	Disciplinaire procedure.....	88
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband .....	89
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten .....	90
6.7	Werken op afstand.....	91
6.8	Melden van informatiebeveiligingsgebeurtenissen.....	93
<b>7</b>	<b>Fysieke beheersmaatregelen .....</b>	<b>94</b>
7.1	Fysieke beveiligingszones .....	94
7.2	Fysieke toegangsbeveiliging.....	95
7.3	Beveiligen van kantoren, ruimten en faciliteiten.....	97
7.4	Monitoren van de fysieke beveiliging.....	98
7.5	Beschermen tegen fysieke en omgevingsdreigingen .....	100
7.6	Werken in beveiligde zones.....	101
7.7	'Clear desk' en 'clear screen' .....	102
7.8	Plaatsen en beschermen van apparatuur.....	103
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein.....	104
7.10	Opslagmedia.....	105
7.11	Nutsvoorzieningen .....	107
7.12	Beveiligen van bekabeling.....	108
7.13	Onderhoud van apparatuur .....	109
7.14	Veilig verwijderen of hergebruiken van apparatuur .....	110
<b>8</b>	<b>Technologische beheersmaatregelen .....</b>	<b>112</b>
8.1	'User endpoint devices'.....	112
8.2	Speciale toegangsrechten .....	114
8.3	Beperking toegang tot informatie .....	116
8.4	Toegangsbeveiliging op broncode .....	118
8.5	Beveiligde authenticatie.....	119
8.6	Capaciteitsbeheer.....	121
8.7	Bescherming tegen malware.....	123
8.8	Beheer van technische kwetsbaarheden.....	125
8.9	Configuratiebeheer.....	129
8.10	Wissen van informatie .....	131
8.11	Maskeren van gegevens.....	133
8.12	Voorkomen van gegevenslekken (Data leakage prevention) .....	135
8.13	Back-up van informatie .....	137
8.14	Redundantie van informatieverwerkende faciliteiten .....	138
8.15	Logging .....	140
8.16	Monitoren van activiteiten.....	143
8.17	Kloksynchronisatie.....	146
8.18	Gebruik van speciale systeemhulpmiddelen .....	147
8.19	Installeren van software op operationele systemen .....	148
8.20	Beveiliging netwerkcomponenten.....	149
8.21	Beveiliging van netwerkdiensten.....	151
8.22	Netwerksegmentatie .....	152
8.23	Toepassen van webfilters.....	153
8.24	Gebruik van cryptografie .....	154
8.25	Beveiligen tijdens de ontwikkelcyclus .....	157
8.26	Toepassingsbeveiligingseisen.....	158
8.27	Veilige systeemarchitectuur en technische uitgangspunten .....	161
8.28	Veilig coderen.....	163

8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie .....	167
8.30	Uitbestede systeemontwikkeling .....	168
8.31	Scheiding van ontwikkel-, test- en productieomgevingen .....	169
8.32	Wijzigingsbeheer .....	171
8.33	Testgegevens .....	173
8.34	Bescherming van informatiesystemen tijdens audits .....	174
<b>Bijlage A (informatief) Attributen gebruiken .....</b>		<b>175</b>
<b>Bijlage B (informatief) Overeenstemming van ISO/IEC 27002:2022 (dit document) met ISO/IEC 27002:2013 .....</b>		<b>188</b>
<b>Bibliografie .....</b>		<b>198</b>

## Voorwoord

ISO (International Organization for Standardization) en IEC (International Electrotechnical Commission) vormen tezamen een stelsel dat gespecialiseerd is in wereldwijde normalisatie. Nationale organisaties die lid zijn van ISO of IEC participeren in het ontwikkelen van internationale normen via technische commissies die door de desbetreffende organisatie zijn ingesteld ten behoeve van de normalisatie in specifieke technische werkvelden. Technische commissies van ISO en IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als ngo's nemen, in samenwerking met ISO en IEC, ook deel aan deze werkzaamheden.

De procedures die zijn gebruikt voor het ontwikkelen van dit document en de procedures die zijn bedoeld voor het verdere onderhoud ervan, worden beschreven in de ISO/IEC-richtlijnen, deel 1. Hierbij wordt met name gewezen op de verschillende goedkeuringscriteria die nodig zijn voor de verschillende soorten documenten. Dit document is opgesteld volgens de redactionele regels die in de ISO/IEC-richtlijnen, deel 2 zijn opgenomen (zie [www.iso.org/directives](http://www.iso.org/directives) of [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. ISO en IEC zijn niet verantwoordelijk voor identificatie van dergelijke patentrechten. Nadere informatie over eventuele patentrechten die zijn geïdentificeerd tijdens het ontwikkelen van het document, is te vinden in de inleiding en/of de ISO-lijst met ontvangen patentverklaringen (zie [www.iso.org/patents](http://www.iso.org/patents)) of de IEC-lijst met ontvangen patentverklaringen (zie [patents.iec.ch](http://patents.iec.ch)).

Eventuele handelsnamen die in dit document worden gebruikt, zijn verstrekt ter informatie voor het gemak van de gebruiker en houden geen aanbeveling in.

Uitleg over de vrijwillige aard van normen, de betekenis van ISO-specifieke termen en uitdrukkingen met betrekking tot conformiteitsbeoordeling, alsmede informatie over hoe ISO voldoet aan de beginselen van de Wereldhandelsorganisatie (WTO) in de Technical Barriers to Trade (TBT), wordt gegeven op: [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). Voor IEC, zie [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

Dit document is opgesteld door ISO/IEC JTC 1, *Information technology, SC 27, Information security, cybersecurity and privacy protection*.

Deze derde editie herroept en vervangt de tweede editie (ISO/IEC 27002:2013), die technisch is herzien. Deze editie bevat ook de technische corrigenda ISO/IEC 27002:2013/Cor. 1:2014 en ISO/IEC 27002:2013/Cor. 2:2015),

De belangrijkste wijzigingen zijn als volgt:

- De titel is aangepast.
- De structuur van het document is gewijzigd, waarbij de beheersmaatregelen met behulp van een eenvoudige taxonomie en gerelateerde attributen worden gepresenteerd.
- Sommige beheersmaatregelen zijn samengevoegd, andere gewist en er is een aantal nieuwe beheersmaatregelen geïntroduceerd. Het volledige overzicht van hoe de beheersmaatregelen met elkaar overeenstemmen, is te vinden in bijlage B.

Deze gecorrigeerde versie van ISO/IEC 27002:2022 bevat de volgende correcties:

- niet-functionerende hyperlinks zijn in het hele document hersteld;
- in de inleidende tabel in paragraaf 5.22 en in tabel A.1 (rij 5.22) is ‘#Borging\_van\_informatie-beveiliging’ verplaatst van de kolom met de kop ‘Beveiligingsdomeinen’ naar de kolom met de kop ‘Operationele capaciteiten’.

Eventuele feedback of vragen over dit document behoren te worden gericht aan het nationale normalisatie-instituut voor de gebruiker. Een volledig overzicht van deze instituten is te vinden op [www.iso.org/members.html](http://www.iso.org/members.html) en [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Inleiding

### 0.1 Achtergrond en context

Dit document is ontworpen voor organisaties van elk type en elke omvang. Het is bedoeld als referentie voor het vaststellen en implementeren van beheersmaatregelen voor het omgaan met informatiebeveiligingsrisico's in een op ISO/IEC 27001 gebaseerd managementsysteem voor informatiebeveiliging (ISMS). Het kan ook worden gebruikt als leidraad voor organisaties die algemeen aanvaarde beheersmaatregelen op het gebied van informatiebeveiliging vaststellen en implementeren. Bovendien is dit document bedoeld voor het ontwikkelen van sector- en organisatiespecifieke richtlijnen voor informatiebeveiligingsbeheer die rekening houden met de specifieke informatiebeveiligingsrisico-omgevingen van die sectoren en organisaties. Andere dan de in dit document opgenomen organisatie- of omgevingsspecifieke beheersmaatregelen kunnen aan de hand van een risicobeoordeling worden vastgesteld voor zover dat nodig is.

Organisaties van elk type en elke omvang (met inbegrip van openbare, particuliere, commerciële en non-profitorganisaties) maken, verzamelen, verwerken, bewaren, verzenden en verwijderen informatie in vele vormen, waaronder elektronisch, fysiek en mondeling (bijv. via gesprekken en presentaties).

De waarde van informatie is niet beperkt tot het geschreven woord, getallen en figuren: kennis, concepten, ideeën en merken zijn voorbeelden van immateriële vormen van informatie. In een onderling verbonden wereld verdienen of vereisen informatie en andere gerelateerde bedrijfsmiddelen bescherming tegen diverse natuurlijke, onbedoelde of opzettelijke bronnen van risico.

Informatiebeveiliging wordt bereikt door een passende reeks beheersmaatregelen te implementeren met inbegrip van beleid, regels, processen, procedures, organisatiestructuren en software- en hardwarefuncties. Om te bewerkstelligen dat aan de specifieke veiligheids- en bedrijfsdoelstellingen van de organisatie wordt voldaan, behoort de organisatie deze beheersmaatregelen waar nodig te definiëren, implementeren, monitoren, beoordelen en verbeteren. Een ISMS zoals omschreven in ISO/IEC 27001 benadert de informatiebeveiligingsrisico's van de organisatie holistisch en gecoördineerd met het doel om een allesomvattende reeks beheersmaatregelen voor informatiebeveiliging vast te stellen en te implementeren binnen het algehele kader van een samenhangend managementsysteem.

Veel informatiesystemen, met inbegrip van het beheer en de uitvoering ervan, zijn niet ontworpen rekening houdend met de beveiligingsaspecten in termen van een ISMS zoals gespecificeerd in ISO/IEC 27001 en dit document. Het niveau van beveiliging dat kan worden bereikt door alleen technische middelen toe te passen, is beperkt en behoort te worden ondersteund door passende beheeractiviteiten en processen van de organisatie. Het bepalen van de passende beheersmaatregelen vereist zorgvuldige planning en aandacht voor details waarbij risicobehandeling wordt uitgevoerd.

Een succesvol ISMS vereist de inzet van al het personeel binnen de organisatie. Ook participatie van andere belanghebbenden, zoals aandeelhouders of leveranciers, kan vereist zijn. Ook kan advies van inhoudelijke deskundigen nodig zijn.

Een passend, toereikend en doeltreffend managementsysteem voor informatiebeveiliging biedt het management van de organisatie en andere belanghebbenden de waarborg dat hun informatie en andere gerelateerde bedrijfsmiddelen redelijk beveiligd en beschermd tegen dreigingen en schade worden gehouden, waardoor de organisatie in staat wordt gesteld de kenbaar gemaakte bedrijfsdoelstellingen te bereiken.

## 0.2 Informatiebeveiligingseisen

Het is essentieel dat een organisatie haar informatiebeveiligingseisen vaststelt.. Er zijn drie belangrijke bronnen voor informatiebeveiligingseisen:

- a) de beoordeling van de risico's waar de organisatie aan blootgesteld is, rekening houdend met de algehele bedrijfsstrategie en -doelstellingen. Een informatiebeveiligingsspecifieke risicobeoordeling kan dit mogelijk maken of ondersteunen. Dit behoort te leiden tot het vaststellen van de beheersmaatregelen die nodig zijn om te bewerkstelligen dat het restrisico voor de organisatie aan haar aanvaardingscriteria voor risico's voldoet;
- b) de eisen van wet- en regelgeving, statutaire en contractuele eisen waaraan een organisatie en haar belanghebbenden (handelspartners, dienstverleners enz.) moeten voldoen, en hun sociaal-culturele omgeving;
- c) de reeks van principes, doelstellingen en bedrijfseisen die gelden voor alle stappen van de levenscyclus van informatie die een organisatie heeft ontwikkeld om haar bedrijfsvoering te ondersteunen.

## 0.3 Beheersmaatregelen

Een beheersmaatregel wordt gedefinieerd als een maatregel waarmee risico's worden gewijzigd of in stand gehouden. Bepaalde beheersmaatregelen in dit document zijn beheersmaatregelen waarmee risico's worden gewijzigd, terwijl andere beheersmaatregelen risico's in stand houden. Een informatiebeveiligingsbeleid bijvoorbeeld kan alleen risico's in stand houden, terwijl naleving van het informatiebeveiligingsbeleid risico's kan wijzigen. Daarnaast beschrijven sommige beheersmaatregelen dezelfde generieke maatregel in verschillende risicocontexten. Dit document geeft een generieke mix van organisatorische, mensgerichte, fysieke en technologische beheersmaatregelen voor informatiebeveiliging die zijn ontleend aan internationaal erkende 'best practices'.

## 0.4 Beheersmaatregelen vaststellen

Het vaststellen van beheersmaatregelen is afhankelijk van de beslissingen van de organisatie na een risicobeoordeling, met een duidelijk gedefinieerde reikwijdte. Beslissingen met betrekking tot geïdentificeerde risico's behoren te worden gebaseerd op de criteria voor het accepteren van risico's, de opties voor het behandelen van risico's en de benadering van risicobeheer die door de organisatie wordt toegepast. Beheersmaatregelen behoren ook met inachtneming van alle relevante nationale en internationale wet- en regelgeving te worden vastgesteld. Welke beheersmaatregelen worden vastgesteld, hangt ook samen met hoe beheersmaatregelen op elkaar inwerken om diepteverdediging te bewerkstelligen.

De organisatie kan beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen. Bij het specificeren van dergelijke beheersmaatregelen behoort de organisatie de middelen en investeringen die nodig zijn om een beheersmaatregel te implementeren en uit te voeren af te zetten tegen de bedrijfswaarde die ermee wordt gerealiseerd. Zie ISO/IEC TR 27016 voor richtlijnen over beslissingen over investeren in een ISMS en de economische gevolgen van deze beslissingen in de context van concurrerende eisen voor middelen.

Er behoort een evenwicht te zijn tussen de middelen die worden ingezet voor het implementeren van beheersmaatregelen en de impact die voor het bedrijf het gevolg kan zijn als er zich beveiligingsincidenten voordoen terwijl die beheersmaatregelen ontbreken. De resultaten van een risicobeoordeling behoren te dienen als richtlijn en het management te helpen bij het bepalen van de passende actie, de prioriteiten voor het beheer van informatiebeveiligingsrisico's en voor het

implementeren van beheersmaatregelen waarvan is vastgesteld dat ze nodig zijn ter bescherming tegen deze risico's.

Een aantal van de beheersmaatregelen in dit document kan worden beschouwd als richtlijn voor informatiebeveiligingsbeheer en als van toepassing op de meeste organisaties. Meer informatie over het vaststellen van beheersmaatregelen en andere opties voor het behandelen van risico's is te vinden in ISO/IEC 27005.

### 0.5 Organisatiespecifieke richtlijnen ontwikkelen

Dit document kan worden beschouwd als uitgangspunt voor het ontwikkelen van organisatie-specifieke richtlijnen. Niet alle beheersmaatregelen en richtlijnen in dit document kunnen op alle organisaties van toepassing zijn. Met het oog op de specifieke behoeften van de organisatie en de geïdentificeerde risico's kunnen aanvullende beheersmaatregelen en richtlijnen vereist zijn die niet in deze norm zijn opgepakt. Als er documenten zijn ontwikkeld die aanvullende richtlijnen of beheersmaatregelen bevatten, kan het nuttig zijn kruisverwijzingen op te nemen naar hoofdstukken in dit document voor toekomstige verwijzing.

### 0.6 Levenscyclusoverwegingen

Informatie heeft een levenscyclus, van aanmaken tot vernietiging. De waarde van en risico's voor informatie kunnen gedurende de gehele levenscyclus van de informatie variëren (bijv. ongeoorloofde openbaarmaking of diefstal van de financiële rekeningen van een bedrijf is niet belangrijk nadat deze zijn gepubliceerd, maar integriteit blijft van kritisch belang), en daarom blijft informatiebeveiliging tot op zekere hoogte in alle stadia belangrijk.

Informatiesystemen en andere voor informatiebeveiliging relevante bedrijfsmiddelen hebben levenscycli waarbinnen ze worden gemaakt, gespecificeerd, ontworpen, ontwikkeld, getest, geïmplementeerd, gebruikt, onderhouden en ten slotte buiten bedrijf worden gesteld en verwijderd. In elk stadium behoort informatiebeveiliging in aanmerking te worden genomen. Nieuwe systeemontwikkelprojecten en wijzigingen aan bestaande systemen bieden kansen om beveiligingsbeheersmaatregelen te verbeteren, rekening houdend met de risico's voor de organisatie en uit incidenten getrokken lering.

### 0.7 Gerelateerde internationale normen

Terwijl dit document richtlijnen biedt voor een brede waaier aan beheersmaatregelen voor informatiebeveiliging die in veel verschillende organisaties gangbaar zijn, bieden andere documenten in de ISO/IEC 27000-familie aanvullende eisen of advies met betrekking tot andere aspecten van het algehele proces van informatiebeveiligingsbeheer.

Zie ISO/IEC 27000 voor een algemene inleiding in ISMS en de documentenfamilie. ISO/IEC 27000 biedt een glossarium dat de meeste in de ISO/IEC 27000-documentenfamilie gebruikte termen definieert, en beschrijft het onderwerp, toepassingsgebied en de doelstellingen voor elk onderdeel van de familie.

Er zijn sectorspecifieke normen met aanvullende beheersmaatregelen die zich op specifieke gebieden richten (bijv. ISO/IEC 27017 voor clouddiensten, ISO/IEC 27701 voor privacy, ISO/IEC 27019 voor energie, ISO/IEC 27011 voor telecommunicatie-organisaties en ISO 27799 voor de zorg). Deze normen zijn opgenomen in de bibliografie en naar sommige ervan wordt verwezen in de onderdelen met richtlijnen en overige informatie in de hoofdstukken 5 t/m 8.

# Informatiebeveiliging, cybersecurity en bescherming van de privacy – Beheersmaatregelen voor informatiebeveiliging

## 1 Onderwerp en toepassingsgebied

Dit document geeft een referentieverzameling van generieke beheersmaatregelen voor informatiebeveiliging met inbegrip van implementatierichtlijnen. Dit document is ontworpen om te worden gebruikt door organisaties:

- a) binnen de context van een managementsysteem voor informatiebeveiliging (ISMS) op basis van ISO/IEC 27001;
- b) om beheersmaatregelen voor informatiebeveiliging op basis van internationaal erkende 'best practices' te implementeren;
- c) voor het ontwikkelen van organisatiespecifieke richtlijnen voor informatiebeveiligingsbeheer.

## 2 Normatieve verwijzingen

In dit document staan geen normatieve verwijzingen.

## 3 Termen, definities en afgekorte termen

### 3.1 Termen en definities

In het kader van dit document zijn de volgende termen en definities van toepassing.

ISO en IEC onderhouden op de volgende adressen terminologiedatabases voor gebruik in het kader van normalisatie:

— ISO Online browsing platform: te bereiken op <https://www.iso.org/obp>

— IEC Electropedia: te bereiken op <https://www.electropedia.org/>

#### 3.1.1

##### **toegangsbeveiliging**

middel om te zorgen dat fysieke en logische toegang tot *bedrijfsmiddelen* (3.1.2) wordt goedgekeurd en beperkt op basis van de eisen voor bedrijfsvoering en informatiebeveiliging

#### 3.1.2

##### **bedrijfsmiddel**

alles wat waarde heeft voor de organisatie

Opmerking 1 bij de term: In de context van informatiebeveiliging kunnen twee soorten bedrijfsmiddelen worden onderscheiden:

- de primaire bedrijfsmiddelen:
  - informatie;
  - bedrijfsprocessen (3.1.27) en -activiteiten;

- de ondersteunende bedrijfsmiddelen (waarop de primaire bedrijfsmiddelen steunen) van allerlei soorten, bijvoorbeeld:
  - hardware;
  - software;
  - netwerk;
  - *personeel* (3.1.20);
  - locatie;
  - structuur van de organisatie.

### 3.1.3

#### **aanval**

geslaagde of mislukte onbevoegde poging om een *bedrijfsmiddel* (3.1.2) te vernietigen, aan te passen, buiten werking te stellen of er toegang toe te verkrijgen, of een poging om een *bedrijfsmiddel* (3.1.2) openbaar te maken, te stelen of er onbevoegd gebruik van te maken

### 3.1.4

#### **authenticatie**

het verschaffen van zekerheid met betrekking tot de juistheid van een geclaimde karakteristiek van een *entiteit* (3.1.11)

### 3.1.5

#### **authenticiteit**

eigenschap dat een *entiteit* (3.1.11) is wat zij claimt te zijn

### 3.1.6

#### **bewakingsketen**

aantoonba(a)r(e) bezit, verplaatsing, behandeling en locatie van materiaal vanaf een bepaald moment tot een ander moment

Opmerking 1 bij de term: Materiaal omvat informatie en andere gerelateerde *bedrijfsmiddelen* (3.1.2) in de context van ISO/IEC 27002.

[BRON: ISO/IEC 27050-1:2019, 3.1, gewijzigd – Opmerking 1 bij de term toegevoegd]

### 3.1.7

#### **vertrouwelijke informatie**

informatie die niet bedoeld is om beschikbaar of bekend te worden gemaakt aan onbevoegde personen, *entiteiten* (3.1.11) of *processen* (3.1.27)

### 3.1.8

#### **beheersmaatregel**

maatregel die risico in stand houdt en/of wijzigt

Opmerking 1 bij de term: Een beheersmaatregel kan onder andere elke vorm van *proces* (3.1.27), *beleid* (3.1.24), voorziening, werkwijze of andere omstandigheid of maatregel zijn waarmee het risico in stand wordt gehouden en/of wordt gewijzigd.

Opmerking 2 bij de term: Beheersmaatregelen hebben mogelijk niet altijd het beoogde of veronderstelde wijzigende effect.

[BRON: ISO 31000:2018, 3.8]

**3.1.9****verstoring**

incident, al dan niet geanticipeerd, dat een niet-geplande, negatieve afwijking van de verwachte levering van producten en diensten volgens de doelstellingen van een organisatie veroorzaakt

[BRON: ISO 22301:2019, 3.10]

**3.1.10****'endpoint device'**

met een netwerk verbonden informatie- en communicatietechnologie (ICT)-hardwareapparaat

Opmerking 1 bij de term: 'Endpoint device' kan verwijzen naar pc's, laptops, smartphones, tablets, thin clients, printers of andere specialistische hardware waaronder slimme meters en IoT- ('internet of things') apparaten.

**3.1.11****entiteit**

object dat relevant is voor het uitvoeringsdoel van een domein dat een herkenbaar onderscheiden bestaan heeft

Opmerking 1 bij de term: Een entiteit kan een fysieke of een logische belichaming hebben.

VOORBEELD Een persoon, een organisatie, een apparaat, een groep van dergelijke objecten, een menselijke abonnee op een telecommunicatiedienst, een simkaart, een paspoort, een netwerkinterfacekaart, een softwaretoepassing, een dienst of een website.

[BRON: ISO/IEC 24760-1:2019, 3.1.1]

**3.1.12****informatieverwerkende faciliteit**

elk informatieverwerkend(e) systeem, dienst of infrastructuur of de fysieke locatie waar dit of deze is ondergebracht

[BRON: ISO/IEC 27000:2018, 3.27, gewijzigd – faciliteiten is vervangen door faciliteit]

**3.1.13****inbreuk op de informatiebeveiliging**

compromittering van de informatiebeveiliging die leidt tot ongewenst(e) vernietiging, verlies, wijziging, bekendmaking van of toegang tot verzonden, opgeslagen of anderszins verwerkte beschermde informatie

**3.1.14****informatiebeveiligingsgebeurtenis**

voorval dat op een mogelijke *inbreuk op de informatiebeveiliging* (3.1.13) of een falen van *beheersmaatregelen* (3.1.8) duidt

[BRON: ISO/IEC 27035-1:2016, 3.3, gewijzigd – niet relevant voor de Nederlandse vertaling]

**3.1.15****informatiebeveiligingsincident**

een of meer samenhangende en geïdentificeerde *informatiebeveiligingsgebeurtenissen* (3.1.14) die de *bedrijfsmiddelen* (3.1.2) van een organisatie kunnen schaden of haar bedrijfsvoering kunnen compromitteren

[BRON: ISO/IEC 27035-1:2016, 3.4]

### 3.1.16

#### **beheer van informatiebeveiligingsincidenten**

uitoefening van een consequente en doeltreffende aanpak bij het behandelen van *informatiebeveiligingsincidenten* (3.1.15)

[BRON: ISO/IEC 27035-1:2016, 3.5]

### 3.1.17

#### **informatiesysteem**

stelsel van toepassingen, diensten, informatietechnologische *bedrijfsmiddelen* (3.1.2) of andere gegevensverwerkende componenten

[BRON: ISO/IEC 27000:2018, 3.35]

### 3.1.18

#### **belanghebbende**

stakeholder

persoon of organisatie die een besluit of activiteit kan beïnvloeden, door een besluit of activiteit kan worden beïnvloed, of zichzelf beschouwt als beïnvloed door een besluit of activiteit

[BRON: ISO/IEC 27000:2018, 3.37]

### 3.1.19

#### **onweerlegbaarheid**

vermogen om te bewijzen dat een geclaimde gebeurtenis of actie zich heeft voorgedaan en welke *entiteiten* (3.1.11) deze hebben veroorzaakt

### 3.1.20

#### **personeel**

personen die onder leiding van de organisatie werk verrichten

Opmerking 1 bij de term: Het concept van personeel omvat de leden van de organisatie, zoals het bestuursorgaan, de directie, medewerkers, tijdelijke medewerkers, contractanten en vrijwilligers.

### 3.1.21

#### **persoonsgegevens**

alle informatie die a) kan worden gebruikt om een verband te leggen tussen de informatie en de natuurlijke persoon op wie die informatie betrekking heeft, of b) direct of indirect met een natuurlijke persoon in verband wordt of kan worden gebracht

Opmerking 1 bij de term: De 'natuurlijke persoon' in de definitie is de *betrokkene* (3.1.22). Om vast te stellen of een betrokkene geïdentificeerd kan worden, behoort rekening te worden gehouden met alle middelen die redelijkerwijs door de privacystakeholder die de gegevens in bezit heeft of door een andere partij kunnen worden gebruikt om het verband te leggen tussen de verzameling persoonsgegevens en de natuurlijke persoon.

[BRON: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

### 3.1.22

#### **betrokkene**

natuurlijke persoon op wie de *persoonsgegevens* (3.1.21) betrekking hebben

Opmerking 1 bij de term: Afhankelijk van de jurisdictie en de specifieke databescherming- en privacywetgeving, kan het synoniem 'datasubject' worden gebruikt in plaats van de term 'betrokkene'.

[BRON: ISO/IEC 29100:2011, 2.11]

**3.1.23****verwerker van persoonsgegevens**

privacystakeholder die *persoonsgegevens* (3.1.21) namens en volgens de instructies van een verwerkingsverantwoordelijke verwerkt \*)

[BRON: ISO/IEC 29100:2011, 2.12]

**3.1.24****beleid**

intenties en richting van een organisatie zoals formeel door haar directie kenbaar gemaakt

[BRON: ISO/IEC 27000:2018, 3.53]

**3.1.25****privacy-effectbeoordeling \*\*)****PEB**

algeheel *proces* (3.1.27) van het identificeren, analyseren, evalueren, raadplegen, communiceren en plannen van de behandeling van mogelijke privacy-effecten met betrekking tot de verwerking van *persoonsgegevens* (3.1.21), ingekaderd binnen het bredere risicobeheerkader van een organisatie

[BRON: ISO/IEC 29134:2017, 3.7, gewijzigd – Opmerking 1 bij de term verwijderd.]

**3.1.26****procedure**

gespecificeerde wijze van uitvoering van een activiteit of *proces* (3.1.27)

[BRON: ISO 30000:2009, 3.12]

**3.1.27****proces**

geheel van samenhangende of elkaar beïnvloedende activiteiten die input gebruiken of omzetten om een resultaat te leveren

[BRON: ISO 9000:2015, 3.4.1, gewijzigd – Opmerkingen bij de term verwijderd.]

**3.1.28****registratie**

informatie die als bewijs en als *bedrijfsmiddel* (3.1.2) wordt aangemaakt, ontvangen en onderhouden door een organisatie of persoon om wettelijke verplichtingen na te komen of voor zakelijke transacties

Opmerking 1 bij de term: Wettelijke verplichtingen omvatten in deze context alle eisen van wet- en regelgeving, statutaire en contractuele eisen.

[BRON: ISO 15489-1:2016, 3.14, gewijzigd – Opmerking 1 bij de term toegevoegd.]

---

\*) Nederlandse voetnoot: Vgl. de definitie van Cyberveilig Nederland: 'De partij die (als leverancier) persoonsgegevens verwerkt in opdracht en ten behoeve van de verwerkingsverantwoordelijke (diens klant)'

\*\*) Nederlandse voetnoot: In Nederland wordt een DPIA ('Data Protection Impact Assessment') gehanteerd. Een organisatie onderzoekt vooraf wat de risico's van gegevensverwerking zijn voor de privacy van personen. Dit is vaak verplicht volgens de Algemene verordening gegevensbescherming. (Bron: Cyberveilig Nederland)

**3.1.29**

**RPO**

punt in de tijd waarnaar gegevens moeten worden hersteld nadat er zich een *verstoring* (3.1.9) heeft voorgedaan

[BRON: ISO/IEC 27031:2011, 3.12]

**3.1.30**

**hersteltijddoelstelling**

recovery time objective

**RTO**

tijdperiode waarbinnen minimale niveaus van diensten en/of producten en de ondersteunende systemen, toepassingen of functies moeten worden hersteld nadat er zich een *verstoring* (3.1.9) heeft voorgedaan

[BRON: ISO/IEC 27031:2011, 3.13]

**3.1.31**

**betrouwbaarheid**

eigenschap van consistent beoogd gedrag en consistente beoogde resultaten

**3.1.32**

**regel**

aanvaard beginsel of aanvaarde instructie waarin de verwachtingen van de organisatie over welke handelingen vereist zijn, wat is toegestaan of niet is toegestaan uiteen worden gezet

Opmerking 1 bij de term: Regels kunnen formeel kenbaar worden gemaakt in *onderwerpspecifieke beleidsregels* (3.1.35) en andere soorten documenten.

**3.1.33**

**gevoelige informatie**

informatie die dient te worden beschermd tegen het niet-beschikbaar zijn, onbevoegde toegang, wijziging of openbaarmaking vanwege mogelijke nadelige gevolgen voor een persoon, organisatie, de nationale veiligheid of de openbare veiligheid

**3.1.34**

**dreiging \*)**

potentiële oorzaak van een ongewenst incident dat kan resulteren in schade aan een systeem of een organisatie

[BRON: ISO/IEC 27000:2018, 3.74]

**3.1.35**

**onderwerpspecifiek beleid**

oogmerken en sturing voor een specifiek onderwerp of thema, zoals formeel kenbaar gemaakt door het passende managementniveau

Opmerking 1 bij de term: Onderwerpspecifieke beleidsregels kunnen formeel *regels* (3.1.32) of normen van de organisatie kenbaar maken.

---

\*) Nederlandse voetnoot: In NEN-ISO/IEC 27000 vertaald als 'bedreiging', maar tegenwoordig heeft de term 'dreiging' de voorkeur.

Opmerking 2 bij de term: Bepaalde organisaties gebruiken andere termen voor deze onderwerpspecifieke beleidsregels.

Opmerking 3 bij de term: De onderwerpspecifieke beleidsregels waarnaar in dit document wordt verwezen, houden verband met informatiebeveiliging.

VOORBEELD Onderwerpspecifiek beleid inzake *toegangsbeveiliging* (3.1.1), onderwerpspecifiek beleid inzake 'clear desk' en 'clear screen'.

### 3.1.36

#### **gebruiker**

*belanghebbende* (3.1.18) met toegang tot de *informatiesystemen* (3.1.17) van de organisatie

VOORBEELD *Personeel* (3.1.20), klanten, leveranciers.

### 3.1.37

#### **'endpoint device' van gebruiker**

'*endpoint device*' (3.1.10) waarmee gebruikers toegang krijgen tot informatieverwerkende diensten

Opmerking 1 bij de term: 'Endpoint device' van gebruiker kan verwijzen naar pc's, laptops, smartphones, tablets, thin clients enz.

### 3.1.38

#### **kwetsbaarheid**

zwak punt van een *bedrijfsmiddel* (3.1.2) of *beheersmaatregel* (3.1.8) waar een of meer *dreigingen* (3.1.34) gebruik van kunnen maken

[BRON: ISO/IEC 27000:2018, 3.77]

## 3.2 Afgekorte termen

ABAC	attribute-based access control
ACL	access control list
BIA	business impact analysis
BYOD	bring your own device
CAPTCHA	completely automated public Turing test to tell computers and humans apart
CPU	central processing unit
DAC	discretionary access control
DNS	domain name system
gps	global positioning system
IAM	identity and access management
ICT	information and communication technology
ID	identifier
IDE	integrated development environment
IDS	intrusion detection system

## ISO/IEC 27002:2022 (nl)

IoT	internet of things
IP	internetprotocol
IPS	intrusion prevention system
IT	information technology
ISMS	information security management system
MAC	mandatory access control
NTP	network time protocol
PIA	privacy impact assessment
PII	personally identifiable information
pin	personal identification number
PKI	public key infrastructure
PTP	precision time protocol
RBAC	role-based access control
RPO	recovery point objective
RTO	recovery time objective
SAST	static application security testing
SD	secure digital
SDN	software-defined networking
SD-WAN	software-defined wide area networking
SIEM	security information and event management
sms	short message service
SQL	structured query language
SSO	single sign on
SWID	software identification
UEBA	user and entity behaviour analytics
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus
VM	virtual machine
VPN	virtual private network
wifi	wireless fidelity

## 4 Structuur van dit document

### 4.1 Hoofdstukken

Dit document is als volgt ingedeeld:

- a) Organisatorische beheersmaatregelen (hoofdstuk 5)
- b) Mensgerichte beheersmaatregelen (hoofdstuk 6)
- c) Fysieke beheersmaatregelen (hoofdstuk 7)
- d) Technologische beheersmaatregelen (hoofdstuk 8)

Er zijn 2 informatieve bijlagen:

- Bijlage A – Attributen gebruiken
- Bijlage B – Overeenstemming met ISO/IEC 27002:2013

In bijlage A wordt uitgelegd hoe een organisatie attributen (zie 4.2) kan gebruiken om haar eigen overzichten aan te maken op basis van de in dit document gedefinieerde of zelfbedachte attributen voor beheersmaatregelen.

Bijlage B laat zien hoe de beheersmaatregelen in deze editie van ISO/IEC 27002 overeenstemmen met de vorige editie uit 2013.

### 4.2 Thema's en attributen

De categorieën waarin beheersmaatregelen kunnen worden ingedeeld volgens de hoofdstukken 5 t/m 8 worden aangeduid als thema's.

Beheersmaatregelen worden ingedeeld in de categorieën:

- a) mensgericht, als ze betrekking hebben op individuele personen;
- b) fysiek, als ze betrekking hebben op fysieke objecten;
- c) technologisch, als ze betrekking hebben op technologie;
- d) organisatorisch, in de overige gevallen.

De organisatie kan attributen gebruiken om verschillende overzichten te creëren. Dit zijn verschillende indelingen in categorieën van beheersmaatregelen, gezien vanuit een ander perspectief op de thema's. Attributen kunnen worden gebruikt om beheersmaatregelen in verschillende overzichten te filteren, sorteren of presenteren voor verschillende doelgroepen. In bijlage A wordt uitgelegd hoe dit kan worden bereikt en wordt een voorbeeld van een overzicht gegeven.

Bij wijze van voorbeeld is elke beheersmaatregel in dit document gerelateerd aan vijf attributen met bijbehorende attribuutwaarden (vooraafgegaan door '#' om ze opzoekbaar te maken) <sup>\*)</sup>. Dit is als volgt opgebouwd:

### a) Type beheersmaatregel

Type beheersmaatregel is een attribuut om beheersmaatregelen te bezien vanuit het oogpunt van wanneer en hoe de beheersmaatregel tot veranderingen van het risico leidt met betrekking tot het zich voordoen van een informatiebeveiligingsincident. De attribuutwaarden bestaan uit #Preventief (de beheersmaatregel is ervoor bedoeld te voorkomen dat er zich een informatiebeveiligingsincident voordoet), #Detectief (de beheersmaatregel treedt in werking wanneer er zich een informatiebeveiligingsincident voordoet) en #Corrigerend (de beheersmaatregel treedt in werking nadat er zich een informatiebeveiligingsincident heeft voorgedaan).

### b) Informatiebeveiligingseigenschappen

Informatiebeveiligingseigenschappen is een attribuut om beheersmaatregelen te bezien vanuit het oogpunt: aan het behoud van welk kenmerk van informatie draagt de beheersmaatregel bij? De attribuutwaarden bestaan uit #Vertrouwelijkheid, #Integriteit en #Beschikbaarheid.

### c) Cybersecurityconcepten

Cybersecurityconcepten is een attribuut om beheersmaatregelen te bekijken vanuit het oogpunt van het verband tussen beheersmaatregelen en de in het in ISO/IEC TS 27110 beschreven cybersecuritykader gedefinieerde cybersecurityconcepten. Deze attribuutwaarden bestaan uit #Identificeren, #Beschermen, #Detecteren, #Reageren en #Herstellen.

### d) Operationele capaciteiten

Operationele capaciteiten is een attribuut om beheersmaatregelen te bekijken vanuit het perspectief van beroepsbeoefenaren op informatiebeveiligingscapaciteiten. De attribuutwaarden bestaan uit #Governance, #Beheer\_van\_bedrijfsmiddelen, #Informatiebescherming, #Personeelsbeveiliging, #Fysieke\_beveiliging, #Systeem-\_en\_netwerkbeveiliging, #Toepassingsbeveiliging, #Veilige\_configuratie, #Identiteits-\_en\_toegangsbeheer, #Beheer\_van\_dreigingen\_en\_kwetsbaarheden, #Continuïteit, #Beveiliging\_in\_leveranciersrelaties, #Juridisch\_en\_compliance, #Beheer\_van\_informatiebeveiligingsgebeurtenissen en #Borging\_van\_informatiebeveiliging.

### e) Beveiligingsdomeinen

Beveiligingsdomeinen is een attribuut om beheersmaatregelen te bekijken vanuit het oogpunt van vier informatiebeveiligingsdomeinen: 'Governance\_en\_Ecosysteem' omvat 'Information System Security Governance & Risk Management' en 'Ecosystem cybersecurity management' (inclusief interne en externe belanghebbenden); 'Bescherming' omvat 'IT-beveiligingsarchitectuur', 'IT-beveiligingsbeheer', 'Identiteits- en toegangsbeheer', 'IT-beveiligingsonderhoud' en 'Fysieke en omgevingsbeveiliging'; 'Verdediging' omvat 'Detectie' en 'Computer Security Incident Management'; onder 'Veerkracht' (Resilience) wordt verstaan 'Continuïteit van de bedrijfsvoering' en 'Crisisbeheersing'. De attribuutwaarden bestaan uit #Governance\_en\_Ecosysteem, #Bescherming, #Verdediging en #Veerkracht.

---

<sup>\*)</sup> Nederlandse voetnoot: In deze vertaling zijn ook in 4.2 de attribuutwaarden van een '#' voorzien.

De in dit document vermelde attributen zijn gekozen op basis van het feit dat ze als generiek genoeg worden beschouwd om door verschillende soorten organisaties te worden gebruikt. Organisaties kunnen ervoor kiezen een of meer van de in dit document vermelde attributen buiten beschouwing te laten. Ze kunnen ook zelf attributen (met de bijbehorende attribuutwaarden) aanmaken om hun eigen organisatieoverzichten te maken. Hoofdstuk A.2 bevat voorbeelden van dergelijke attributen.

### 4.3 Indeling beheersmaatregel

De indeling van elke beheersmaatregel bevat het volgende:

- **Titel van de beheersmaatregel:** Korte naam van de beheersmaatregel;
- **Attribuuttabel:** Een tabel toont de waarde(n) van elk attribuut voor de beheersmaatregel in kwestie;
- **Beheersmaatregel:** Wat de beheersmaatregel is;
- **Doel:** Waarom de beheersmaatregel behoort te worden geïmplementeerd;
- **Richtlijn:** Hoe de beheersmaatregel behoort te worden geïmplementeerd;
- **Overige informatie:** Tekst met uitleg of verwijzingen naar andere gerelateerde documenten.

Omwille van de leesbaarheid zijn lange richtlijnteksten die op meer onderwerpen ingaan, soms onderverdeeld. De titels van deze secties zijn onderstreept.

## 5 Organisatorische beheersmaatregelen

### 5.1 Beleidsregels voor informatiebeveiliging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Eco-systeem #Veerkracht

#### **Beheersmaatregel**

Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoren te worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.

#### **Doel**

De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management overeenkomstig de bedrijfseisen en de eisen van wet- en regelgeving, statutaire en contractuele eisen bewerkstelligen.

## **Richtlijn**

De organisatie behoort op het hoogste niveau een 'informatiebeveiligingsbeleid' te definiëren dat is goedgekeurd door de directie en dat de aanpak van de organisatie beschrijft om haar informatiebeveiliging te bereiken.

Het informatiebeveiligingsbeleid behoort eisen in aanmerking te nemen die zijn ontleend aan:

- a) bedrijfsstrategie en -eisen;
- b) wet- en regelgeving en contracten;
- c) de huidige en verwachte risico's en dreigingen inzake informatiebeveiliging.

Het informatiebeveiligingsbeleid behoort uiteenzettingen te bevatten betreffende:

- a) de definitie van informatiebeveiliging;
- b) informatiebeveiligingsdoelstellingen of het kader voor het vaststellen van informatiebeveiligingsdoelstellingen;
- c) principes die als leidraad dienen voor alle activiteiten in verband met informatiebeveiliging;
- d) een verbintenis om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging;
- e) een verbintenis tot continue verbetering van het managementsysteem voor informatiebeveiliging;
- f) toekenning van verantwoordelijkheden voor informatiebeveiligingsbeheer aan gedefinieerde rollen;
- g) procedures voor het behandelen van vrijgestelde situaties en uitzonderingen.

Eventuele wijzigingen aan het informatiebeveiligingsbeleid behoren ter goedkeuring aan de directie te worden voorgelegd.

Op een lager niveau behoort het informatiebeveiligingsbeleid te worden ondersteund door onderwerpspecifieke beleidsregels naarmate nodig is, om de implementatie van beheersmaatregelen voor informatiebeveiliging verder verplicht te stellen. De typische structuur van onderwerpspecifieke beleidsregels is dusdanig dat ze ingaan op de behoeften van bepaalde doelgroepen binnen een organisatie of dat ze bepaalde beveiligingsgebieden bestrijken. Onderwerpspecifieke beleidsregels behoren te worden afgestemd op het informatiebeveiligingsbeleid van de organisatie en dit aan te vullen.

Voorbeelden van dergelijke onderwerpen zijn:

- a) toegangsbeveiliging;
- b) fysieke beveiliging en beveiliging van de omgeving;
- c) beheer van bedrijfsmiddelen;
- d) overdragen van informatie;
- e) beveiligde configuratie van en omgang met 'endpoint devices' van gebruikers;

- f) netwerkbeveiliging;
- g) beheer van informatiebeveiligingsincidenten;
- h) back-up;
- i) cryptografie en sleutelbeheer;
- j) classificatie van en omgaan met informatie;
- k) beheer van technische kwetsbaarheden;
- l) veilig ontwikkelen.

De verantwoordelijkheid voor het ontwikkelen, beoordelen en goedkeuren van de onderwerpspecifieke beleidsregels behoort te worden toegewezen aan relevant personeel, op basis van passend bevoegdheidsniveau en technische bekwaamheid. De beoordeling behoort mede het beoordelen te omvatten van mogelijkheden voor het verbeteren van het informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels en het informatiebeveiligingsbeheer van de organisatie als antwoord op veranderingen in:

- a) de bedrijfsstrategie van de organisatie;
- b) de technische omgeving van de organisatie;
- c) wet- en regelgeving en contracten;
- d) informatiebeveiligingsrisico's;
- e) huidige en verwachte dreigingen inzake informatiebeveiliging;
- f) lering die wordt getrokken uit informatiebeveiligingsgebeurtenissen en -incidenten.

Bij de beoordeling van informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoort rekening te worden gehouden met de resultaten van directiebeoordelingen en audits. Indien er één beleidsregel wordt gewijzigd, behoort, met het oog op de consistentie, te worden overwogen ook andere gerelateerde beleidsregels te beoordelen en bij te werken.

Het informatiebeveiligingsbeleid en de onderwerpspecifieke beleidsregels behoren in een vorm die relevant, toegankelijk en begrijpelijk is voor de beoogde lezer te worden gecommuniceerd aan relevant personeel en relevante belanghebbenden. Van ontvangers van de beleidsregels behoort te worden verlangd dat ze bevestigen dat ze de beleidsregels, indien van toepassing, begrijpen en zich eraan zullen houden. De organisatie kan voor deze beleidsdocumenten formaten en namen vaststellen die aan de behoeften van de organisatie voldoen. In bepaalde organisaties kunnen het informatiebeveiligingsbeleid en de onderwerpspecifieke beleidsregels in een en hetzelfde document worden opgenomen. De organisatie kan deze onderwerpspecifieke beleidsregels aanduiden als normen, richtlijnen, beleidsregels enz.

Als het informatiebeveiligingsbeleid of een onderwerpspecifieke beleidsregel buiten de organisatie wordt verspreid, behoort erop te worden gelet dat geen vertrouwelijke informatie openbaar wordt gemaakt.

Tabel 1 illustreert de verschillen tussen informatiebeveiligingsbeleid en onderwerpspecifiek beleid.

**Tabel 1 — Verschillen tussen informatiebeveiligingsbeleid en onderwerpspecifiek beleid**

	Informatiebeveiligingsbeleid	Onderwerpspecifiek beleid
<b>Detailniveau</b>	Algemeen of op hoofdlijnen	Specifiek en gedetailleerd
<b>Gedocumenteerd en formeel goedgekeurd door</b>	De directie	Het passende managementniveau

**Overige informatie**

Onderwerpspecifieke beleidsregels kunnen van organisatie tot organisatie verschillen.

**5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht

**Beheersmaatregel**

Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.

**Doel**

Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.

**Richtlijn**

Het toewijzen van de rollen en verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met het beleid voor informatiebeveiliging en onderwerpspecifieke beleidsregels (zie 5.1). De organisatie behoort verantwoordelijkheden te definiëren en te beheren voor:

- de bescherming van informatie en andere gerelateerde bedrijfsmiddelen;
- het uitvoeren van specifieke informatiebeveiligingsprocessen;
- beheeractiviteiten met betrekking tot informatiebeveiligingsrisico's en in het bijzonder voor het accepteren van de overblijvende risico's (bijv. voor de eigenaren van risico's);
- al het personeel dat gebruikmaakt van informatie en andere gerelateerde bedrijfsmiddelen van een organisatie.

Deze verantwoordelijkheden behoren waar nodig te worden aangevuld met meer gedetailleerde richtlijnen voor specifieke locaties en informatieverwerkende faciliteiten. Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend, kunnen beveiligingstaken aan

anderen toewijzen. Zij blijven echter verantwoordelijk en behoren vast te stellen of gedelegeerde taken correct zijn verricht.

Elk beveiligingsgebied waarvoor personen verantwoordelijk zijn, behoort te worden gedefinieerd, gedocumenteerd en gecommuniceerd. Autorisatieniveaus behoren te worden gedefinieerd en gedocumenteerd. Personen die een specifieke rol op het gebied van informatiebeveiliging op zich nemen, behoren competent te zijn wat betreft de kennis en vaardigheden die de rol vereist en behoren te worden ondersteund bij het op de hoogte blijven van de ontwikkelingen die verband houden met de rol en die vereist zijn om aan de verantwoordelijkheden van de rol te kunnen voldoen.

### Overige informatie

Veel organisaties benoemen een manager informatiebeveiliging die de algehele verantwoordelijkheid draagt voor de ontwikkeling en implementatie van informatiebeveiliging en om de identificatie van risico's en beperkende beheersmaatregelen te ondersteunen.

Echter, de verantwoordelijkheid voor het verzorgen en implementeren van de beheersmaatregelen blijft vaak een taak van individuele managers. Een gangbare praktijk is om voor elk bedrijfsmiddel een eigenaar te benoemen die verantwoordelijk wordt voor de dagelijkse bescherming ervan.

Afhankelijk van de omvang en de middelen van een organisatie kan informatiebeveiliging door speciale rollen of door functies die naast bestaande rollen worden uitgevoerd, worden afgedekt.

## 5.3 Functiescheiding

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Governance #Identiteits- _en_toegangsbeheer	#Governance_en_Ecosys- teem

### Beheersmaatregel

Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.

### Doel

Het risico op fraude, fouten en het omzeilen van beheersmaatregelen voor informatiebeveiliging verminderen.

### Richtlijn

De functiescheiding en verantwoordelijkheidszones hebben tot doel conflicterende functies te scheiden en onder verschillende personen te verdelen om te voorkomen dat mogelijk conflicterende functies door één persoon alleen worden uitgevoerd.

De organisatie behoort vast te stellen voor welke functies en verantwoordelijkheidszones het nodig is dat ze worden gesegmenteerd. Hieronder volgen voorbeelden van activiteiten waarvoor segmentatie nodig kan zijn:

- a) het initiëren, goedkeuren en uitvoeren van een verandering;
- b) het verzoeken om, goedkeuren en implementeren van toegangsrechten;

- c) het ontwerpen, implementeren en beoordelen van code;
- d) het ontwikkelen van software en het beheren van productiesystemen;
- e) het gebruiken en beheren van toepassingen;
- f) het gebruiken van toepassingen en het beheren van databases;
- g) het ontwerpen, auditen en borgen van beheersmaatregelen voor informatiebeveiliging.

Bij het ontwerpen van beheersmaatregelen met het oog op scheiding behoort rekening te worden gehouden met de mogelijkheid van samenzwering. Voor kleine organisaties kan het moeilijk zijn om functies te scheiden, maar het principe behoort te worden toegepast voor zover dit mogelijk en haalbaar is. Wanneer het moeilijk is om functies te scheiden, behoren andere beheersmaatregelen te worden overwogen, zoals het monitoren van activiteiten, audittrajecten en supervisie door het management.

Bij het gebruik van op functies gebaseerde toegangsbeveiligingssystemen behoort ervoor te worden gezorgd dat aan personen geen conflicterende functies worden toegekend. Wanneer er een groot aantal functies is, behoort de organisatie te overwegen geautomatiseerde hulpmiddelen te gebruiken om conflicten te identificeren en de verwijdering ervan mogelijk te maken. Functies behoren zorgvuldig te worden gedefinieerd en ingesteld zodat toegangsproblemen tot een minimum kunnen worden beperkt indien een functie wordt verwijderd of opnieuw wordt toegewezen.

#### Overige informatie

Geen overige informatie.

### 5.4 Managementverantwoordelijkheden

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem

#### Beheersmaatregel

Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.

#### Doel

Bewerkstelligen dat het management zijn rol bij informatiebeveiliging begrijpt en maatregelen neemt om ervoor te zorgen dat al het personeel zich bewust is van zijn verantwoordelijkheden op het gebied van informatiebeveiliging en deze ook nakomt.

#### Richtlijn

Het management behoort er blijk van te geven dat het het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels, procedures en beheersmaatregelen voor informatiebeveiliging ondersteunt.

Het management behoort ervoor te zorgen dat personeelsleden:

- a) op de juiste manier worden geïnstrueerd over hun informatiebeveiligingsrollen en -verantwoordelijkheden voordat zij toegang krijgen tot informatie en andere gerelateerde bedrijfsmiddelen van de organisatie;
- b) richtlijnen ontvangen die de verwachtingen met betrekking tot hun informatiebeveiligingsrol binnen de organisatie aangeven;
- c) verplicht worden te voldoen aan het informatiebeveiligingsbeleid en de onderwerpspecifieke beleidsregels van de organisatie;
- d) een niveau van bewustwording van informatiebeveiliging bereiken dat relevant is voor hun rollen en verantwoordelijkheden binnen de organisatie (zie 6.3);
- e) de arbeids- of contractvoorwaarden en de voorwaarden van overeenkomsten, met inbegrip van het informatiebeveiligingsbeleid en passende werkmethoden, naleven \*);
- f) de passende vaardigheden en kwalificaties op het gebied van informatiebeveiliging blijven houden door voortdurende bijscholing;
- g) waar mogelijk, een vertrouwelijk kanaal krijgen om overtredingen van het informatiebeveiligingsbeleid, onderwerpspecifiek beleid of procedures voor informatiebeveiliging te melden ('klokkenluiden'). Dit kan anonieme meldingen mogelijk maken, of bepalingen bevatten die ervoor zorgen dat de identiteit van de melder alleen bekend is bij degenen die dergelijke meldingen moeten behandelen;
- h) voldoende middelen en tijd voor projectplanning krijgen voor het implementeren van de beveiligingsgerelateerde processen en beheersmaatregelen van de organisatie.

#### Overige informatie

Geen overige informatie.

### 5.5 Contact met overheidsinstanties

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Reageren #Herstellen	#Governance	#Verdediging #Veerkracht

#### Beheersmaatregel

De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.

#### Doel

Een passende stroom van informatie met betrekking tot informatiebeveiliging tussen de organisatie en relevante juridische, regelgevende en toezichthoudende instanties bewerkstelligen.

\*) Nederlandse voetnoot: Anders geformuleerd dan in de brontekst,

## Richtlijn

De organisatie behoort aan te geven wanneer en door wie contact behoort te worden opgenomen met overheidsinstanties (bijv. politie, regelgevende organen, toezichthouders) en hoe geïdentificeerde informatiebeveiligingsincidenten tijdig behoren te worden gemeld.

Contacten met overheidsinstanties behoren ook te worden gebruikt om inzicht mogelijk te maken in de bestaande en toekomstige verwachtingen van deze instanties (bijv. toepasselijke regelgeving met betrekking tot informatiebeveiliging).

## Overige informatie

Organisaties die worden aangevallen, kunnen instanties verzoeken om actie te ondernemen tegen de aanvaller.

Het onderhouden van dergelijke contacten kan een eis zijn voor het ondersteunen van het beheer van informatiebeveiligingsincidenten (zie 5.24 t/m 5.28) of de noodplan- en bedrijfscontinuïteitsprocessen (zie 5.29 en 5.30). Contacten met regelgevende organen zijn ook nuttig om te anticiperen op en voorbereidingen te treffen voor komende veranderingen in relevante wet- en regelgeving die op de organisatie van invloed zijn. Contacten met andere instanties omvatten contacten met nutsbedrijven, eerstehulpdiensten, elektriciteitsleveranciers en gezondheids- en veiligheidsinstanties [bijv. de brandweer (in verband met de bedrijfscontinuïteit), telecommunicatiebedrijven (in verband met verbindingen en beschikbaarheid) en waterleidingbedrijven (in verband met koelvoorzieningen voor apparatuur)].

## 5.6 Contact met speciale belangengroepen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren #Herstellen	#Governance	#Verdediging

### Beheersmaatregel

De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.

### Doel

Een passende stroom van informatie met betrekking tot informatiebeveiliging bewerkstelligen.

### Richtlijn

Lidmaatschap van speciale belangengroepen of fora behoort te worden overwogen als middel om:

- kennis te verbeteren over 'best practices' en op de hoogte te blijven van relevante beveiligingsinformatie;
- ervoor te zorgen dat de kennis van informatiebeveiliging actueel is;
- vroegtijdige waarschuwingen te ontvangen inzake alarm, adviezen en patches die verband houden met aanvallen en kwetsbaarheden;
- toegang te krijgen tot gespecialiseerd advies over informatiebeveiliging;

- e) informatie over nieuwe technologieën, producten, diensten, dreigingen of kwetsbaarheden te delen en uit te wisselen;
- f) geschikte contactpunten te verkrijgen als er informatiebeveiligingsincidenten aan de orde zijn (zie 5.24 t/m 5.28).

### Overige informatie

Geen overige informatie.

## 5.7 Informatie en analyses over dreigingen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Detecteren #Reageren	#Beheer_van_dreigingen _en_kwetsbaarheden	#Verdediging #Veerkracht

### Beheersmaatregel

Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.

### Doel

Bewustwording bieden van de mogelijke dreigingen voor de organisatie zodat de passende mitigerende maatregelen kunnen worden getroffen.

### Richtlijn

Informatie over bestaande of opkomende dreigingen wordt verzameld en geanalyseerd teneinde:

- a) weloverwogen maatregelen mogelijk te maken om te voorkomen dat de dreigingen schade aan de organisatie toebrengen;
- b) de impact van dergelijke dreigingen te beperken.

Informatie en analyses over dreigingen kunnen in drie lagen worden opgedeeld die alle drie in aanmerking behoren te worden genomen:

- a) informatie over strategische dreigingen: uitwisseling van informatie op hoofdlijnen over het veranderende dreigingslandschap (bijv. soorten aanvallers of soorten aanvallen);
- b) informatie en analyses over tactische dreigingen: informatie over de desbetreffende methodieken, instrumenten en technologieën waarvan aanvallers zich bedienen;
- c) informatie en analyses over operationele dreigingen: details over specifieke aanvallen, met inbegrip van technische indicatoren.

Informatie en analyses over dreigingen behoren:

- a) relevant te zijn (d.w.z. verband te houden met de bescherming van de organisatie);
- b) inzicht te bieden (d.w.z. de organisatie een nauwkeurig en gedetailleerd inzicht te verschaffen in het dreigingslandschap);
- c) contextueel te zijn om situationeel bewustwording te bieden (d.w.z. door context toe te voegen aan de informatie op basis van het tijdstip van de gebeurtenissen, waar zij zich voordoen, eerdere ervaringen en prevalentie in soortgelijke organisaties);
- d) bruikbaar te zijn (d.w.z. dat de organisatie snel en doeltreffend kan handelen op basis van de informatie).

Activiteiten op het gebied van informatie en analyses over dreigingen behoren het volgende te omvatten:

- a) het vaststellen van doelstellingen voor het produceren van informatie en analyses over dreigingen;
- b) het identificeren, doorlichten en selecteren van interne en externe informatiebronnen die nodig en geschikt zijn om te voorzien in informatie die vereist is om de gewenste informatie en analyses over dreigingen te produceren;
- c) het verzamelen van informatie uit geselecteerde interne en externe bronnen;
- d) het verwerken van verzamelde informatie om deze voor te bereiden op analyse (bijv. door informatie te vertalen, op te maken of te bevestigen);
- e) het analyseren van informatie om inzicht te krijgen in hoe deze verband houdt met de organisatie en de betekenis ervan voor de organisatie;
- f) het in een begrijpelijke vorm meedelen ervan aan en delen met relevante personen.

Informatie over dreigingen behoort te worden geanalyseerd en later te worden gebruikt:

- a) door processen te implementeren om uit bronnen van informatie en analyses over dreigingen verzamelde informatie op te nemen in de beheerprocessen voor informatiebeveiligingsrisico's van de organisatie;
- b) als aanvullende input voor technische preventieve en detectieve beheersmaatregelen, zoals firewalls, inbraakdetectiesystemen of antimalwareoplossingen;
- c) als input voor de processen en technieken voor het testen van de informatiebeveiliging.

De organisatie behoort informatie en analyses over dreigingen op wederzijdse basis met andere organisaties te delen om de algemene informatie en analyses over dreigingen te verbeteren.

### **Overige informatie**

Organisaties kunnen informatie en analyses over dreigingen gebruiken om dreigingen te voorkomen, detecteren of erop te reageren. Organisaties kunnen zelf informatie en analyses over dreigingen produceren, maar het is gebruikelijker dat ze informatie en analyses over dreigingen ontvangen en gebruiken die door andere bronnen wordt geproduceerd.

Informatie en analyses over dreigingen worden vaak verstrekt door onafhankelijke aanbieders of adviseurs, overheidsinstanties of groepen die gezamenlijk informatie over dreigingen verzamelen en analyseren.

De doeltreffendheid van beheersmaatregelen zoals 5.25, 8.7, 8.16 of 8.23 is afhankelijk van de kwaliteit van de beschikbare informatie en analyses over dreigingen.

## 5.8 Informatiebeveiliging in projectmanagement

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Governance	#Governance_en_Ecosysteem #Bescherming

### Beheersmaatregel

Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.

### Doel

Ervoor zorgen dat informatiebeveiligingsrisico's binnen projecten en te leveren producten en diensten gedurende de gehele levenscyclus van het project op doeltreffende wijze binnen het projectmanagement worden aangepakt.

### Richtlijn

Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement om ervoor te zorgen dat informatiebeveiligingsrisico's in het kader van projectmanagement worden aangepakt. Dit kan worden toegepast op elk type project ongeacht de complexiteit, omvang, duur, discipline of het toepassingsgebied (bijv. een project voor een proces voor kernactiviteiten, IT, 'facility management' of andere ondersteunende processen).

Het projectmanagement dat wordt toegepast, behoort te vereisen dat:

- a) informatiebeveiligingsrisico's tijdens een vroeg stadium en periodiek gedurende de volledige levenscyclus van het project als onderdeel van de projectrisico's worden beoordeeld en behandeld;
- b) informatiebeveiligingseisen [bijv. beveiligingseisen voor toepassingen (8.26), eisen inzake de naleving van intellectuele-eigendomsrechten (5.32) enz.] in de vroege stadia van projecten worden aangepakt;
- c) informatiebeveiligingsrisico's in verband met de uitvoering van projecten, zoals de beveiliging van interne en externe communicatieaspecten, gedurende de gehele levenscyclus van het project in aanmerking worden genomen en behandeld;
- d) de vorderingen met betrekking tot de behandeling van informatiebeveiligingsrisico's worden beoordeeld en de doeltreffendheid van de behandeling wordt beoordeeld en beproefd.

De passendheid van de informatiebeveiligingsoverwegingen en -activiteiten behoort in vooraf bepaalde stadia te worden gecontroleerd door geschikte personen of governance-instanties, zoals de projectstuurgroep.

Verantwoordelijkheden en bevoegdheden voor informatiebeveiliging relevant voor het project behoren te worden gedefinieerd en te worden toegewezen aan gespecificeerde rollen.

Informatiebeveiligingseisen voor door het project te leveren producten of diensten behoren te worden vastgesteld met gebruikmaking van verschillende methoden zoals het afleiden van nalevingseisen uit informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en regelgeving. Verdere informatiebeveiligingseisen kunnen worden ontleend aan activiteiten zoals dreigingsmodellering, beoordelingen van incidenten, het gebruik van kwetsbaarheidsdrempels of het opstellen van noodplannen om zo te bewerkstelligen dat de architectuur en het ontwerp van informatiesystemen worden beschermd tegen bekende dreigingen die gebaseerd zijn op de operationele omgeving.

Er behoren informatiebeveiligingseisen te worden vastgesteld voor alle soorten projecten, niet alleen voor ICT-ontwikkelprojecten. Bij het vaststellen van deze eisen behoort ook het volgende in aanmerking te worden genomen:

- a) welke informatie het betreft (vaststelling van de informatie), wat de bijbehorende informatiebeveiligingsbehoeften zijn (classificatie; zie 5.12) en de mogelijke negatieve bedrijfsimpact die het gevolg kan zijn van ontoereikende beveiliging;
- b) de noodzaak om de desbetreffende informatie en andere gerelateerde bedrijfsmiddelen te beschermen, met name wat betreft vertrouwelijkheid, integriteit en beschikbaarheid;
- c) de vereiste mate van betrouwbaarheid of zekerheid ten opzichte van de beweerde identiteit van entiteiten om de authenticatie-eisen af te leiden;
- d) processen voor het verlenen van toegang en autorisatie, voor klanten en andere zakelijke gebruikers en voor bevoorrechte of technische gebruikers, zoals relevante projectleden, mogelijk operationeel personeel of externe leveranciers;
- e) het informeren van gebruikers over hun plichten en verantwoordelijkheden;
- f) eisen die zijn afgeleid van bedrijfsprocessen, zoals registreren en monitoren van transacties, eisen voor onweerlegbaarheid;
- g) eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot informatiebeveiliging (bijv. interfaces voor het registreren en monitoren of systemen voor het detecteren van lekken van gegevens);
- h) naleving van de wettelijke, statutaire, regelgevende en contractuele omgeving waarin de organisatie actief is;
- i) het vereiste niveau van vertrouwen of zekerheid dat derden zullen voldoen aan het informatiebeveiligingsbeleid en de onderwerpspecifieke beleidsregels van de organisatie, met inbegrip van relevante beveiligingsclausules in overeenkomsten of contracten.

### Overige informatie

De projectontwikkelaanpak, zoals de Waterfall-levenscyclus of de Agile-levenscyclus, behoort gestructureerde informatiebeveiliging te ondersteunen die kan worden aangepast aan de volgens een beoordeling vastgestelde informatiebeveiligingsrisico's, aansluitend bij het karakter van het project. Het vroegtijdig nadenken over informatiebeveiligingseisen voor het product of de dienst (bijv. tijdens de plannings- en ontwerpfasen) kan leiden tot doeltreffender en kostenefficiëntere oplossingen voor kwaliteits- en informatiebeveiliging. ISO 21500 en ISO 21502 geven richtlijnen voor projectmanagementconcepten en -processen die belangrijk zijn voor de prestaties van projecten.

ISO/IEC 27005 geeft richtlijnen voor het gebruik van risicobeheerprocessen om beheersmaatregelen te identificeren die aan informatiebeveiligingseisen voldoen.

## 5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beheer_van_bedrijfsmiddelen	#Governance_en_Ecosysteem #Bescherming

### Beheersmaatregel

Er behoort een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, te worden opgesteld en onderhouden.

### Doel

De informatie en andere gerelateerde bedrijfsmiddelen van de organisatie identificeren om de informatiebeveiliging ervan te behouden en passend eigenaarschap toe te wijzen.

### Richtlijn

#### Inventarislijst

De organisatie behoort haar informatie en andere gerelateerde bedrijfsmiddelen te identificeren en het belang ervan wat betreft informatiebeveiliging vast te stellen. Documentatie behoort te worden onderhouden in speciale of bestaande inventarislijsten indien van toepassing.

De inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen behoort nauwkeurig, actueel, consistent en in overeenstemming met andere inventarisoverzichten te zijn. Opties om de nauwkeurigheid van een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen te bewerkstelligen zijn onder andere:

- regelmatig beoordelingen van geïdentificeerde informatie en andere gerelateerde bedrijfsmiddelen aan de hand van de inventarislijst van bedrijfsmiddelen uitvoeren;
- de inventarislijst automatisch laten bijwerken als er een bedrijfsmiddel wordt geïnstalleerd, gewijzigd of verwijderd.

De locatie van een bedrijfsmiddel behoort al naargelang de situatie in de inventarislijst te worden opgenomen.

De inventarislijst hoeft niet één lijst te zijn van informatie en andere gerelateerde bedrijfsmiddelen. Aangezien de inventarislijst van bedrijfsmiddelen door de relevante functies behoort te worden onderhouden, kan deze worden beschouwd als een verzameling dynamische inventarislijsten, zoals inventarislijsten voor informatiebedrijfsmiddelen, hardware, software, virtuele machines (VM's), faciliteiten, personeel, competenties, capaciteiten en registraties.

Elk bedrijfsmiddel behoort te worden geclassificeerd overeenkomstig de classificatie van de met dat bedrijfsmiddel gerelateerde informatie (zie 5.12).

Het niveau van granulariteit van de inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen behoort te passen bij de behoeften van de organisatie. Soms is het vanwege de aard

van het bedrijfsmiddel niet praktisch uitvoerbaar om specifieke instanties van bedrijfsmiddelen in de informatielevenscyclus te documenteren. Een voorbeeld van een bedrijfsmiddel met een korte levensduur is een instantie van een VM die van korte duur kan zijn.

### Eigendom

Voor de geïdentificeerde informatie- en andere gerelateerde bedrijfsmiddelen behoort de eigendom van het bedrijfsmiddel te worden toegewezen aan een persoon of een groep en behoort de classificatie te worden geïdentificeerd (zie 5.12, 5.13). Er behoort een procedure te worden geïmplementeerd die ervoor zorgt dat de benoeming van de eigenaar van bedrijfsmiddelen tijdig plaatsvindt. Het eigenaarschap behoort te worden toegekend als bedrijfsmiddelen worden aangemaakt of als bedrijfsmiddelen naar de organisatie worden overgebracht. Het eigenaarschap van een bedrijfsmiddel behoort naarmate nodig is opnieuw te worden toegekend wanneer de huidige eigenaren van een bedrijfsmiddel vertrekken of een andere functie krijgen.

### Taken van de eigenaar

De eigenaar van het bedrijfsmiddel behoort verantwoordelijk te zijn voor het juiste beheer ervan voor de gehele levenscyclus van het bedrijfsmiddel en behoort ervoor te zorgen dat:

- a) informatie en andere gerelateerde bedrijfsmiddelen worden geïnventariseerd;
- b) informatie en andere gerelateerde bedrijfsmiddelen passend worden geclassificeerd en beschermd;
- c) de classificatie periodiek wordt beoordeeld;
- d) er een lijst wordt opgesteld van de componenten die technologische bedrijfsmiddelen ondersteunen, zoals database-, opslag-, softwarecomponenten en -subcomponenten, en deze worden gekoppeld;
- e) eisen voor het aanvaardbare gebruik van informatie en andere gerelateerde bedrijfsmiddelen (zie 5.10) worden vastgesteld;
- f) de toegangsbeperkingen overeenstemmen met de classificatie, doeltreffend zijn en periodiek worden beoordeeld;
- g) informatie en andere gerelateerde bedrijfsmiddelen die worden gewist of verwijderd, veilig worden behandeld en uit de inventarislijst worden verwijderd;
- h) hij betrokken is bij het identificeren en het beheer van de risico's in verband met zijn bedrijfsmiddel(en);
- i) hij het personeel ondersteunt dat de rollen en de verantwoordelijkheden heeft voor het beheren van zijn informatie.

### **Overige informatie**

Inventarislijsten van informatie en andere gerelateerde bedrijfsmiddelen zijn vaak nodig om de doeltreffende bescherming van informatie zeker te stellen en kunnen voor andere doeleinden vereist zijn, zoals om gezondheids- en veiligheids-, verzekerings- of financiële redenen. Inventarislijsten van informatie en andere gerelateerde bedrijfsmiddelen ondersteunen ook risicobeheer, auditactiviteiten, kwetsbaarhedenbeheer, incidentrespons- en herstelplanning.

Taken en verantwoordelijkheden kunnen worden gedelegeerd (bijv. aan een beheerder die de dagelijkse zorg heeft over de bedrijfsmiddelen), maar de persoon of groep die ze heeft gedelegeerd blijft verantwoordelijk.

Het kan nuttig zijn om groepen van informatie en andere gerelateerde bedrijfsmiddelen aan te wijzen die samen een bepaalde dienst verlenen. In dat geval is de eigenaar van deze dienst verantwoordelijk voor het leveren van de dienst, met inbegrip van de werking van de bedrijfsmiddelen die de dienst verzorgen.

Zie ISO/IEC 19770-1 voor aanvullende informatie over het beheer van IT-bedrijfsmiddelen. Zie ISO 55001 voor aanvullende informatie over het beheer van bedrijfsmiddelen.

## 5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Governance_en_Ecosysteem #Bescherming

### Beheersmaatregel

Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden vastgesteld, gedocumenteerd en geïmplementeerd.

### Doel

Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen passend worden beschermd, gebruikt en behandeld.

### Richtlijn

Personeel en externe gebruikers die informatie en andere gerelateerde bedrijfsmiddelen van de organisatie gebruiken of er toegang toe hebben, behoren bewust te worden gemaakt van de informatiebeveiligingseisen voor het beschermen van en omgaan met de informatie van de organisatie en andere gerelateerde bedrijfsmiddelen. Zij behoren verantwoordelijk te zijn voor het gebruik dat zij maken van informatieverwerkende faciliteiten.

De organisatie behoort onderwerpspecifiek beleid inzake het aanvaardbare gebruik van informatie en andere gerelateerde bedrijfsmiddelen vast te stellen en dit mee te delen aan iedereen die informatie en andere gerelateerde bedrijfsmiddelen gebruikt of hanteert. Het onderwerpspecifieke beleid inzake aanvaardbaar gebruik behoort duidelijk aan te geven hoe van personen wordt verwacht dat ze informatie en andere gerelateerde bedrijfsmiddelen gebruiken. In het onderwerpspecifieke beleid behoort het volgende te worden opgenomen:

- verwacht en onaanvaardbaar gedrag van personen vanuit het oogpunt van informatiebeveiliging;
- wat wordt beschouwd als toegestaan en verboden gebruik van informatie en andere gerelateerde bedrijfsmiddelen;
- welke monitoringactiviteiten de organisatie uitvoert.

Er behoren procedures voor aanvaardbaar gebruik te worden opgesteld voor de volledige levenscyclus van de informatie overeenkomstig de classificatie ervan (zie 5.12) en de vastgestelde risico's. Met de volgende aspecten behoort rekening te worden gehouden:

- a) toegangsbeperkingen die de beschermingseisen van elk classificatieniveau ondersteunen;
- b) onderhoud van een registratie van de bevoegde gebruikers van informatie en andere gerelateerde bedrijfsmiddelen;
- c) bescherming van tijdelijke of permanente kopieën van de informatie tot een niveau dat consistent is met de bescherming van de originele informatie;
- d) opslag van bedrijfsmiddelen die samenhangen met informatie in overeenstemming met de voorschriften van de fabrikant (zie 7.8);
- e) duidelijke markering van alle kopieën van (elektronische of fysieke) opslagmedia ter attentie van de bevoegde ontvanger (zie 7.10);
- f) autorisatie van het verwijderen van informatie en andere gerelateerde bedrijfsmiddelen en ondersteunde wismethode(n) (zie 8.10).

### Overige informatie

Het is mogelijk dat de desbetreffende bedrijfsmiddelen niet direct tot de organisatie behoren, zoals openbare clouddiensten. Het gebruik van zulke bedrijfsmiddelen van derden en van bedrijfsmiddelen van de organisatie in verband met zulke externe bedrijfsmiddelen (bijv. informatie, software) behoort te worden geïdentificeerd al naargelang de situatie en beheerst, bijv. door middel van overeenkomsten met aanbieders van clouddiensten. Indien er gebruik wordt gemaakt van een op samenwerking gerichte werkomgeving, behoort er ook zorgvuldig te worden gehandeld.

## 5.11 Retourneren van bedrijfsmiddelen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen	#Bescherming

### Beheersmaatregel

Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren.

### Doel

De bedrijfsmiddelen van de organisatie beschermen als onderdeel van de procedure voor het wijzigen of beëindigen van het dienstverband, het contract of de overeenkomst.

### Richtlijn

In de wijzigings- of beëindigingsprocedure behoort formeel het retourneren van alle eerder verstrekte fysieke en elektronische bedrijfsmiddelen die het eigendom zijn van of toevertrouwd zijn aan de organisatie, te worden opgenomen.

Ingeval personeel en andere belanghebbenden apparatuur van de organisatie kopen of eigen persoonlijke apparatuur gebruiken, behoren procedures te worden gevolgd om ervoor te zorgen dat alle relevante informatie wordt getraceerd en aan de organisatie wordt overgedragen en nauwkeurig van de apparatuur wordt verwijderd (zie 7.14).

Indien personeel en andere belanghebbenden beschikken over kennis die belangrijk is voor de lopende bedrijfsvoering, behoort die informatie te worden gedocumenteerd en aan de organisatie te worden overgedragen.

Tijdens de opzegtermijn en daarna behoort de organisatie het onbevoegd kopiëren van relevante informatie (bijv. intellectuele eigendom) door personeel van wie het dienstverband is opgezegd, te voorkomen.

De organisatie behoort alle te retourneren informatie en andere gerelateerde bedrijfsmiddelen duidelijk te identificeren en documenteren. Deze informatie en bedrijfsmiddelen kunnen onder andere zijn:

- a) 'endpoint devices' van gebruikers;
- b) draagbare opslagapparatuur;
- c) specialistische apparatuur;
- d) authenticatiehardware (bijv. mechanische sleutels, fysieke tokens en chipkaarten) voor informatiesystemen, locaties en fysieke archieven;
- e) fysieke kopieën van informatie.

### Overige informatie

Het kan lastig zijn informatie te retourneren die zich bevindt op bedrijfsmiddelen die geen eigendom zijn van de organisatie. In dergelijke gevallen is het nodig het gebruik van informatie door middel van andere beheersmaatregelen voor informatiebeveiliging, zoals het beheer van toegangsrechten (5.18) of het gebruik van cryptografie (8.24) te beperken.

## 5.12 Classificeren van informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Informatiebe-scherming	#Bescherming #Verdediging

### Beheersmaatregel

Informatie behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante belanghebbenden.

### Doel

Bewerkstelligen dat het identificeren van en het inzicht in de beschermingsbehoeften voor informatie in overeenstemming zijn met het belang ervan voor de organisatie.

## **Richtlijn**

De organisatie behoort een onderwerpspecifiek beleid inzake het classificeren van informatie vast te stellen en aan alle relevante belanghebbenden mee te delen.

De organisatie behoort in het classificatieschema rekening te houden met eisen voor vertrouwelijkheid, integriteit en beschikbaarheid.

Classificaties en gerelateerde beschermende beheersmaatregelen voor informatie behoren rekening te houden met de bedrijfsbehoeften ten aanzien van het delen of beperken van informatie, het beschermen van de integriteit van informatie en het waarborgen van beschikbaarheid, alsmede wettelijke eisen met betrekking tot de vertrouwelijkheid, integriteit of beschikbaarheid van de informatie. Andere bedrijfsmiddelen dan informatie kunnen ook worden geclassificeerd in overeenstemming met de classificatie van informatie die is opgeslagen in, verwerkt door of anderszins behandeld of beschermd door het bedrijfsmiddel.

Eigenaren van informatie behoren verantwoordelijk te zijn voor de classificatie ervan.

Het classificatieschema behoort regels voor het classificeren te bevatten en criteria voor het na verloop van tijd opnieuw beoordelen van de classificatie. Resultaten van classificatie behoren te worden geactualiseerd in overeenstemming met wijzigingen in de waarde, gevoeligheid en het belang van informatie in de loop van de levenscyclus.

Het schema behoort te worden afgestemd op het onderwerpspecifieke beleid inzake toegangsbeveiliging (zie 5.1) en het behoort te kunnen ingaan op specifieke bedrijfsbehoeften van de organisatie.

De classificatie kan worden vastgesteld aan de hand van de mate van effect die compromittering van de informatie zou hebben op de organisatie. Elk in het schema gedefinieerd niveau behoort een naam te krijgen die betekenis heeft in de context van de toepassing van het classificatieschema.

Het schema behoort organisatiebreed consistent te zijn en te zijn opgenomen in de procedures van de organisatie zodat iedereen informatie en relevante andere gerelateerde bedrijfsmiddelen op dezelfde manier classificeert. Op deze manier heeft iedereen een gemeenschappelijk begrip van beschermingseisen en past iedereen de passende bescherming toe.

Het binnen de organisatie gebruikte classificatieschema kan verschillen van de schema's die andere organisaties gebruiken, zelf als de namen voor niveaus op elkaar lijken. Bovendien kan de classificatie van informatie die tussen organisaties wordt getransporteerd verschillen, afhankelijk van de context ervan binnen elke organisatie, zelfs als de organisaties dezelfde classificatieschema's gebruiken. Daarom behoren overeenkomsten met andere organisaties waarin het delen van informatie voorkomt, procedures te bevatten voor het identificeren van de classificatie van die informatie en voor het interpreteren van de classificatieniveaus van andere organisaties. De overeenstemming tussen verschillende schema's kan worden vastgesteld door te zoeken naar gelijkwaardigheid in de gerelateerde methoden voor hantering en bescherming.

## **Overige informatie**

Classificatie biedt personen die met informatie omgaan, een beknopte indicatie van hoe deze te behandelen en te beschermen. Het aanmaken van informatiegroepen met gelijksoortige beschermingsbehoeften en het specificeren van informatiebeveiligingsprocedures die gelden voor alle informatie in elke groep, vergemakkelijken dit. Deze aanpak vermindert de behoefte aan afzonderlijke risicobeoordeling en speciaal ontworpen beheersmaatregelen.

Het is mogelijk dat informatie na verloop van tijd niet meer gevoelig of essentieel is. Als de informatie bijvoorbeeld openbaar is gemaakt, gelden er niet langer vertrouwelijkheidseisen voor, maar kan het

nog steeds nodig zijn deze vanwege de integriteits- en beschikbaarheidseigenschappen ervan te beschermen. Met deze aspecten behoort rekening te worden gehouden omdat overclassificatie kan leiden tot het implementeren van onnodige beheersmaatregelen, wat resulteert in extra kosten, terwijl onderclassificatie kan leiden tot onvoldoende beheersmaatregelen om de informatie tegen compromittering te beschermen.

Bij wijze van voorbeeld kan een classificatieschema betreffende de vertrouwelijkheid van informatie worden gebaseerd op de volgende vier niveaus:

- a) openbaarmaking veroorzaakt geen schade;
- b) openbaarmaking veroorzaakt geringe reputatieschade of een geringe operationele impact;
- c) openbaarmaking heeft een kortdurende significante impact op de operationele of bedrijfsdoelstellingen;
- d) openbaarmaking heeft een ernstige impact op de langetermijnbedrijfsdoelstellingen of brengt het voortbestaan van de organisatie in gevaar.

### 5.13 Labelen van informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Informatiebe-scherming	#Verdediging #Bescherming

#### Beheersmaatregel

Om informatie te labelen behoort een passende reeks procedures te worden vastgesteld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

#### Doel

Het communiceren van de classificatie van informatie mogelijk maken en het automatiseren van informatieverwerking en -beheer ondersteunen.

#### Richtlijn

Procedures voor het labelen van informatie behoren te gaan over informatie en andere gerelateerde bedrijfsmiddelen in alle formaten. De labeling behoort in overeenstemming te zijn met het classificatieschema vastgesteld in 5.12. De labels behoren gemakkelijk herkenbaar te zijn. De procedures behoren richtlijnen te geven over waar en hoe labels zijn bevestigd, rekening houdend met hoe de informatie wordt bereikt of hoe de bedrijfsmiddelen worden gehanteerd afhankelijk van de soorten opslagmedia. De procedures kunnen het volgende definiëren:

- a) gevallen waarin labelen niet wordt toegepast (bijv. bij niet-vertrouwelijke informatie, om de werklust te verminderen);
- b) de manier van labelen van informatie die wordt verzonden door of opgeslagen op elektronische of fysieke middelen, of een ander formaat;
- c) hoe om te gaan met gevallen waarin labelen niet mogelijk is (bijv. vanwege technische beperkingen).

Voorbeelden van labeltechnieken zijn:

- a) fysieke labels;
- b) kop- en voetteksten;
- c) metagegevens;
- d) watermerken;
- e) rubberen stempels.

Digitale informatie behoort gebruik te maken van metagegevens om informatie te identificeren, beheren en beheersen, met name wat betreft vertrouwelijkheid. Metagegevens behoren ook het doelmatig en correct zoeken naar informatie mogelijk te maken. Metagegevens behoren mogelijk te maken dat systemen interactie met elkaar hebben en op basis van de toegekende classificatielabels besluiten nemen.

De procedures behoren te beschrijven hoe metagegevens aan informatie worden gekoppeld, welke labels behoren te worden gebruikt en hoe gegevens behoren te worden gehanteerd, in overeenstemming met het informatiemodel en de ICT-architectuur van de organisatie.

Relevante aanvullende metagegevens behoren te worden toegevoegd door systemen wanneer ze informatie verwerken, afhankelijk van de informatiebeveiligingseigenschappen ervan.

Personeel en andere belanghebbenden behoren op de hoogte te worden gebracht van de labelprocedures. Al het personeel behoort de benodigde training te krijgen om te waarborgen dat informatie juist wordt gelabeld en dienovereenkomstig wordt behandeld.

Output van systemen die informatie bevatten die is geclassificeerd als gevoelig of essentieel, behoort een passend classificatielabel te dragen.

### **Overige informatie**

Het labelen van geclassificeerde informatie is een belangrijke eis voor het delen van informatie.

Andere nuttige metagegevens die aan de informatie kunnen worden gekoppeld, zijn welk proces van de organisatie de informatie heeft aangemaakt, en op welk tijdstip.

Het labelen van informatie en andere gerelateerde bedrijfsmiddelen kan soms negatieve effecten hebben. Geclassificeerde bedrijfsmiddelen zijn gemakkelijker te identificeren door kwaadwillenden, die daarvan mogelijk misbruik maken.

Bepaalde systemen voorzien individuele bestanden of registraties in databases niet van labels met de classificatie, maar beschermen alle informatie op het hoogste classificatieniveau van de informatie die erin vervat is of mag zijn. Het is gebruikelijk in dergelijke systemen dat informatie wordt geïdentificeerd en vervolgens gelabeld op het moment van exporteren.

## 5.14 Overdragen van informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfs-middelen #Informatiebescherming	#Bescherming

### Beheersmaatregel

Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.

### Doel

Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.

### Richtlijn

#### Algemeen

De organisatie behoort een onderwerpspecifiek beleid inzake de overdracht van informatie vast te stellen en aan alle relevante belanghebbenden mee te delen. Regels, procedures en overeenkomsten om informatie die wordt overgedragen te beschermen, behoren de classificatie van de desbetreffende informatie te weerspiegelen. Wanneer informatie wordt overgedragen tussen de organisatie en derden, behoren transportovereenkomsten (met inbegrip van authenticatie van de ontvanger) te worden vastgesteld en gehandhaafd om informatie in alle vormen tijdens overdracht te beschermen (zie 5.10).

Informatie kan worden overgedragen via elektronische overdracht, door fysieke opslagmedia over te dragen en via mondelinge overdracht.

Voor alle soorten van overdracht van informatie behoren de regels, procedures en overeenkomsten het volgende te omvatten:

- a) beheersmaatregelen die ervoor zijn ontworpen om overgedragen informatie te beschermen tegen interceptie, toegang door onbevoegden, kopiëren, wijziging, foutieve routing, vernietiging en 'denial of service', met inbegrip van toegangsbeveiligingsniveaus die passend zijn bij de classificatie van de desbetreffende informatie en eventuele speciale beheersmaatregelen die vereist zijn om gevoelige informatie te beschermen, zoals het gebruik van cryptografische technieken (zie 8.24);
- b) beheersmaatregelen om de traceerbaarheid en onweerlegbaarheid te waarborgen, met inbegrip van het in stand houden van een bewakingsketen voor informatie tijdens het overdragen;
- c) identificatie van passende contactpersonen met betrekking tot het overdragen, met inbegrip van de eigenaren van de informatie, risico-eigenaren, beveiligingsfunctionarissen en beheerders van informatie, voor zover van toepassing;
- d) verantwoordelijkheden en aansprakelijkheden in geval van informatiebeveiligingsincidenten, zoals verlies van fysieke opslagmedia of gegevens;

- e) gebruik van een afgesproken labelsysteem voor gevoelige of essentiële informatie dat waarborgt dat de betekenis van de labels meteen duidelijk is en dat de informatie passend is beschermd (zie 5.13);
- f) betrouwbaarheid en beschikbaarheid van de overdrachtdienst;
- g) het onderwerpspecifieke beleid of richtlijnen over aanvaardbaar gebruik van overdragen van informatiefaciliteiten (zie 5.10);
- h) richtlijnen voor het bewaren en verwijderen van alle bedrijfsregistraties, met inbegrip van berichten;

OPMERKING Er kan lokale wet- en regelgeving bestaan inzake het bewaren en verwijderen van bedrijfsregistraties.

- i) aandacht voor andere relevante eisen van wet- en regelgeving, statutaire en contractuele eisen (zie 5.31, 5.32, 5.33, 5.34) in verband met het overdragen van informatie (bijv. eisen voor elektronische handtekeningen).

#### Elektronisch transport

In regels, procedures en overeenkomsten behoort ook rekening te worden gehouden met de volgende punten bij het gebruik van elektronische communicatiefaciliteiten voor het overdragen van informatie:

- a) het detecteren van en beschermen tegen malware die kan worden overgebracht door het gebruik van elektronische communicatie (zie 8.7);
- b) bescherming van als bijlage gecommuniceerde gevoelige elektronische informatie;
- c) het voorkómen dat documenten en berichten in mededelingen naar het verkeerde adres of nummer worden gestuurd;
- d) het verkrijgen van toestemming voorafgaand aan het gebruiken van externe openbare diensten zoals instant messaging, sociale netwerken, het delen van bestanden of opslag in de cloud;
- e) sterkere authenticatieniveaus bij het overdragen van informatie via openbaar toegankelijke netwerken;
- f) beperkingen die samenhangen met het gebruik van elektronische communicatiefaciliteiten (bijv. het geautomatiseerd doorsturen van e-mail naar externe e-mailadressen voorkomen);
- g) personeel en andere belanghebbenden adviseren geen berichten met essentiële informatie via sms of andere vormen van instant messaging te verzenden, aangezien deze op openbare plekken (en derhalve door onbevoegden) kunnen worden gelezen of kunnen worden opgeslagen op apparaten die niet afdoende zijn beschermd;
- h) personeel en andere belanghebbenden informeren over problemen in verband met het gebruiken van faxapparatuur of -diensten, namelijk:
  - 1) onbevoegde toegang tot ingebouwde berichtenboxen om berichten op te vragen;
  - 2) opzettelijk of onbedoeld programmeren van machines, waardoor berichten naar bepaalde nummers worden gestuurd.

Fysiek overdragen van opslagmedia

Bij het overdragen van fysieke opslagmedia, waaronder papier, behoort in de regels, procedures en overeenkomsten ook te zijn voorzien in:

- a) verantwoordelijkheden voor het beheersen en notificeren van overdracht, verzending en ontvangst;
- b) het garanderen van correcte adressering en overdracht van het bericht;
- c) verpakking die de inhoud beschermt tegen fysieke schade waarvan aannemelijk is dat deze zich kan voordoen tijdens het overdragen en overeenkomstig de specificaties van fabrikanten, bijv. verpakking die bescherming biedt tegen omgevingsfactoren die de doeltreffendheid kunnen verminderen van het herstellen van opslagmedia, zoals blootstelling aan warmte, vocht of elektromagnetische velden; met gebruikmaking van de minimale technische normen voor verpakking en verzending (bijv. het gebruik van ondoorzichtige enveloppen);
- d) een door het management goedgekeurde lijst van goedgekeurde betrouwbare koeriers;
- e) koeriersidentificatienormen;
- f) afhankelijk van het classificatieniveau van de informatie in of op de over te dragen opslagmedia, de toepassing van beheersmaatregelen waardoor manipulatie duidelijk wordt aangetoond of die tegen manipulatie bestendig zijn (bijv. tassen, containers);
- g) procedures om de identificatie van koeriers te verifiëren;
- h) een goedgekeurde lijst van derden die vervoers- of koeriersdiensten verlenen, afhankelijk van de classificatie van de informatie;
- i) het bijhouden van registraties die de inhoud van de opslagmedia en de toegepaste bescherming identificeren, een lijst bevatten van bevoegde ontvangers waarin ook wordt vastgelegd hoe vaak de media zijn overgedragen naar de beheerder en in ontvangst zijn genomen op de plaats van bestemming.

Mondelinge overdracht

Om de mondelinge overdracht van informatie te beschermen, behoren personeel en andere belanghebbenden eraan te worden herinnerd dat zij:

- a) geen vertrouwelijke mondelinge gesprekken behoren te voeren op openbare plekken of via onveilige communicatiekanalen, aangezien deze door onbevoegden kunnen worden afgeluisterd;
- b) geen berichten die vertrouwelijke informatie bevatten, behoren achter te laten op antwoordapparaten of als spraakbericht, omdat deze kunnen worden afgespeeld door onbevoegde personen, op gemeenschappelijke systemen kunnen worden opgeslagen of onjuist kunnen worden opgeslagen als gevolg van foutieve nummerkeuze;
- c) op het juiste niveau behoren te zijn gescreend om naar het gesprek te mogen luisteren;
- d) behoren te waarborgen dat passende beheersmaatregelen voor de ruimte zijn geïmplementeerd (bijv. geluidsdichtheid, dichte deur);
- e) gevoelige gesprekken altijd behoren te beginnen met een disclaimer zodat de aanwezigen het classificatieniveau kennen van wat ze gaan horen en eventuele eisen met betrekking tot de omgang ermee.

## Overige informatie

Geen overige informatie.

### 5.15 Toegangsbeveiliging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer	#Bescherming

#### Beheersmaatregel

Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.

#### Doel

Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.

#### Richtlijn

Eigenaren van informatie en andere gerelateerde bedrijfsmiddelen behoren informatiebeveiligings- en bedrijfseisen met betrekking tot toegangsbeveiliging vast te stellen. Er behoort onderwerpspecifiek beleid inzake toegangsbeveiliging te worden gedefinieerd waarin rekening wordt gehouden met deze eisen en dit behoort naar alle desbetreffende belanghebbenden te worden gecommuniceerd.

Bij deze eisen en het onderwerpspecifieke beleid behoort rekening te worden gehouden met het volgende:

- vaststellen voor welke entiteiten welke soort toegang tot de informatie en andere gerelateerde bedrijfsmiddelen vereist is;
- beveiliging van toepassingen (zie 8.26);
- fysieke toegang waarvoor ondersteuning door passende fysieke toegangsbeveiliging nodig is (zie 7.2, 7.3, 7.4);
- regels voor informatieverspreiding en -autorisatie (bijv. het 'need-to-know'-principe), informatiebeveiligingsniveaus en -classificatie (zie 5.10, 5.12, 5.13);
- beperkingen op speciale toegangsrechten (zie 8.2);
- functiescheiding (zie 5.3);
- relevante wet- en regelgeving en contractuele verplichtingen met betrekking tot het beperken van de toegang tot gegevens of diensten (zie 5.31, 5.32, 5.33, 5.34, 8.3);
- scheiding van toegangsbeveiligingsfuncties (bijv. toegangsverzoek, -autorisatie, -administratie);
- formele autorisatie voor verzoeken om toegang (zie 5.16 en 5.18);

- j) het beheer van toegangsrechten (zie 5.18);
- k) registratie (zie 8.15).

Er behoren regels voor toegangsbeveiliging te worden geïmplementeerd door passende toegangsrechten en -beperkingen voor de desbetreffende entiteiten te definiëren en toe te wijzen (zie 5.16). Een entiteit kan zowel staan voor een menselijke gebruiker, als voor een technisch of logisch object (bijv. een machine, apparaat of dienst). Om het toegangsbeveiligingsbeheer te vereenvoudigen, kunnen er specifieke rollen aan groepen entiteiten worden toegewezen.

Bij het definiëren en implementeren van regels voor toegangsbeveiliging behoort rekening te worden gehouden met het volgende:

- a) consistentie tussen de toegangsrechten en de informatieclassificatie;
- b) consistentie tussen de toegangsrechten en de behoeften en eisen met betrekking tot de fysieke beveiliging van de buitengrenzen;
- c) het in aanmerking nemen van alle soorten beschikbare verbindingen in gedistribueerde omgevingen zodat entiteiten alleen toegang krijgen tot informatie en andere gerelateerde bedrijfsmiddelen, waaronder netwerken en netwerkdiensten waarvoor zij als gebruiker bevoegd zijn;
- d) het overwegen hoe elementen of factoren die relevant zijn voor dynamische toegangsbeveiliging kunnen worden weergegeven.

### Overige informatie

Er worden vaak overkoepelende principes gebruikt in de toegangsbeveiligingscontext. Twee van de meest gebruikte principes zijn:

- a) 'need-to-know': een entiteit krijgt alleen toegang tot de informatie die de entiteit in kwestie nodig heeft voor het uitvoeren van zijn functies (verschillende functies of rollen betekenen verschillende 'need-to-know'-informatie en daardoor verschillende toegangsprofielen);
- b) noodzaak tot gebruik ('need-to-use'): een entiteit krijgt alleen toegang tot de informatietechnologie-infrastructuur indien daarvoor een duidelijke noodzaak bestaat.

Bij het opstellen van regels voor toegangsbeveiliging behoort aandacht te worden besteed aan het volgende:

- a) het vaststellen van regels gebaseerd op de vooronderstelling van het 'least privilege' (minste rechten): 'Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten', in plaats van de zwakkere regel 'Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden';
- b) wijzigingen in informatielabels (zie 5.13) die automatisch door informatieverwerkende faciliteiten worden aangebracht, en wijzigingen die naar keuze van de gebruiker worden aangebracht;
- c) wijzigingen in toegangsrechten voor gebruikers die automatisch door het informatiesysteem worden aangebracht, en wijzigingen die door een beheerder worden aangebracht;
- d) de momenten van het definiëren en regelmatig beoordelen van de goedkeuring.

Regels voor toegangsbeveiliging behoren te worden ondersteund door formele procedures (zie 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) en gedefinieerde verantwoordelijkheden (zie 5.2, 5.17).

Er zijn diverse manieren om toegangsbeveiliging te implementeren, waaronder MAC ('mandatory access control' - verplichte toegangsbeveiliging), DAC ('discretionary access control' - discretionaire toegangsbeveiliging), RBAC ('role-based access control' - op rollen gebaseerde toegangsbeveiliging) en ABAC ('attribute-based access control' - op attributen gebaseerde toegangsbeveiliging).

Regels voor toegangsbeveiliging kunnen ook dynamische elementen bevatten (bijv. een functie die toegangsinstanties uit het verleden of specifieke omgevingswaarden beoordeelt). Regels voor toegangsbeveiliging kunnen met verschillende granulariteit worden geïmplementeerd, uiteenlopend van het afdekken van volledige netwerken of systemen tot specifieke gegevensvelden, en hierbij kunnen ook eigenschappen zoals de locatie van de gebruiker of het soort netwerkverbinding dat voor de toegang wordt gebruikt, in aanmerking worden genomen. Deze principes, evenals de wijze waarop granulaire toegangsbeveiliging wordt gedefinieerd, kunnen een aanmerkelijk kosteneffect hebben. Strengere regels en meer granulariteit leiden doorgaans tot hogere kosten. Aan de hand van bedrijfseisen en risico-overwegingen behoort te worden gedefinieerd welke regels voor toegangsbeveiliging worden toegepast en welke granulariteit vereist is.

## 5.16 Identiteitsbeheer

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-en-toegangsbeheer	#Bescherming

### Beheersmaatregel

De volledige levenscyclus van identiteiten behoort te worden beheerd.

### Doel

De unieke identificatie van personen en systemen die toegang hebben tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, en een juiste toewijzing van toegangsrechten mogelijk maken.

### Richtlijn

De processen die worden gebruikt in de context van identiteitsbeheer, behoren te bewerkstelligen dat:

- indien identiteiten aan personen zijn toegewezen, een specifieke identiteit slechts aan één persoon wordt gekoppeld zodat de persoon ertoe kan worden gehouden rekenschap af te leggen voor met deze specifieke identiteit verrichte handelingen;
- aan meer personen toegewezen identiteiten (bijv. gedeelde identiteiten) alleen zijn toegestaan wanneer ze om zakelijke of operationele redenen nodig zijn en ze aan speciale goedkeuring en documentatie worden onderworpen;
- naar behoren gescheiden goedkeuring en onafhankelijk lopend toezicht wordt uitgeoefend indien identiteiten aan niet-menselijke entiteiten zijn toegewezen;
- identiteiten tijdig gedeactiveerd of verwijderd worden als ze niet meer nodig zijn (bijv. als de gerelateerde entiteiten worden verwijderd of niet langer worden gebruikt of als de aan een identiteit gekoppelde persoon de organisatie heeft verlaten of van rol is veranderd);

- e) in een specifiek domein één enkele identiteit aan één enkele entiteit wordt gekoppeld [d.w.z. dat wordt vermeden dat meerdere identiteiten binnen dezelfde context aan dezelfde entiteit worden gekoppeld (dubbele identiteiten)];
- f) registraties worden bijgehouden van alle belangrijke gebeurtenissen betreffende het gebruik en het beheer van gebruikersidentiteiten en authenticatie-informatie.

De organisatie behoort een ondersteunend proces te hebben ingesteld voor het omgaan met veranderingen aan informatie met betrekking tot gebruikersidentiteiten. Deze processen kunnen het opnieuw verifiëren van vertrouwde documenten met betrekking tot een persoon omvatten.

Wanneer gebruik wordt gemaakt van door derden verstrekte of uitgegeven identiteiten (bijv. toegangsgegevens voor sociale media), behoort de organisatie te bewerkstelligen dat deze identiteiten van derden de vereiste mate van vertrouwen bieden en dat eventueel daarmee samenhangende risico's bekend zijn en voldoende worden behandeld. Dit kan beheersmaatregelen in verband met de derden (zie 5.19) alsmede beheersmaatregelen in verband met gerelateerde authenticatie-informatie (zie 5.17) omvatten.

### Overige informatie

Het verlenen of intrekken van toegang tot informatie en andere gerelateerde bedrijfsmiddelen is doorgaans een meerstapsprocedure:

- a) het bevestigen van de zakelijke eisen voor het vaststellen van een identiteit;
- b) het verifiëren van de identiteit van een entiteit alvorens deze een logische identiteit toe te kennen;
- c) het vaststellen van een identiteit;
- d) het configureren en activeren van de identiteit. Dit omvat ook het configureren en initieel instellen van gerelateerde authenticatiediensten;
- e) het verlenen of intrekken van specifieke toegangsrechten aan de identiteit, op basis van passende beslissingen over autorisatie of rechten (zie 5.18).

## 5.17 Beheren van authenticatie-informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer	#Bescherming

### Beheersmaatregel

De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.

### Doel

Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.

## Richtlijn

### Toewijzing van authenticatie-informatie

Het toewijzings- en beheerproces behoort te bewerkstelligen dat:

- a) tijdens inschrijfprocessen automatisch gegenereerde persoonlijke wachtwoorden of pincodes als tijdelijke geheime authenticatie informatie niet geraden kunnen worden en gebruikers deze na het eerste gebruik moeten wijzigen;
- b) er procedures worden vastgesteld om de identiteit van een gebruiker vast te stellen voordat nieuwe, vervangende of tijdelijke authenticatie-informatie wordt verstrekt;
- c) authenticatie-informatie, met inbegrip van tijdelijke authenticatie-informatie, op een beveiligde manier aan de gebruikers wordt verzonden (bijv. via een geauthenticeerd en beschermd kanaal) en het gebruik van onbeschermd (onversleutelde) e-mailberichten voor dit doel wordt vermeden;
- d) gebruikers de ontvangst van authenticatie-informatie bevestigen;
- e) standaard authenticatie-informatie zoals vooraf gedefinieerd of door verkopers verstrekt onmiddellijk na het installeren van systemen of software wordt gewijzigd;
- f) registraties van belangrijke gebeurtenissen in verband met de toewijzing en het beheer van authenticatie-informatie worden bewaard en de vertrouwelijkheid ervan gewaarborgd is, en dat de registratiemethode is goedgekeurd (bijv. met behulp van een goedgekeurd wachtwoordkluisinstrument).

### Verantwoordelijkheden van gebruikers

Elke persoon die toegang heeft tot of gebruikmaakt van authenticatie-informatie, behoort erop te worden gewezen ervoor te zorgen dat:

- a) geheime authenticatie-informatie zoals wachtwoorden geheim wordt gehouden. Persoonlijke geheime authenticatie-informatie mag niet met anderen worden gedeeld. Geheime authenticatie-informatie die wordt gebruikt in de context van identiteiten die zijn gekoppeld aan meer gebruikers of aan niet-persoonlijke entiteiten, wordt uitsluitend gedeeld met bevoegden.
- b) aangetaste of gecompromitteerde authenticatie-informatie wordt gewijzigd onmiddellijk na kennisgeving ervan of na andere aanwijzingen dat deze is gecompromitteerd;
- c) wanneer wachtwoorden als authenticatie-informatie worden gebruikt, er sterke wachtwoorden volgens aanbevelingen aan de hand van 'best practices' worden gekozen, bijvoorbeeld:
  - 1) wachtwoorden worden niet gebaseerd op gegevens die iemand anders gemakkelijk met behulp van persoonsgerelateerde informatie (zoals namen, telefoonnummers en geboortedata) kan raden of achterhalen;
  - 2) wachtwoorden worden niet gebaseerd op woordenboekwoorden of combinaties daarvan;
  - 3) gebruik gemakkelijk te onthouden wachzinnen en probeer daarin alfanumerieke en speciale tekens te gebruiken;
  - 4) wachtwoorden hebben een minimumlengte;

- d) een en hetzelfde wachtwoord niet voor verschillende diensten en op verschillende systemen wordt gebruikt;
- e) de verplichting om deze regels na te leven ook wordt opgenomen in de arbeidsovereenkomst (zie 6.2);

#### Systeem voor wachtwoordbeheer

Wanneer wachtwoorden worden gebruikt als authenticatie-informatie, behoort het wachtwoordbeheersysteem:

- a) gebruikers de mogelijkheid te bieden hun eigen wachtwoord te kiezen en te wijzigen, en een bevestigingsprocedure te bevatten om foutieve invoer te adresseren;
- b) sterke wachtwoorden af te dwingen volgens aanbevelingen aan de hand van 'best practices' [zie c) van 'Verantwoordelijkheden van gebruikers'];
- c) gebruikers te dwingen hun wachtwoord bij het eerste inloggen te wijzigen;
- d) af te dwingen dat wachtwoorden worden gewijzigd wanneer dat nodig is, bijv. na een beveiligingsincident of bij beëindiging of wijziging van dienstverband wanneer een gebruiker beschikt over bekende wachtwoorden voor identiteiten die actief blijven (bijv. gedeelde identiteiten);
- e) het hergebruik van eerdere wachtwoorden te voorkomen;
- f) het gebruik van veelgebruikte wachtwoorden en gecompromitteerde gebruikersnamen, wachtwoordcombinaties uit gehackte systemen te voorkomen;
- g) wachtwoorden niet op het scherm te tonen als ze worden ingevoerd;
- h) wachtwoorden in beschermde vorm op te slaan en te versturen.

Wachtwoordversleuteling en hashing behoren te worden uitgevoerd volgens goedgekeurde cryptografische technieken voor wachtwoorden (zie 8.24).

#### **Overige informatie**

Wachtwoorden of wachtzinnen zijn een algemeen gebruikt type authenticatie-informatie en zijn een gebruikelijk middel om de identiteit van een gebruiker te verifiëren. Andere typen authenticatie-informatie zijn cryptografische sleutels en andere gegevens die zijn opgeslagen op hardwaretokens (bijv. chipkaarten) die authenticatiecodes produceren, en biometrische gegevens zoals irisscans of vingerafdrukken. Aanvullende informatie is te vinden in de ISO/IEC 24760-reeks.

Verplichten dat wachtwoorden vaak worden gewijzigd kan een probleem zijn, aangezien gebruikers geïrriteerd kunnen raken door de frequente wijzigingen, nieuwe wachtwoorden kunnen vergeten, ze op onveilige plaatsen kunnen noteren, of onveilige wachtwoorden kunnen kiezen. Als 'Single Sign On' (SSO) of andere authenticatiebeheerinstrumenten (bijv. wachtwoordkluizen) beschikbaar worden gesteld, vermindert dat de hoeveelheid authenticatie-informatie die gebruikers moeten beschermen, waardoor de doeltreffendheid van deze beheersmaatregel kan toenemen. Echter, deze instrumenten kunnen ook de impact van openbaarmaking van authenticatie-informatie vergroten.

Bepaalde toepassingen vereisen dat wachtwoorden voor gebruikers door een onafhankelijke instantie worden toegewezen. In dergelijke gevallen zijn de punten a), c) en d) van 'Systeem voor wachtwoordbeheer' niet van toepassing.

## 5.18 Toegangsrechten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer	#Bescherming

### Beheersmaatregel

Toegangsrechten met betrekking tot informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.

### Doel

Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.

### Richtlijn

#### Verlenen en intrekken van toegangsrechten

De procedure voor het toewijzen of intrekken van fysieke en logische toegangsrechten aan de geauthenticeerde identiteit van een entiteit behoort te omvatten:

- autorisatie van de eigenaar van de informatie en andere gerelateerde bedrijfsmiddelen verkrijgen voor het gebruik van de informatie en andere gerelateerde bedrijfsmiddelen (zie 5.9). De verlening van aparte goedkeuring voor toegangsrechten door het management kan ook passend zijn;
- de bedrijfseisen en het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie in overweging nemen;
- overwegen functies te scheiden, waaronder het scheiden van de rollen van goedkeuring en implementatie van de toegangsrechten en het scheiden van conflicterende rollen;
- bewerkstelligen dat toegangsrechten worden ingetrokken wanneer iemand geen toegang meer nodig heeft tot de informatie en andere gerelateerde bedrijfsmiddelen, en met name bewerkstelligen dat toegangsrechten van gebruikers die de organisatie hebben verlaten, tijdig worden ingetrokken;
- overwegen tijdelijke toegangsrechten voor beperkte duur te verlenen en deze op de aflooptdatum in te trekken, met name voor tijdelijk personeel of indien slechts tijdelijk toegang vereist is voor het personeel;
- verifiëren dat het toegekende toegangsniveau in overeenstemming is met de onderwerpspecifieke beleidsregels inzake toegangsbeveiliging (zie 5.15) en aansluit op andere informatiebeveiligingseisen zoals functiescheiding (zie 5.3);
- waarborgen dat toegangsrechten pas worden geactiveerd (bijv. door dienstverleners) nadat de autorisatieprocedures succesvol zijn afgerond;
- een centraal overzicht bijhouden van toegangsrechten die aan een (logische of fysieke) gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatie en andere gerelateerde bedrijfsmiddelen;

- i) de toegangsrechten aanpassen van gebruikers die van rol of functie zijn veranderd;
- j) fysieke en logische toegangsrechten verwijderen of aanpassen, hetgeen kan worden gedaan door sleutels, authenticatie-informatie, ID-kaarten of abonnementen te verwijderen, in te trekken, te herroepen of te vervangen;
- k) een registratie bijhouden van wijzigingen in de logische en fysieke toegangsrechten van gebruikers.

#### Beoordeling van toegangsrechten

Bij het regelmatig beoordelen van fysieke en logische toegangsrechten behoren de volgende aspecten in overweging te worden genomen:

- a) de toegangsrechten van gebruikers na een verandering binnen dezelfde organisatie (bijv. verandering van functie, promotie, demotie) of beëindiging van het dienstverband (zie 6.1 t/m 6.5);
- b) autorisaties voor speciale toegangsrechten.

#### Overweging voorafgaand aan een wijziging of beëindiging van het dienstverband

De toegangsrechten van een gebruiker tot informatie en gerelateerde bedrijfsmiddelen behoren te worden beoordeeld en aangepast of ingetrokken voorafgaand aan een wijziging aan of beëindiging van het dienstverband, op basis van de evaluatie van risicofactoren zoals:

- a) of de beëindiging of wijziging is geïnitieerd door de gebruiker of door het management en de reden voor de beëindiging;
- b) de actuele verantwoordelijkheden van de gebruiker;
- c) de waarde van de bedrijfsmiddelen die op dat moment toegankelijk zijn.

#### **Overige informatie**

Er behoort op te worden gelet dat gebruikerstoegangsrollen worden vastgesteld op basis van bedrijfseisen die een aantal toegangsrechten samenvatten in specifieke gebruikerstoegangsprofielen. Toegangsverzoeken en beoordelingen van toegangsrechten zijn gemakkelijker te beheren op het niveau van dergelijke rollen dan op het niveau van bijzondere rechten.

Er behoort op te worden gelet dat in personeels- en dienstencontracten bepalingen worden opgenomen die sancties noemen voor personeel dat onbevoegde toegang probeert te verkrijgen (zie 5.20, 6.2, 6.4, 6.6).

Ingeval het management de beëindiging van het dienstverband heeft geïnitieerd, bestaat het risico dat ontevreden personeel of externe gebruikers opzettelijk informatie corrumperen of informatieverwerkende faciliteiten saboteren. Personen die ontslag nemen of worden ontslagen, kunnen in de verleiding komen informatie te verzamelen voor toekomstig gebruik.

Klonen is een doelmatige manier waarop organisaties toegang aan gebruikers kunnen toewijzen. Dit behoort echter met zorg te gebeuren, op basis van door de organisatie vastgestelde onderscheiden rollen, in plaats van een identiteit met alle gerelateerde toegangsrechten zomaar te klonen. Aan het klonen is het inherente risico verbonden dat het leidt tot buitensporige toegangsrechten tot informatie en andere gerelateerde bedrijfsmiddelen.

## 5.19 Informatiebeveiliging in leveranciersrelaties

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_ leveranciersrelaties	#Governance_en_ Ecosysteem #Bescherming

### Beheersmaatregel

Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheren.

### Doel

Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.

### Richtlijn

De organisatie behoort een onderwerpspecifiek beleid inzake leveranciersrelaties vast te stellen en aan alle relevante belanghebbenden mee te delen.

De organisatie behoort processen en procedures te identificeren en te implementeren om de beveiligingsrisico's in verband met het gebruik van door leveranciers geleverde producten en diensten op te pakken. Dit behoort ook van toepassing te zijn op het gebruik door de organisatie van middelen van aanbieders van clouddiensten. Deze processen en procedures behoren de door de organisatie te implementeren processen en procedures te omvatten, alsmede de processen en procedures waarvan de organisatie vereist dat de leverancier ze implementeert om te starten met het gebruik van de producten of diensten van een leverancier of voor de beëindiging van het gebruik van de producten en diensten van een leverancier, zoals:

- het vaststellen en documenteren van de soorten leveranciers, bijv. ICT-diensten, logistieke voorzieningen, financiële diensten, ICT-infrastructuurcomponenten die gevolgen kunnen hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie van de organisatie;
- het vaststellen hoe leveranciers worden geëvalueerd en geselecteerd op basis van de gevoeligheid van informatie, producten en diensten (bijv. met marktanalyse, referenties van klanten, beoordeling van documenten, beoordelingen op locatie, certificeringen);
- het evalueren en selecteren van producten of diensten van een leverancier met toereikende beheersmaatregelen voor informatiebeveiliging en deze beoordelen; met name de juistheid en volledigheid van de door de leverancier geïmplementeerde beheersmaatregelen die de integriteit van de informatie van, en de informatieverwerking door, de leverancier en daarmee de informatiebeveiliging van de organisatie garanderen;
- het definiëren van de informatie, ICT-diensten en fysieke infrastructuur van de organisatie waartoe leveranciers toegang hebben en die ze kunnen monitoren, beheersen of gebruiken;
- het definiëren van de door leveranciers geleverde soorten ICT-infrastructuurcomponenten en -diensten die van invloed kunnen zijn op de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie van de organisatie;

- f) het beoordelen en beheren van de informatiebeveiligingsrisico's in verband met:
- 1) het gebruik door leveranciers van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, met inbegrip van risico's die uitgaan van mogelijk kwaadwillig personeel van de leverancier;
  - 2) storingen of kwetsbaarheden van de door de leveranciers geleverde producten (met inbegrip van softwarecomponenten en subcomponenten die in deze producten worden gebruikt) of diensten;
- g) het monitoren van het voldoen aan vastgestelde informatiebeveiligingseisen voor elke soort leverancier en elke soort toegang, met inbegrip van beoordeling van derden en productvalidatie;
- h) het beperken van het niet voldoen door een leverancier ongeacht of dit is opgemerkt door monitoring of door andere middelen;
- i) het omgaan met incidenten en noodsituaties die verband houden met producten en diensten van leveranciers, met inbegrip van verantwoordelijkheden van zowel de organisatie als van de leveranciers;
- j) veerkracht- en, indien nodig, herstel- en calamiteitenmaatregelen om de beschikbaarheid te bewerkstelligen van de informatie van, en de informatieverwerking door, de leverancier en als gevolg daarvan de beschikbaarheid van de informatie van de organisatie;
- k) bewustwording en training voor het personeel van de organisatie dat contacten onderhoudt met personeel van de leverancier betreffende passende regels van betrokkenheid, onderwerpspecifieke beleidsregels, processen en procedures en gedrag, gebaseerd op het type leverancier en het soort toegang dat de leverancier heeft tot systemen en informatie van de organisatie;
- l) het beheren van het nodige transport van informatie, gerelateerde bedrijfsmiddelen en al het andere dat moet worden veranderd, en waarborgen dat informatiebeveiliging tijdens de gehele transportperiode wordt gehandhaafd;
- m) eisen om veilige beëindiging van de leveranciersrelatie te bewerkstelligen, met inbegrip van:
- 1) het intrekken van toegangsrechten;
  - 2) het omgaan met informatie;
  - 3) het vaststellen van de eigendom van intellectuele eigendom die tijdens de verbintenis is ontwikkeld;
  - 4) de overdraagbaarheid van informatie in geval van verandering van leverancier of 'insourcing';
  - 6) beheer van registraties;\*)
  - 7) het retourneren van bedrijfsmiddelen;
  - 8) beveiligde verwijdering van informatie en andere gerelateerde bedrijfsmiddelen;
  - 9) voortdurende geheimhoudingseisen;
- n) het niveau van beveiliging van personeel en fysieke beveiliging dat wordt verwacht van personeel en faciliteiten van de leverancier.

---

\*) Nederlandse voetnoot: Nummering als in de brontekst.

Er behoort te worden nagedacht over de procedures voor het voortzetten van de verwerking van informatie indien de leverancier zijn producten of diensten niet meer kan leveren (bijv. als gevolg van een incident, omdat de leverancier zijn bedrijf heeft gestaakt, of bepaalde onderdelen niet meer levert als gevolg van technologische ontwikkelingen) om vertraging bij het regelen van vervangende producten of diensten te voorkomen (bijv. door van tevoren een alternatieve leverancier aan te wijzen of altijd gebruik te maken van alternatieve leveranciers).

### Overige informatie

In gevallen waarin het voor een organisatie niet mogelijk is eisen te stellen aan een leverancier, behoort de organisatie:

- a) de in deze beheersmaatregel gegeven richtlijnen in aanmerking te nemen bij het nemen van beslissingen over de keuze van een leverancier en zijn product of dienst;
- b) op basis van een risicobeoordeling benodigde compenserende beheersmaatregelen te implementeren.

Informatie kan in gevaar worden gebracht door leveranciers met een ontoereikend informatiebeveiligingsbeheer. Om de toegang tot informatie en andere gerelateerde bedrijfsmiddelen door de leverancier te beheren, behoren beheersmaatregelen te worden vastgesteld en toegepast. Indien er bijvoorbeeld een speciale noodzaak is om de informatie vertrouwelijk te houden, kunnen geheimhoudingsovereenkomsten of cryptografische technieken worden gebruikt. Een ander voorbeeld vormen risico's voor de bescherming van persoonlijke gegevens als de leveranciersovereenkomst betrekking heeft op de overdracht van, of toegang tot informatie over de grens. De organisatie behoort zich ervan bewust te zijn dat de wettelijke of contractuele verantwoordelijkheid voor het beschermen van de informatie bij de organisatie ligt.

Risico's kunnen ook worden veroorzaakt door ontoereikende beheersmaatregelen van door leveranciers geleverde ICT-infrastructuurcomponenten of -diensten. Componenten of diensten met storingen of kwetsbaarheden kunnen inbreuken op de informatiebeveiliging in de organisatie of voor een andere entiteit veroorzaken. Ze kunnen bijvoorbeeld besmetting met malware, aanvallen of andere schade aan andere entiteiten dan de organisatie veroorzaken.

Zie ISO/IEC 27036-2 voor nadere details.

## 5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_ leveranciersrelaties	#Governance_en_ Ecosysteem #Bescherming

### Beheersmaatregel

Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.

### Doel

Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.

**Richtlijn**

Leveranciersovereenkomsten behoren te worden vastgesteld en gedocumenteerd om te waarborgen dat er tussen de organisatie en de leverancier duidelijkheid bestaat ten aanzien van de verplichtingen van beide partijen om te voldoen aan relevante informatiebeveiligingseisen.

Om aan de vastgestelde informatiebeveiligingseisen te voldoen kan worden overwogen de volgende voorwaarden in de overeenkomsten op te nemen:

- a) omschrijving van de te verstrekken of te benaderen informatie en methoden om de informatie te verschaffen of toegankelijk te maken;
- b) classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie (zie 5.10, 5.12, 5.13);
- c) mapping tussen het eigen classificatieschema van de organisatie en het classificatieschema van de leverancier;
- d) eisen van wet- en regelgeving, statutaire en contractuele eisen, met inbegrip van gegevensbescherming, het omgaan met persoonsgegevens, rechten van intellectuele eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat eraan wordt voldaan;
- e) de verplichting van elke contractpartij om overeengekomen beheersmaatregelen te implementeren, met inbegrip van toegangsbeveiliging, prestatiebeoordeling, monitoren, melden, rapportage en auditen en de verplichtingen van de leverancier om te voldoen aan de informatiebeveiligingseisen van de organisatie;
- f) de regels van aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van onaanvaardbaar gebruik indien noodzakelijk;
- g) procedures of voorwaarden voor autorisatie en voor het intrekken van de autorisatie voor het gebruik van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie door personeel van de leverancier (bijv. aan de hand van een specifieke lijst van personeel van leveranciers dat bevoegd is om de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie te gebruiken);
- h) informatiebeveiligingseisen met betrekking tot de ICT-infrastructuur van de leverancier; met name minimale informatiebeveiligingseisen voor elk type informatie en elk type toegang, te gebruiken als basis voor individuele overeenkomsten met leveranciers op basis van de bedrijfsbehoeften en risicocriteria van de organisatie;
- i) schadeloosstellingen en herstel indien de contractant niet aan de eisen voldoet;
- j) eisen voor incidentbeheer en -procedures (in het bijzonder notificatie en samenwerking tijdens herstel van het incident);
- k) trainings- en bewustwordingseisen voor specifieke procedures en informatiebeveiligingseisen (bijv. voor incidentresponsprocedures, autorisatieprocedures);
- l) relevante voorzieningen voor uitbesteding, met inbegrip van de te implementeren beheersmaatregelen, zoals een overeenkomst over de inzet van onderleveranciers (bijv. eisen dat voor hen dezelfde verplichtingen gelden als voor de leverancier, eisen dat er een lijst van onderleveranciers wordt verstrekt en kennisgeving telkens voordat er iets verandert);

- m) relevante contacten, met inbegrip van een contactpersoon voor aangelegenheden betreffende informatiebeveiliging;
- n) screeningeisen, indien wettelijk toegestaan, voor het personeel van leveranciers, met inbegrip van verantwoordelijkheden voor het uitvoeren van de screening en kennisgevingsprocedures indien de screening niet is voltooid of de resultaten aanleiding geven tot twijfel of bezorgdheid;
- o) de bewijs- en borgingsmechanismen van attesten van derden voor relevante informatiebeveiligingseisen met betrekking tot de processen van leveranciers en een onafhankelijk rapport over de doeltreffendheid van beheersmaatregelen;
- p) het recht om de processen en beheersmaatregelen van de leverancier in verband met de overeenkomst te auditen;
- q) verplichting van de leverancier om periodiek een rapport te verstrekken over de doeltreffendheid van beheersmaatregelen, en overeenkomst over tijdige correctie van relevante kwesties die in het rapport aan de orde worden gesteld;
- r) procedures voor het oplossen van defecten en conflicten;
- s) voorzien in back-up die is afgestemd op de behoeften van de organisatie (wat betreft frequentie en type en opslaglocatie);
- t) het bewerkstelligen van de beschikbaarheid van een alternatieve faciliteit (d.w.z. noodherstellocatie) waarvoor niet dezelfde dreigingen gelden als voor de primaire faciliteit en overwegingen met betrekking tot alternatieve beheersmaatregelen waarop wordt teruggevallen indien de primaire beheersmaatregelen falen;
- u) de beschikking over een proces voor wijzigingsbeheer dat bewerkstelligt dat de organisatie vooraf op de hoogte wordt gebracht en de mogelijkheid heeft om wijzigingen niet te aanvaarden;
- v) fysieke beveiligingsbeheersmaatregelen die passen bij de classificatie van de informatie;
- w) beheersmaatregelen voor overdragen van informatie om de informatie te beschermen tijdens fysiek transport of tijdens logische overdracht;
- x) beëindigingsclausules bij het afsluiten van de overeenkomst, met inbegrip van beheer van registraties, het retourneren van bedrijfsmiddelen, beveiligde verwijdering van informatie en andere gerelateerde bedrijfsmiddelen en eventuele doorlopende geheimhoudingsverplichtingen;
- y) het voorzien in een methode om de door de leverancier opgeslagen informatie van de organisatie op beveiligde wijze te vernietigen zodra die informatie niet meer nodig is;
- z) het bewerkstelligen van ondersteuning bij de overdracht aan een andere leverancier of aan de organisatie zelf bij het einde van de overeenkomst.

De organisatie behoort een register van afspraken met externe partijen (bijv. contracten, een memorandum van overeenstemming, overeenkomsten voor het delen van informatie) op te stellen en te onderhouden om bij te houden waar haar informatie naartoe gaat. De organisatie behoort ook haar overeenkomsten met externe partijen regelmatig te beoordelen, te valideren en bij te werken om te garanderen dat ze nog steeds vereist zijn en geschikt zijn voor het doel en dat ze relevante clausules over informatiebeveiliging bevatten.

## Overige informatie

De overeenkomsten kunnen voor de verschillende organisaties en de verschillende soorten leveranciers aanzienlijk variëren. Derhalve behoort erop te worden toegezien dat alle relevante eisen voor het oppakken van informatiebeveiligingsrisico's erin worden opgenomen.

Voor gegevens over overeenkomsten met leveranciers, zie de ISO/IEC 27036-reeks. Voor gegevens over overeenkomsten voor clouddiensten, zie de ISO/IEC 19086-reeks.

## 5.21 Beheren van informatiebeveiliging in de ICT-keten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_ leveranciersrelaties	#Governance_en_ Ecosysteem #Bescherming

### Beheersmaatregel

Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren.

### Doel

Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.

### Richtlijn

In aanvulling op de algemene informatiebeveiligingseisen voor leveranciersrelaties behoren de volgende informatiebeveiligingsonderwerpen in aanmerking te worden genomen binnen de beveiliging van de ITC-toeleveringsketen:

- a) informatiebeveiligingseisen definiëren die van toepassing zijn op het verwerven van ICT-producten of -diensten;
- b) eisen dat leveranciers de beveiligingseisen van de organisatie in de gehele toeleveringsketen bekendmaken indien zij delen van de ICT-dienst die zij aan de organisatie leveren, uitbesteden;
- c) eisen dat de leveranciers van ICT-producten passende beveiligingspraktijken in de gehele toeleveringsketen bekendmaken indien deze producten componenten bevatten die worden ingekocht bij of verkregen van andere leveranciers of andere entiteiten (bijv. softwareontwikkelaars en leveranciers van hardwarecomponenten die op basis van onderaanneming werken);
- d) verzoeken dat de leveranciers van ICT-producten informatie verstrekken waarin de in producten gebruikte softwarecomponenten worden beschreven;
- e) verzoeken dat de leveranciers van ICT-producten informatie verstrekken waarin de geïmplementeerde beveiligingsfuncties van hun product en de voor het veilige gebruik ervan vereiste configuratie worden beschreven;
- f) een monitoringproces en aanvaardbare methoden voor het valideren dat de geleverde ICT-producten en -diensten voldoen aan de gestelde beveiligingseisen, implementeren. Voorbeelden

van zulke methoden voor het beoordelen van leveranciers zijn penetratietests en bewijs of validatie van attesten van derden voor de informatiebeveiligingsactiviteiten van de leverancier;

- g) een proces implementeren voor het vaststellen en documenteren van componenten van producten of diensten die essentieel zijn voor het handhaven van de functionaliteit en daarom verhoogde aandacht, toezicht en verdere opvolging vereisen als deze buiten de organisatie worden gebouwd, in het bijzonder indien de leverancier delen van componenten van producten of diensten aan andere leveranciers uitbestedt;
- h) zekerheid verkrijgen dat essentiële componenten en de herkomst ervan in de toeleveringsketen kunnen worden getraceerd;
- i) zekerheid verkrijgen dat de geleverde ICT-producten functioneren zoals voorzien zonder onverwachte of ongewenste verschijnselen;
- j) processen implementeren om te garanderen dat componenten van leveranciers echt zijn en ongewijzigd zijn ten opzichte van de specificaties. Voorbeeldmaatregelen zijn labels tegen manipulatie, cryptografische hashverificaties of digitale handtekeningen. Monitoren op prestaties die niet aan de specificaties voldoen, kan een manier zijn om manipulatie of namaak aan te tonen. Er behoort preventie en detectie van manipulatie te worden geïmplementeerd tijdens verschillende fasen van de levenscyclus van systeemontwikkeling, met inbegrip van de ontwerp-, ontwikkel-, integratie-, operationele en onderhoudsfasen;
- k) waarborgen dat ICT-producten de vereiste beveiligingsniveaus halen, bijv. door middel van een formele certificerings- of beoordelingsregeling, zoals de Common Criteria Recognition Arrangement;
- l) regels definiëren voor het delen van informatie met betrekking tot de toeleveringsketen en potentiële kwesties en compromissen tussen de organisatie en leveranciers;
- m) specifieke processen implementeren voor het beheren van de levenscyclus en beschikbaarheid van ICT-componenten en gerelateerde beveiligingsrisico's. Dit omvat het beheren van de risico's dat onderdelen niet langer beschikbaar zijn omdat leveranciers hun bedrijf hebben gestaakt of deze onderdelen als gevolg van technologische ontwikkelingen niet meer aanbieden. Het identificeren van een alternatieve leverancier en het proces om software en competentie naar de alternatieve leverancier over te brengen behoren te worden overwogen.

### **Overige informatie**

De specifieke risicobeheerpraktijken betreffende de ICT-toeleveringsketen komen boven op de algemene praktijken van informatiebeveiliging, kwaliteit, projectmanagement en systeemengineering, maar vervangen deze niet.

Organisaties wordt geadviseerd om samen te werken met leveranciers voor een goed begrip van de ICT-toeleveringsketen en de aangelegenheden die een belangrijke uitwerking hebben op de producten en diensten die worden geleverd. De organisatie kan informatiebeveiligingspraktijken van de ICT-toeleveringsketen beïnvloeden door in overeenkomsten met leveranciers de aangelegenheden bekend te maken waaraan door andere leveranciers in de ICT-toeleveringsketen invulling behoort te worden gegeven.

ICT behoort te worden verkregen van bronnen met een goede reputatie. De betrouwbaarheid van software en hardware is een kwestie van kwaliteitscontrole. Hoewel het voor een organisatie over het algemeen niet mogelijk is om de kwaliteitscontrolesystemen van haar leveranciers te inspecteren, kan zij wel een betrouwbaar oordeel vellen op basis van de reputatie van de leverancier.

De ICT-toeleveringsketen zoals hier bedoeld omvat ook clouddiensten.

Voorbeelden van ICT-toeleveringsketens zijn:

- a) 'cloud services provisioning', waar de aanbieder van de clouddienst afhankelijk is van de softwareontwikkelaars, aanbieders van telecommunicatiediensten, hardware-aanbieders;
- b) internet of things (IoT), waarbij de dienst ook de fabrikanten van apparatuur, de aanbieders van de clouddienst (bijv. de exploitanten van het IoT-platform), de ontwikkelaars voor mobiele en internettoepassingen en de leverancier van softwarebibliotheken betreft;
- c) hostingdiensten, waar de aanbieder op externe servicebalies vertrouwt, met inbegrip van eerste, tweede en derde niveaus van ondersteuning.

Zie ISO/IEC 27036-3 voor nadere details met inbegrip van richtlijnen voor risicobeoordeling.

Software-identificatietags (SWID) kunnen ook bijdragen aan betere informatiebeveiliging in de toeleveringsketen, door informatie te geven over de herkomst van software. Zie ISO/IEC 19770-2 voor nadere details.

## 5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_ leveranciersrelaties #Borging_van_infor- matiebeveiliging	#Governance_en_ Ecosysteem #Bescherming #Verdediging

### Beheersmaatregel

De organisatie behoort de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.

### Doel

Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

### Richtlijn

Het monitoren en beoordelen van, en het beheren van veranderingen aan, leveranciersdiensten behoort te bewerkstelligen dat aan de informatiebeveiligingsvoorwaarden van de overeenkomsten wordt voldaan, informatiebeveiligingsincidenten en -problemen naar behoren worden beheerd en veranderingen in leveranciersdiensten of de bedrijfsstatus niet van invloed zijn op de dienstverlening.

Hiertoe behoort een proces voor het beheer van de relatie tussen de organisatie en de leverancier te bestaan om:

- a) de prestatieniveaus van de dienstverlening te monitoren om de naleving van de overeenkomsten te verifiëren;
- b) door leveranciers aangebrachte veranderingen te monitoren, waaronder:
  - 1) verbeteringen van de huidige aangeboden dienstverlening;
  - 2) ontwikkelingen van nieuwe toepassingen en systemen;
  - 3) wijzigingen in of updates van beleid en procedures van de leverancier;
  - 4) nieuwe of gewijzigde beheersmaatregelen om informatiebeveiligingsincidenten op te lossen en om de informatiebeveiliging te verbeteren;
- c) veranderingen in leveranciersdiensten te monitoren, waaronder:
  - 1) veranderingen en verbeteringen van netwerken;
  - 2) gebruik van nieuwe technologieën;
  - 3) aanvaarding van nieuwe producten of nieuwere versies of uitgaven;
  - 4) nieuwe ontwikkelinstrumenten en omgevingen;
  - 5) veranderingen in fysieke locatie van dienstverleningsfaciliteiten;
  - 6) verandering van onderleveranciers;
  - 7) uitbesteding aan een andere leverancier;
- d) de rapporten over de dienstverlening die zijn opgesteld door de leverancier, te beoordelen en regelmatig voortgangsbesprekingen te regelen voor zover door de overeenkomsten vereist;
- e) audits van leveranciers en onderleveranciers uit te voeren, in samenhang met de beoordeling van rapporten van onafhankelijke auditoren, indien beschikbaar, en vastgestelde kwesties op te volgen;
- f) informatie te verstrekken over informatiebeveiligingsincidenten en deze informatie te beoordelen voor zover vereist door de overeenkomsten en ondersteunende richtlijnen en procedures;
- g) audittrajecten van leveranciers en registraties van informatiebeveiligingsgebeurtenissen, operationele problemen, weigeringen, opsporing van storingen en onderbrekingen in verband met de geleverde dienst te beoordelen;
- h) te reageren op geïdentificeerde informatiebeveiligingsgebeurtenissen of -incidenten en deze te beheren;
- i) kwetsbaarheden in de informatiebeveiliging te identificeren en beheren;
- j) informatiebeveiligingsaspecten van de relaties van de leverancier met zijn eigen leveranciers te beoordelen;
- k) te bewerkstelligen dat de leverancier voldoende capaciteit voor de diensten onderhoudt samen met werkbare plannen die zijn ontworpen om te waarborgen dat de overeengekomen continuïteitsniveaus van de dienstverlening na grote storingen of calamiteiten in de dienstverlening worden onderhouden (zie 5.29, 5.30, 5.35, 5.36, 8.14);

- l) ervoor te zorgen dat leveranciers verantwoordelijkheden toewijzen voor het beoordelen van naleving en voor het dwingend uitvoeren van de eisen van de overeenkomsten;
- m) regelmatig te evalueren of de leveranciers afdoende informatiebeveiligingsniveaus in stand houden.

De verantwoordelijkheid voor het beheer van leveranciersrelaties behoort te worden toegekend aan een daarvoor aangewezen persoon of team. Om te monitoren dat de eisen van de overeenkomst, in het bijzonder de informatiebeveiligingseisen, worden nagekomen, behoren voldoende technische vaardigheden en middelen beschikbaar te worden gesteld. Als tekortkomingen in de dienstverlening worden waargenomen behoren passende maatregelen te worden getroffen.

### Overige informatie

Zie ISO/IEC 27036-3 voor nadere details.

## 5.23 Informatiebeveiliging voor het gebruik van clouddiensten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beveiliging_in_l leveranciersrelaties	#Governance_en_ ecosysteem #Bescherming

### Beheersmaatregel

Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.

### Doel

Informatiebeveiliging voor het gebruik van clouddiensten specificeren en beheren.

### Richtlijn

De organisatie behoort een onderwerpspecifiek beleid inzake het gebruik van clouddiensten vast te stellen en aan alle relevante belanghebbenden mee te delen.

De organisatie behoort te definiëren en te communiceren hoe zij voornemens is informatiebeveiligingsrisico's in verband met het gebruik van clouddiensten te beheren. Dit kan een uitbreiding zijn of deel uitmaken van de bestaande aanpak voor de manier waarop een organisatie door externe partijen geleverde diensten beheert (zie 5.21 en 5.22).

Het gebruik van clouddiensten kan gepaard gaan met een gedeelde verantwoordelijkheid voor informatiebeveiliging en samenwerking tussen de aanbieder van de clouddienst en de organisatie die als afnemer van de clouddienst optreedt. Het is essentieel dat de verantwoordelijkheden voor zowel de aanbieder als de organisatie, handelend als afnemer van de clouddienst, op de juiste wijze worden gedefinieerd en geïmplementeerd.

De organisatie behoort het volgende te definiëren:

- alle relevante informatiebeveiligingseisen in verband met het gebruik van de clouddiensten;
- selectiecriteria voor clouddiensten en de reikwijdte van het gebruik van clouddiensten;

- c) rollen en verantwoordelijkheden met betrekking tot het gebruik en beheer van clouddiensten;
- d) welke beheersmaatregelen voor informatiebeveiliging door de aanbieder van de clouddienst en welke door de organisatie als afnemer van de clouddienst worden beheerd;
- e) hoe door de aanbieder van de clouddienst verstrekte informatiebeveiligingscapaciteiten kunnen worden verkregen en gebruikt;
- f) hoe zekerheid kan worden verkregen over de door aanbieders van clouddiensten geïmplementeerde beheersmaatregelen voor informatiebeveiliging;
- g) hoe beheersmaatregelen, interfaces en wijzigingen aan diensten behoren te worden beheerd wanneer een organisatie gebruikmaakt van meerdere clouddiensten, met name van verschillende aanbieders van clouddiensten;
- h) procedures voor het omgaan met informatiebeveiligingsincidenten die zich voordoen met betrekking tot het gebruik van clouddiensten;
- i) haar aanpak voor het monitoren, beoordelen en evalueren van het doorlopend gebruik van clouddiensten om informatiebeveiligingsrisico's te beheren;
- j) hoe het gebruik van clouddiensten met inbegrip van exitstrategieën voor clouddiensten kan worden gewijzigd of beëindigd.

Overeenkomsten voor clouddiensten zijn vaak vooraf gedefinieerd zonder dat het mogelijk is erover te onderhandelen. Voor alle clouddiensten behoort de organisatie overeenkomsten voor clouddiensten met de aanbieder(s) van clouddiensten te beoordelen. Een overeenkomst voor clouddiensten behoort in te gaan op de eisen van de organisatie ten aanzien van vertrouwelijkheid, integriteit, beschikbaarheid en het omgaan met persoonsgegevens, met passende doelstellingen voor het niveau van dienstverlening van de clouddienst en kwalitatieve doelstellingen voor de clouddienst. De organisatie behoort ook relevante risicobeoordelingen uit te voeren om de risico's in verband met het gebruik van de clouddienst te identificeren. Eventuele overblijvende risico's in verband met het gebruik van de clouddienst behoren duidelijk te worden geïdentificeerd en aanvaard door het passende management van de organisatie.

Een overeenkomst tussen de aanbieder van een clouddienst en de organisatie, in haar rol van afnemer van de clouddienst, behoort de volgende bepalingen te bevatten voor de bescherming van de gegevens van de organisatie en de beschikbaarheid van diensten:

- a) het leveren van oplossingen op basis van door de industrie aanvaarde normen voor architectuur en infrastructuur;
- b) het beheren van toegangsbeveiligingsmaatregelen van de clouddienst conform de eisen van de organisatie;
- c) het implementeren van oplossingen voor het monitoren van en beschermen tegen malware;
- d) het verwerken en op goedgekeurde locaties (bijv. een bepaald land of bepaalde regio) of binnen een bepaald rechtsgebied of krachtens een bepaalde rechtsbevoegdheid opslaan van gevoelige informatie van de organisatie;
- e) het bieden van gerichte steun indien er zich een informatiebeveiligingsincident voordoet in de cloudomgeving;

- f) het bewerkstelligen dat aan de informatiebeveiligingseisen van de organisatie wordt voldaan indien clouddiensten verder worden uitbesteed aan een externe leverancier (of verbieden dat clouddiensten worden uitbesteed);
- g) het ondersteunen van de organisatie bij het verzamelen van digitaal bewijsmateriaal, met inachtneming van wet- en regelgeving inzake digitaal bewijsmateriaal in verschillende rechtsgebieden;
- h) het voorzien in passende ondersteuning en beschikbaarheid van diensten gedurende een passend tijdsbestek wanneer de organisatie niet langer gebruik wil maken van de clouddienst;
- i) het voorzien in de vereiste back-ups van gegevens en configuratie-informatie en het veilig beheren van back-ups voor zover van toepassing, op basis van de capaciteiten van de leverancier van de clouddienst die wordt ingezet door de organisatie in haar rol als afnemer van de clouddienst;
- j) het verstrekken en retourneren van informatie zoals configuratiebestanden, broncode en gegevens die eigendom zijn van de organisatie in haar rol van afnemer van de clouddienst op verzoek of bij beëindiging van de dienst.

In haar rol van afnemer van de clouddienst behoort de organisatie te overwegen of de overeenkomst behoort te vereisen dat de aanbieders van clouddiensten vooraf kennis geven van wezenlijke wijzigingen aan hoe de dienst aan de organisatie wordt geleverd die gevolgen hebben voor de afnemer, waaronder:

- a) wijzigingen aan de technische infrastructuur (bijv. verhuizing, herconfiguratie of wijzigingen in hardware of software) die van invloed zijn op, of tot veranderingen leiden in, de aangeboden clouddienst;
- b) het verwerken of opslaan van informatie in een nieuw geografisch of juridisch rechtsgebied;
- c) het gebruik van collega-aanbieders van clouddiensten of andere onderaannemers (met inbegrip van het wijzigen van bestaande of het gebruik van nieuwe partijen).

De organisatie die clouddiensten gebruikt, behoort nauw contact te onderhouden met haar aanbieders van de clouddiensten. Deze contacten maken wederzijdse uitwisseling mogelijk van informatie over informatiebeveiliging voor het gebruik van de clouddiensten, met inbegrip van een mechanisme voor zowel de aanbieder als de organisatie, in haar rol van afnemer van de clouddiensten, om elk kenmerk van de diensten te monitoren en tekortkomingen ten opzichte van de in de overeenkomsten opgenomen verbintenissen te melden.

### **Overige informatie**

Deze beheersmaatregel bekijkt cloudbeveiliging vanuit het oogpunt van de afnemer van de clouddienst(en).

Aanvullende informatie met betrekking tot clouddiensten is te vinden in ISO/IEC 17788, ISO/IEC 17789 en ISO/IEC 22123-1. Specifieke informatie met betrekking tot clouds en overdraagbaarheid bij exitstrategieën is te vinden in ISO/IEC 19941. Specifieke informatie met betrekking tot informatiebeveiliging en publieke clouddiensten wordt beschreven in ISO/IEC 27017. Specifieke informatie met betrekking tot de bescherming van persoonsgegevens in publieke clouds die als verwerker van persoonsgegevens fungeren, wordt beschreven in ISO/IEC 27018. Leveranciersrelaties voor clouddiensten worden behandeld in ISO/IEC 27036-4 en clouddienstovereenkomsten en de inhoud ervan worden behandeld in de ISO/IEC 19086-reeks, waarbij ISO/IEC 19086-4 specifiek ingaat op beveiliging en privacy.

## 5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_infor- matiebeveiligings- gebeurtenissen	#Verdediging

### Beheersmaatregel

De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.

### Doel

Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.

### Richtlijn

#### Rollen en verantwoordelijkheden

De organisatie behoort passende processen voor het beheer van informatiebeveiligingsincidenten op te stellen. Rollen en verantwoordelijkheden voor het uitvoeren van de procedures voor incidentenbeheer behoren te worden vastgesteld en op doeltreffende wijze te worden gecommuniceerd aan de relevante interne en externe belanghebbenden.

Het volgende behoort te worden overwogen:

- a) een gemeenschappelijke methode opstellen voor het melden van informatiebeveiligingsgebeurtenissen met inbegrip van een contactpunt (zie 6.8);
- b) een proces opstellen voor het beheer van incidenten om de organisatie de capaciteit te bieden voor het beheren van informatiebeveiligingsincidenten, met inbegrip van beheer, documentatie, detectie, triage, prioritering, analyse, communicatie en het coördineren van belanghebbenden;
- c) een proces opstellen voor het reageren op incidenten waardoor de organisatie het vermogen krijgt informatiebeveiligingsincidenten te beoordelen, erop te reageren en er lering uit te trekken;
- d) alleen competent personeel toestaan de kwesties te behandelen die verband houden met informatiebeveiligingsincidenten binnen de organisatie. Dit personeel behoort te worden voorzien van documentatie over de procedures en periodieke training;
- e) een proces opstellen voor het identificeren van vereiste training, certificering en voortdurende professionele ontwikkeling van personeel dat de taak heeft op incidenten te reageren.

#### Procedures voor incidentenbeheer

De doelstellingen voor het beheer van informatiebeveiligingsincidenten behoren met het management te worden overeengekomen en er behoort te worden gewaarborgd dat de personen die verantwoordelijk zijn voor het beheer van informatiebeveiligingsincidenten, op de hoogte zijn van de prioriteiten van de organisatie voor het behandelen van informatiebeveiligingsincidenten met inbegrip van een op de mogelijke gevolgen en ernst gebaseerde tijdspanne voor het oplossen ervan. Er

behoren procedures voor incidentenbeheer te worden geïmplementeerd die aan deze doelstellingen en prioriteiten voldoen.

Het management behoort te bewerkstelligen dat er een plan voor het beheer van informatiebeveiligingsincidenten wordt opgesteld waarbij rekening wordt gehouden met verschillende scenario's en dat er procedures worden ontwikkeld en geïmplementeerd voor de volgende activiteiten:

- a) het evalueren van informatiebeveiligingsgebeurtenissen volgens criteria voor wat een informatiebeveiligingsincident uitmaakt;
- b) het monitoren (zie 8.15 en 8.16), detecteren (zie 8.16), classificeren (zie 5.25), analyseren en melden (zie 6.8) van informatiebeveiligingsgebeurtenissen en -incidenten (door mensen of door automatische middelen);
- c) het beheren van informatiebeveiligingsincidenten tot ze volledig zijn afgehandeld, met inbegrip van reactie en escalatie (zie 5.26), volgens het type en de categorie van het incident, mogelijke inschakeling van crisisbeheersing en activering van continuïteitsplannen, gecontroleerd herstel na een incident en communicatie met interne en externe belanghebbenden;
- d) afstemming met interne en externe belanghebbenden zoals overheidsinstanties, externe belangengroepen en fora, leveranciers en klanten (zie 5.5 en 5.6);
- e) het registreren van incidentbeheeractiviteiten;
- f) het behandelen van bewijs (zie 5.28);
- g) analyse van de onderliggende oorzaak of post-mortemprocedures;
- h) identificatie van getrokken lering en eventueel vereiste verbeteringen van de procedures voor incidentenbeheer of de beheersmaatregelen voor informatiebeveiliging in het algemeen.

#### Meldings- en rapportageprocedures

Meldings- en rapportageprocedures behoren de volgende aspecten te omvatten:

- a) de in geval van een informatiebeveiligingsgebeurtenis te treffen maatregelen (bijv. onmiddellijk alle relevante details zoals de optredende storing en berichten op het scherm noteren, onmiddellijk melden bij het contactpunt en alleen gecoördineerde actie ondernemen);
- b) het gebruik van incidentenformulieren om het personeel te ondersteunen bij het verrichten van alle noodzakelijke handelingen bij het melden van informatiebeveiligingsincidenten;
- c) passende feedbackprocedures om te bewerkstelligen dat de personen die informatiebeveiligingsgebeurtenissen melden, voor zover mogelijk over de resultaten worden geïnformeerd nadat de kwestie is opgepakt en afgesloten;
- d) het opstellen van rapportage over incidenten.

Bij het implementeren van procedures voor incidentenbeheer behoren externe eisen ten aanzien van het binnen het gedefinieerde tijdsbestek melden van incidenten aan relevante belanghebbenden (bijv. eisen voor het melden van inbreuken aan de regelgevende instanties) in aanmerking te worden genomen.

### Overige informatie

Informatiebeveiligingsincidenten kunnen de grenzen van organisaties en landen overschrijden. Om op dergelijke incidenten te kunnen reageren is het nuttig om indien van toepassing opvolging te coördineren en informatie over deze incidenten te delen met externe organisaties.

De ISO/IEC 27035-reeks biedt gedetailleerde richtlijnen over het beheer van informatiebeveiligingsincidenten.

## 5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen

Type beheersmaatregel	Informatiebeveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging

### Beheersmaatregel

De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.

### Doel

Doeltreffende categorisering en prioritering van informatiebeveiligingsgebeurtenissen bewerkstelligen.

### Richtlijn

Er behoort een categoriserings- en prioriteringsschema voor informatiebeveiligingsincidenten te worden overeengekomen voor het identificeren van de gevolgen en prioriteit van een incident. Het schema behoort de criteria te omvatten voor het als informatiebeveiligingsincident categoriseren van gebeurtenissen. Het contactpunt behoort elke informatiebeveiligingsgebeurtenis aan de hand van het overeengekomen schema te beoordelen.

Personeel dat verantwoordelijk is voor het coördineren van en reageren op informatiebeveiligingsincidenten behoort de beoordeling uit te voeren en een besluit te nemen over informatiebeveiligingsgebeurtenissen.

Resultaten van de beoordeling en het besluit behoren in detail te worden geregistreerd ten behoeve van toekomstige raadpleging en verificatie.

### Overige informatie

De ISO/IEC 27035-reeks geeft verdere richtlijnen over het beheer van incidenten.

## 5.26 Reageren op informatiebeveiligingsincidenten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Beheer_van_infor- matiebeveiligings- gebeurtenissen	#Verdediging

### Beheersmaatregel

Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.

### Doel

Een doelmatige en doeltreffende reactie op informatiebeveiligingsincidenten bewerkstelligen.

### Richtlijn

De organisatie behoort procedures voor het reageren op informatiebeveiligingsincidenten op te stellen en aan alle relevante belanghebbenden mee te delen.

Een speciaal team met de vereiste competentie (zie 5.24) behoort te reageren op informatiebeveiligingsincidenten.

De reactie behoort de volgende aspecten te omvatten:

- a) de systemen die door het incident worden getroffen inperken als de gevolgen van het incident zich kunnen uitbreiden;
- b) zo snel mogelijk na het incident bewijs verzamelen (zie 5.28);
- c) escalatie, zoals vereist, met inbegrip van crisisbeheersingsactiviteiten en mogelijk door bedrijfscontinuïteitsplannen in te roepen (zie 5.29 en 5.30);
- d) bewerkstelligen dat alle betrokken responsactiviteiten op de juiste manier worden vastgelegd voor latere analyse;
- e) het bestaan van het informatiebeveiligingsincident of relevante details daarvan volgens het 'need-to-know'-principe aan alle relevante in- en externe belanghebbenden communiceren;
- f) met interne en externe partijen, waaronder overheidsinstanties, belangengroepen en fora, leveranciers en klanten, afstemmen om de doeltreffendheid van de reactie te verbeteren en de gevolgen voor andere organisaties tot het minimum te helpen beperken;
- g) het incident formeel afsluiten en registreren zodra het incident met succes is opgepakt;
- h) indien vereist, forensische analyse van de informatiebeveiliging uitvoeren (zie 5.28);

- i) postincidentanalyse uitvoeren om de onderliggende oorzaak te identificeren. Zorg ervoor dat het wordt gedocumenteerd en gecommuniceerd volgens gedefinieerde procedures (zie 5.27);
- j) kwetsbaarheden en zwakke punten in de informatiebeveiliging, onder andere met betrekking tot beheersmaatregelen die het incident hebben veroorzaakt, eraan hebben bijgedragen of het niet hebben voorkomen, identificeren en beheren.

#### Overige informatie

De ISO/IEC 27035-reeks geeft verdere richtlijnen over het beheer van incidenten.

### 5.27 Leren van informatiebeveiligingsincidenten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_informatiebeveiligings-gebeurtenissen	#Verdediging

#### Beheersmaatregel

Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.

#### Doel

De waarschijnlijkheid of de gevolgen van toekomstige incidenten verminderen.

#### Richtlijn

De organisatie behoort procedures op te stellen om de soorten, volumes en kosten van informatiebeveiligingsincidenten te kwantificeren en te monitoren.

De informatie die is verkregen uit de evaluatie van informatiebeveiligingsincidenten behoort te worden gebruikt om:

- a) het plan voor incidentenbeheer, met inbegrip van incidentscenario's en -procedures, te verbeteren (zie 5.24);
- b) terugkerende of ernstige incidenten en de oorzaken ervan te identificeren, teneinde de risicobeoordeling van de informatiebeveiliging van de organisatie te actualiseren, en de nodige aanvullende beheersmaatregelen vast te stellen en te implementeren om de waarschijnlijkheid of de gevolgen van soortgelijke incidenten in de toekomst te verkleinen. Mechanismen om dat mogelijk te maken zijn onder meer het verzamelen, kwantificeren en monitoren van informatie over soorten incidenten, volumes en kosten;
- c) de bewustwording en training van gebruikers (zie 6.3) te verbeteren door voorbeelden te geven van wat er kan gebeuren, hoe te reageren op dergelijke incidenten en hoe ze in de toekomst kunnen worden vermeden.

#### Overige informatie

De ISO/IEC 27035-reeks geeft verdere richtlijnen.

## 5.28 Verzamelen van bewijsmateriaal

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging

### Beheersmaatregel

De organisatie behoort procedures vast te stellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.

### Doel

In het kader van disciplinaire en gerechtelijke stappen consistent en doeltreffend beheer bewerkstelligen van bewijsmateriaal in verband met informatiebeveiligingsincidenten.

### Richtlijn

Bij het in het kader van disciplinaire en gerechtelijke stappen omgaan met bewijs met betrekking tot informatiebeveiligingsgebeurtenissen behoren interne procedures te worden ontwikkeld en gevolgd. De eisen van verschillende rechtsgebieden behoren in aanmerking te worden genomen om de kans zo groot mogelijk te maken dat het bewijs wordt toegelaten in de relevante rechtsgebieden.

In het algemeen behoren deze procedures voor het beheren van bewijs instructies in te houden voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs in overeenstemming met de verschillende soorten opslagmedia, apparaten en de status van de apparaten (d.w.z. in- of uitgeschakeld). Gewoonlijk is het nodig bewijsmateriaal dusdanig te verzamelen dat het voor de bevoegde nationale rechters of een ander disciplinair forum toelaatbaar is. Het behoort mogelijk te zijn aan te tonen dat:

- a) registraties volledig zijn en op geen enkele wijze zijn gemanipuleerd;
- b) kopieën van elektronische bewijsstukken waarschijnlijk identiek zijn aan de originelen;
- c) elk informatiesysteem waarvan bewijsmateriaal is verkregen, correct werkte op het moment van vastlegging van het bewijsmateriaal.

Indien beschikbaar, behoort certificatie of andere relevante methoden om personeel en middelen te kwalificeren te worden gezocht om de waarde van het verkregen bewijs te versterken.

Digitaal bewijs kan grenzen van organisaties of rechtsgebieden overschrijden. In zulke gevallen behoort te worden gewaarborgd dat de organisatie het recht heeft de vereiste informatie als digitaal bewijs te verzamelen.

### Overige informatie

Direct na het ontdekken van een informatiebeveiligingsgebeurtenis is het niet altijd duidelijk of de gebeurtenis zal leiden tot gerechtelijke stappen. Het gevaar bestaat dan ook dat noodzakelijk bewijs bewust of toevallig wordt vernietigd voordat de ernst van het incident wordt onderkend. Het is raadzaam om vroegtijdig juridisch advies of de rechtshandhavers in te schakelen als gerechtelijke stappen worden overwogen en advies in te winnen over het vereiste bewijs.

ISO/IEC 27037 biedt definities en richtlijnen voor het identificeren, verzamelen, verkrijgen en bewaren van digitaal bewijs.

De ISO/IEC 27050-reeks behandelt elektronische ontdekking, hetgeen gepaard gaat met het als bewijsmiddel verwerken van elektronisch opgeslagen informatie.

## 5.29 Informatiebeveiliging tijdens een verstoring

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht

### Beheersmaatregel

De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.

### Doel

Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.

### Richtlijn

De organisatie behoort haar eisen vast te stellen voor het tijdens een verstoring aanpassen van beheersmaatregelen voor informatiebeveiliging. Informatiebeveiligingseisen behoren te worden opgenomen in de processen voor bedrijfscontinuïteitsbeheer van de organisatie.

Er behoren plannen te worden ontwikkeld, geïmplementeerd, getest, beoordeeld en geëvalueerd om de beveiliging van informatie van essentiële bedrijfsprocessen in stand te houden of te herstellen na een (ver)storing. De beveiliging van informatie behoort op het vereiste niveau en binnen de vereiste tijdsbestekken te worden hersteld.

De organisatie behoort het volgende te implementeren en te onderhouden:

- a) beheersmaatregelen voor informatiebeveiliging, ondersteunende systemen en hulpmiddelen binnen bedrijfscontinuïteits- en ICT-continuïteitsplannen;
- b) processen om bestaande beheersmaatregelen voor informatiebeveiliging tijdens een verstoring in stand te houden;
- c) compenserende beheersmaatregelen voor beheersmaatregelen voor informatiebeveiliging die tijdens een verstoring niet kunnen worden gehandhaafd.

### Overige informatie

In de context van de bedrijfscontinuïteits- en ICT-continuïteitsplanning kan het nodig zijn de informatiebeveiligingseisen aan te passen, afhankelijk van de soort verstoring, in vergelijking met de normale operationele omstandigheden. Als onderdeel van de bedrijfsimpactanalyse en de risicobeoordeling die worden uitgevoerd binnen bedrijfscontinuïteitsbeheer, behoren de gevolgen van het wegvallen van de geheimhouding en de integriteit van informatie, naast de noodzaak om de beschikbaarheid in stand te houden, te worden overwogen en geprioriteerd.

Informatie over systemen voor bedrijfscontinuïteitsbeheer is te vinden in ISO 22301 en ISO 22313. Verdere richtlijnen voor bedrijfsimpactanalyse (BIA) zijn te vinden in ISO/TS 22317.

### 5.30 ICT-gereedheid voor bedrijfscontinuïteit

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Corrigerend	#Beschikbaarheid	#Reageren	#Continuïteit	#Veerkracht

#### Beheersmaatregel

De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.

#### Doel

De beschikbaarheid van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie tijdens een verstoring waarborgen.

#### Richtlijn

De ICT-gereedheid voor bedrijfscontinuïteit is een belangrijk onderdeel van bedrijfscontinuïteitsbeheer en informatiebeveiligingsbeheer om te bewerkstelligen dat ook tijdens een verstoring aan de doelstellingen van de organisatie kan blijven worden voldaan.

De ICT-continuïteitseisen zijn het resultaat van de bedrijfsimpactanalyse (BIA). Het BIA-proces behoort gebruik te maken van impactsoorten en -criteria om de impact in de tijd als gevolg van de verstoring van bedrijfsactiviteiten die producten en diensten leveren te beoordelen. De omvang en de duur van de daaruit voortvloeiende gevolgen behoren te worden gebruikt om geprioriteerde activiteiten waaraan een hersteltijd-doelstelling (RTO) behoort te worden toegekend te identificeren. De BIA behoort vervolgens vast te stellen welke middelen nodig zijn om geprioriteerde activiteiten te ondersteunen. Er behoort ook een RTO te worden gespecificeerd voor deze middelen. Een deel van deze middelen behoort ICT-diensten te omvatten.

De BIA waarbij ICT-diensten worden betrokken, kan worden uitgebreid om de prestatie- en capaciteitseisen van ICT-systemen en de RPO's van informatie die nodig is om activiteiten te ondersteunen tijdens een verstoring, te definiëren.

Op basis van de output van de BIA en risicobeoordeling waarbij ICT-diensten worden betrokken, behoort de organisatie strategieën voor ICT-continuïteit te identificeren en selecteren waarin opties voor voorafgaand aan, tijdens en na een verstoring in overweging worden genomen. De strategieën voor bedrijfscontinuïteit kunnen uit een of meer oplossingen bestaan. Op basis van de strategieën behoren plannen te worden opgesteld, geïmplementeerd en getest om na een (ver)storing van essentiële processen het vereiste beschikbaarheidsniveau van ICT-diensten binnen de vereiste tijdsbestekken te halen.

De organisatie behoort ervoor te zorgen dat:

- a) er een adequate organisatiestructuur is die is voorbereid op een verstoring, deze verzacht en erop reageert, ondersteund door personeel met de nodige verantwoordelijkheid, autoriteit en competentie;
- b) ICT-continuïteitsplannen, met inbegrip van respons- en herstelprocedures waarin wordt beschreven hoe de organisatie gepland heeft een verstoring van de ICT-diensten te beheren:
  - 1) regelmatig door middel van oefeningen en tests worden geëvalueerd;
  - 2) door het management worden goedgekeurd;
- c) ICT-continuïteitsplannen de volgende ICT-continuïteitsinformatie omvatten:
  - 1) prestatie- en capaciteitsspecificaties om te voldoen aan de bedrijfscontinuïteitseisen en -doelstellingen zoals gespecificeerd in de BIA;
  - 2) de RTO van elke geprioriteerde ICT-dienst en de procedures voor het herstel van die componenten;
  - 3) de RPO van de als informatie gedefinieerde geprioriteerde ICT-middelen en de procedures om de informatie te herstellen.

### **Overige informatie**

Het beheer van de ICT-continuïteit vormt een essentieel onderdeel van de bedrijfscontinuïteitseisen met betrekking tot beschikbaarheid om in staat te zijn:

- a) te reageren op en te herstellen van verstoringen van ICT-diensten ongeacht de oorzaak;
- b) te bewerkstelligen dat de continuïteit van geprioriteerde activiteiten door de vereiste ICT-diensten wordt ondersteund;
- c) te reageren voordat er zich een verstoring van de ICT-diensten voordoet en zodra er ten minste één incident is waargenomen dat kan leiden tot een verstoring van de ICT-diensten.

Verdere richtlijnen over de ICT-gereedheid voor bedrijfscontinuïteit zijn te vinden in ISO/IEC 27031.

Verdere richtlijnen over een systeem voor bedrijfscontinuïteitsbeheer zijn te vinden in ISO 22301 en ISO 22313.

Verdere richtlijnen over BIA zijn te vinden in ISO/TS 22317.

### **5.31 Wettelijke, statutaire, regelgevende en contractuele eisen**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Juridisch_en_compliance	#Governance_en_Ecosysteem #Bescherming

**Beheersmaatregel**

Eisen van wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen behoren te worden vastgesteld, gedocumenteerd en actueel gehouden.

**Doel**

De naleving bewerkstelligen van wettelijke, statutaire, regelgevende en contractuele eisen in verband met informatiebeveiliging.

**Richtlijn**Algemeen

Externe eisen, met inbegrip van wettelijke, statutaire, regelgevende en contractuele eisen behoren in aanmerking te worden genomen bij het:

- a) ontwikkelen van informatiebeveiligingsbeleid en -procedures;
- b) ontwerpen, implementeren of wijzigen van beheersmaatregelen voor informatiebeveiliging;
- c) classificeren van informatie en andere gerelateerde bedrijfsmiddelen in het kader van het proces voor het vaststellen van informatiebeveiligingseisen voor interne behoeften of voor overeenkomsten met leveranciers;
- d) uitvoeren van risicobeoordelingen met het oog op informatiebeveiliging en het vaststellen van de activiteiten voor de behandeling van informatiebeveiligingsrisico's;
- e) vaststellen van processen plus de bijbehorende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging;
- f) vaststellen van de contractuele eisen voor leveranciers die relevant zijn voor de organisatie en de reikwijdte van de levering van producten en diensten.

Wet- en regelgeving

De organisatie behoort:

- a) alle wet- en regelgeving te identificeren die relevant zijn voor de informatiebeveiliging van de organisatie om op de hoogte te zijn van de eisen voor haar soort bedrijf;
- b) het voldoen eraan in alle relevante landen in aanmerking te nemen, indien de organisatie:
  - zaken doet in andere landen;
  - producten en diensten gebruikt uit andere landen waar wet- en regelgeving van invloed kunnen zijn op de organisatie;
  - informatie over de grenzen van rechtsgebieden transporteert waar wet- en regelgeving van invloed kunnen zijn op de organisatie;
- c) de geïdentificeerde wet- en regelgeving regelmatig te beoordelen om op de hoogte te blijven van wijzigingen en nieuwe wetgeving te identificeren;
- d) de specifieke processen en individuele verantwoordelijkheden om aan deze eisen te voldoen te definiëren en documenteren.

### Cryptografie

Cryptografie is een gebied waarvoor vaak specifieke wettelijke eisen gelden. Het naleven van de relevante overeenkomsten en wet- en regelgeving met betrekking tot de volgende punten behoort in aanmerking te worden genomen:

- a) beperkingen op de import of export van computerhardware en -software voor het uitvoeren van cryptografische functies;
- b) beperkingen op de import of export van computerhardware en -software die zo zijn ontworpen dat er cryptografische functies aan kunnen worden toegevoegd;
- c) beperkingen op de toepassing van cryptografie;
- d) verplichte of discretionaire methoden voor de toegang van de overheidsinstanties van de landen tot versleutelde informatie;
- e) geldigheid van digitale handtekeningen, zegels en certificaten.

Het wordt aanbevolen juridisch advies in te winnen om ervoor te zorgen dat de relevante wet- en regelgeving wordt nageleefd, vooral wanneer versleutelde informatie of cryptografie-instrumenten tot voorbij de grenzen van rechtsgebieden worden verplaatst.

### Contracten

Contractuele eisen in verband met informatiebeveiliging behoren de eisen te omvatten die zijn vermeld in:

- a) contracten met klanten;
- b) contracten met leveranciers (zie 5.20);
- c) verzekeringscontracten.

### **Overige informatie**

Geen overige informatie.

## **5.32 Intellectuele-eigendomsrechten**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Juridisch_en_compliance	#Governance_en_Ecosysteem

### **Beheersmaatregel**

De organisatie behoort passende procedures te implementeren om intellectuele eigendomsrechten te beschermen.

**Doel**

De naleving bewerkstelligen van eisen van wet- en regelgeving, statutaire en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van gepatenteerde producten.

**Richtlijn**

De volgende richtlijnen behoren in overweging te worden genomen om materiaal dat kan worden beschouwd als intellectuele eigendom te beschermen:

- a) onderwerpspecifiek beleid inzake de bescherming van intellectuele-eigendomsrechten definiëren en communiceren;
- b) procedures voor het voldoen aan intellectuele-eigendomsrechten publiceren die het gebruik van software en informatieproducten volgens de eisen definiëren;
- c) software alleen aanschaffen bij bekende bronnen met een goede reputatie, om te waarborgen dat het auteursrecht niet wordt geschonden;
- d) geschikte registers van bedrijfsmiddelen bijhouden, en alle bedrijfsmiddelen waarbij bescherming van intellectuele-eigendomsrechten vereist is, identificeren;
- e) bewijs en bewijsmateriaal bijhouden van de eigendom van licenties, handleidingen enz.
- f) bewerkstelligen dat een maximaal aantal gebruikers of middelen (bijv. CPU's) dat eventueel door de licentie is toegestaan, niet wordt overschreden;
- g) beoordelingen uitvoeren om te bewerkstelligen dat alleen goedgekeurde software en in licentie gegeven producten zijn geïnstalleerd;
- h) procedures vaststellen voor het handhaven van de juiste licentievoorwaarden;
- i) procedures vaststellen voor het verwijderen of aan anderen overdragen van software;
- j) voldoen aan voorwaarden voor software en informatie verkregen van openbare netwerken en externe bronnen;
- k) niet dupliceren, naar een ander formaat converteren of een uittreksel maken van commerciële opnamen (video, audio), tenzij dit auteursrechtelijk of volgens de licenties die van toepassing zijn, is toegestaan;
- l) geen normen (bijv. internationale normen van ISO/IEC), boeken, artikelen, rapporten of andere documenten geheel of ten dele kopiëren, tenzij dit auteursrechtelijk of volgens de licenties die van toepassing zijn, is toegestaan.

**Overige informatie**

Onder intellectuele-eigendomsrechten vallen auteursrechten op software of documenten, ontwerprechten, handelsmerken, patenten en broncode-licenties.

Eigendomssoftwareproducten worden gewoonlijk geleverd op basis van een licentieovereenkomst die de licentievoorwaarden vermeldt, bijv. het gebruik van de producten beperken tot bepaalde machines of het kopiëren beperken tot het maken van back-upkopieën. Zie de ISO/IEC 19770-reeks voor nadere informatie over het beheer van IT-bedrijfsmiddelen.

Gegevens kunnen worden verkregen uit externe bronnen. Doorgaans worden dergelijke gegevens verkregen op grond van een overeenkomst voor het delen van gegevens of een soortgelijk juridisch

instrument. In zulke overeenkomsten voor het delen van gegevens behoort duidelijk te worden gemaakt welke verwerking is toegestaan voor de verkregen gegevens. Het is ook raadzaam dat de herkomst van de gegevens duidelijk wordt vermeld. Zie ISO/IEC 23751 voor meer informatie over overeenkomsten voor het delen van gegevens.

Eisen van wet- en regelgeving, statutaire en contractuele eisen kunnen beperkingen inhouden voor het kopiëren van eigendomsmateriaal. In het bijzonder kan worden bepaald dat alleen materiaal mag worden gebruikt dat is ontwikkeld door de organisatie zelf of dat door de ontwikkelaar in licentie is gegeven aan de organisatie of aan de organisatie is geleverd. Schending van auteursrecht kan leiden tot gerechtelijke stappen, die kunnen resulteren in een geldboete of een strafproces.

Afgezien van het feit dat het nodig is dat de organisatie voldoet aan haar verplichtingen wat betreft de intellectuele-eigendomsrechten van derden, behoren de risico's dat personeel en derden de eigen intellectuele-eigendomsrechten van de organisatie niet behartigen ook te worden beheerst.

### 5.33 Beschermen van registraties

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Juridisch_en_compliance #Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Verdediging

#### Beheersmaatregel

Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.

#### Doel

De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen, alsmede gemeenschaps- of maatschappelijke verwachtingen, met betrekking tot de bescherming en beschikbaarheid van registraties.

#### Richtlijn

De organisatie behoort de volgende stappen te ondernemen om de authenticiteit, betrouwbaarheid, integriteit en bruikbaarheid van registraties te beschermen, aangezien de bedrijfscontext en de eisen voor het beheer ervan na verloop van tijd veranderen:

- richtlijnen uitvaardigen inzake de opslag, de bewakingsketen voor de hantering, en het verwijderen van registraties, hetgeen ook het voorkomen van manipulatie van registraties omvat. Deze richtlijnen behoren te worden afgestemd op het onderwerpspecifieke beleid van de organisatie inzake het beheer van registraties en andere eisen aan registraties;
- een bewaarschema opstellen waarin registraties en de periode dat ze behoren te worden bewaard, zijn gedefinieerd.

Het systeem waarmee gegevens worden opgeslagen en behandeld, behoort de identificatie van registraties en hun bewaarperiode te waarborgen, rekening houdend, indien van toepassing, met nationale of regionale wet- of regelgeving, evenals de verwachtingen vanuit de gemeenschap of de

maatschappij. Dit systeem behoort toe te staan dat registraties na afloop van die termijn op een passende manier worden vernietigd als de organisatie ze niet langer nodig heeft.

Bij besluitvorming over bescherming van specifieke registraties van de organisatie behoort de informatiebeveiligingsclassificatie daarvan, gebaseerd op het classificatieschema van de organisatie, in overweging te worden genomen. Registraties behoren te worden gecategoriseerd naar types registratie (bijv. boekhoudkundige, transactie-, personeels-, juridische registraties). Bij elk type behoren de bewaartermijn en de toegestane soorten opslagmedia (fysiek of elektronisch) te worden vermeld.

Systemen voor gegevensopslag behoren zo te worden gekozen dat vereiste registraties binnen een aanvaardbare tijdsperiode en in een aanvaardbaar formaat kunnen worden opgevraagd, afhankelijk van de desbetreffende eisen.

Als elektronische opslagmedia worden gekozen behoren procedures te worden vastgesteld om te waarborgen dat de registraties tijdens de bewaarperiode toegankelijk blijven (leesbaarheid van zowel de opslagmedia als van het gegevensformaat), om te voorkomen dat de informatie verloren gaat als gevolg van toekomstige technologische veranderingen. Ook gerelateerde cryptografische sleutels en programma's die samenhangen met versleutelde archieven of digitale handtekeningen, behoren te worden bewaard om decodering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties (zie 8.24).

Procedures voor het bewaren en behandelen van deze media behoren te worden geïmplementeerd in overeenstemming met de aanbevelingen van fabrikanten van opslagmedia. Er behoort rekening te worden gehouden met de mogelijkheid dat media die worden gebruikt om registraties te bewaren, in kwaliteit achteruitgaan.

### **Overige informatie**

Registraties documenteren individuele gebeurtenissen of transacties of kunnen samenvoegingen zijn van gegevens die ervoor zijn opgezet om arbeidsprocessen, activiteiten of functies te documenteren. Ze vormen het bewijs van zowel bedrijfsactiviteiten als van informatiebedrijfsmiddelen. Elke informatieverzameling, ongeacht structuur of vorm, kan als registratie worden beheerd. Dit omvat informatie in de vorm van een document, een verzameling gegevens of andere soorten digitale of analoge informatie die in het kader van de bedrijfsvoering worden aangemaakt, vastgelegd en beheerd.

In het kader van het beheren van registraties zijn metagegevens gegevens die de context, inhoud en structuur van registraties, evenals het beheer ervan in de loop van de tijd, beschrijven. Metagegevens zijn een essentieel bestanddeel van elke registratie.

Het kan nodig zijn sommige registraties veilig te bewaren om te voldoen aan eisen van wet- en regelgeving, statutaire en contractuele eisen, en om essentiële bedrijfsactiviteiten te ondersteunen. De bewaartermijn en de soort informatie die behoort te worden bewaard, kunnen zijn vastgelegd in nationale wet- of regelgeving. Verdere informatie over beheer van registraties is te vinden in ISO 15489.

### 5.34 Privacy en bescherming van persoonsgegevens

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Informatiebescherming #Juridisch_en_compliance	#Bescherming

#### Beheersmaatregel

De organisatie behoort de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen.

#### Doel

De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot de informatiebeveiligingsaspecten voor de bescherming van persoonsgegevens.

#### Richtlijn

De organisatie behoort een onderwerpspecifiek beleid inzake privacy en bescherming van persoonsgegevens vast te stellen en aan alle relevante belanghebbenden mee te delen.

De organisatie behoort procedures te ontwikkelen en te implementeren voor het behoud van privacy en het beschermen van persoonsgegevens. Deze procedures behoren te worden gecommuniceerd aan alle relevante belanghebbenden die betrokken zijn bij het verwerken van persoonsgegevens.

Naleving van deze procedures en van alle relevante wet- en regelgeving betreffende het behoud van privacy en het beschermen van persoonsgegevens vereist passende rollen, verantwoordelijkheden en beheersmaatregelen. Vaak kan dit het beste worden bereikt door een persoon te benoemen die hiervoor verantwoordelijk is, zoals een privacyfunctionaris, die richtlijnen behoort te geven aan personeel, dienstverleners en andere belanghebbenden over hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd.

Verantwoordelijkheid voor het omgaan met persoonsgegevens behoort met inachtneming van de desbetreffende wet- en regelgeving te worden behandeld.

Er behoren passende technische en organisatorische maatregelen te worden geïmplementeerd om persoonsgegevens te beschermen.

#### Overige informatie

Een aantal landen heeft wetgeving ingevoerd waardoor er beheersmaatregelen zijn ingesteld voor het verzamelen, verwerken, verzenden en wissen van persoonsgegevens. Afhankelijk van de respectieve nationale wetgeving kunnen dergelijke beheersmaatregelen verplichtingen opleggen aan personen die persoonsgegevens verzamelen, verwerken en verspreiden, en kunnen zij ook de bevoegdheid voor het versturen van persoonsgegevens naar andere landen beperken.

ISO/IEC 29100 voorziet in een kader op hoog niveau voor de bescherming van persoonsgegevens binnen ICT-systemen. Verdere informatie over privacy-informatiebeheersystemen is te vinden in ISO/IEC 27701. Specifieke informatie met betrekking tot privacy-informatiebeheer voor publieke clouds die als verwerkers van persoonsgegevens fungeren is te vinden in ISO/IEC 27018.

ISO/IEC 29134 geeft richtlijnen voor privacy-effectbeoordelingen (PIA) en een voorbeeld van de structuur en inhoud van een PIA-rapport. In vergelijking met ISO/IEC 27005 is dit toegespitst op het verwerken van persoonsgegevens en is het relevant voor die organisaties die persoonsgegevens verwerken. Dit kan helpen bij het identificeren van privacyrisico's en mogelijke beperkende maatregelen om deze risico's tot een aanvaardbaar niveau terug te brengen.

### 5.35 Onafhankelijke beoordeling van informatiebeveiliging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Borging_van_infor- matiebeveiliging	#Governance_en_ Ecosysteem

#### Beheersmaatregel

De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.

#### Doel

Waarborgen dat de organisatie continu een geschikte, toereikende en doeltreffende aanpak voor het beheer van informatiebeveiliging hanteert.

#### Richtlijn

De organisatie behoort te beschikken over processen om onafhankelijke beoordelingen uit te voeren.

Het management behoort periodieke onafhankelijke beoordelingen te plannen en te initiëren. De beoordelingen behoren tevens het beoordelen van verbetermogelijkheden en de noodzaak om wijzigingen aan te brengen in de informatiebeveiligingsaanpak te omvatten, met inbegrip van het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en andere beheersmaatregelen.

Dergelijke beoordelingen behoren te worden uitgevoerd door personen met een onafhankelijke positie ten opzichte van het te beoordelen gebied (bijv. door de interne auditor, een onafhankelijke manager of een externe organisatie die gespecialiseerd is in dergelijke beoordelingen). Personen die deze beoordelingen uitvoeren, behoren te beschikken over de passende competentie. Om te garanderen dat de persoon die de beoordelingen uitvoert voldoende onafhankelijk is om een beoordeling uit te voeren, behoort hij of zij geen deel uit te maken van de hiërarchie.

De resultaten van de onafhankelijke beoordelingen behoren te worden gerapporteerd aan het management dat de beoordelingen heeft geïnitieerd en, indien van toepassing, de directie. Deze registraties behoren te worden bewaard.

Indien in de onafhankelijke beoordelingen wordt vastgesteld dat de aanpak en de implementatie van het beheer van informatiebeveiliging van de organisatie niet voldoen [bijv. gedocumenteerde doelstellingen en eisen zijn niet gehaald of niet in overeenstemming met de koers voor informatiebeveiliging zoals opgenomen in het beleid voor informatiebeveiliging en onderwerpspecifieke beleidsregels (zie 5.1)], behoort het management corrigerende maatregelen te initiëren.

In aanvulling op de periodieke onafhankelijke beoordelingen behoort de organisatie te overwegen onafhankelijke beoordelingen uit te voeren wanneer:

- a) wet- en regelgeving die van invloed is op de organisatie, verandert;
- b) er zich belangrijke incidenten voordoen;
- c) de organisatie een nieuw bedrijf start of een bestaand bedrijf verandert;
- d) de organisatie een nieuw product of nieuwe dienst gaat gebruiken of het gebruik van een actueel gebruikt(e) product of dienst wijzigt;
- e) de organisatie de beheersmaatregelen en procedures voor informatiebeveiliging significant wijzigt.

### Overige informatie

ISO/IEC 27007 en ISO/IEC TS 27008 voorzien in richtlijnen voor het uitvoeren van onafhankelijke beoordelingen.

## 5.36 Naleving van beleid, regels en normen voor informatiebeveiliging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Juridisch_en_compliance #Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem

### Beheersmaatregel

De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.

### Doel

Bewerkstelligen dat informatiebeveiliging in overeenstemming met het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en normen van de organisatie wordt geïmplementeerd en uitgevoerd.

### Richtlijn

Managers of de eigenaren van diensten, producten of informatie behoren vast te stellen op welke manier wordt beoordeeld of aan informatiebeveiligingseisen zoals gedefinieerd in het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels, normen en andere toepasselijke regelgeving, wordt nageleefd. Voor een doeltreffende regelmatige beoordeling behoort te worden overwogen om automatische meet- en rapportage-instrumenten in te zetten.

Indien de beoordeling een geval van niet-naleving oplevert, behoren managers:

- a) de oorzaken van de niet-naleving vast te stellen;
- b) de noodzaak te evalueren tot het treffen van corrigerende maatregelen om naleving te bewerkstelligen;

- c) passende corrigerende maatregelen te implementeren;
- d) de getroffen corrigerende maatregelen te beoordelen om de doeltreffendheid ervan te verifiëren en om gebreken of zwakke plekken te identificeren.

Resultaten van door managers of de eigenaren van diensten, producten of informatie uitgevoerde beoordelingen en getroffen corrigerende maatregelen behoren te worden geregistreerd en deze registraties behoren te worden bewaard. Managers behoren de resultaten te rapporteren aan de personen die onafhankelijke beoordelingen uitvoeren (zie 5.35) wanneer een onafhankelijke beoordeling plaatsvindt binnen hun verantwoordelijkheidsgebied.

Corrigerende maatregelen behoren tijdig te worden voltooid, naarmate passend is gezien het risico. Indien deze maatregelen niet voor de volgende geplande beoordeling zijn voltooid, behoren de vorderingen in ieder geval als onderdeel van die beoordeling te worden behandeld.

### Overige informatie

Operationele monitoring van het gebruik van systemen wordt behandeld in 8.15, 8.16, 8.17.

## 5.37 Gedocumenteerde bedieningsprocedures

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Herstellen	#Beheer_van_bedrijfs_middelen #Fysieke_beveiliging #Systeem-en_netwerkbeveiliging #Toepassingsbeveiliging #Veilige_configuratie #Identiteits-en_toegangsbeheer #Beheer_van_dreigingen_en_kwetsbaarheden #Continuïteit #Beheer_van_informatiebeveiligingsgebeurtenissen	#Governance_en_Ecosysteem #Bescherming #Verdediging

### Beheersmaatregel

Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.

### Doel

De correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.

## **Richtlijn**

Er behoren gedocumenteerde procedures te worden opgesteld voor de operationele activiteiten van de organisatie die verband houden met informatiebeveiliging, bijvoorbeeld:

- a) wanneer het nodig is dat de activiteit door veel mensen op dezelfde manier wordt uitgevoerd;
- b) wanneer de activiteit zelden wordt uitgevoerd en waarschijnlijk vergeten zal zijn als zij weer wordt uitgevoerd;
- c) wanneer de activiteit nieuw is en een risico inhoudt als zij niet correct wordt uitgevoerd;
- d) voorafgaand aan de overdracht van de activiteit aan nieuwe medewerkers.

In de bedieningsprocedures behoort het volgende te worden gespecificeerd:

- a) welke personen verantwoordelijk zijn;
- b) de beveiligde installatie en configuratie van systemen;
- c) verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig;
- d) back-up (zie 8.13) en veerkracht;
- e) de planning van eisen, waaronder onderlinge afhankelijkheden met andere systemen;
- f) instructies voor het omgaan met fouten of andere uitzonderlijke omstandigheden [bijv. beperkingen ten aanzien van het gebruik van systeemhulpmiddelen (zie 8.18)] die zich tijdens de uitvoering van een functie kunnen voordoen;
- g) ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden;
- h) instructies voor het behandelen van opslagmedia (zie 7.10 en 7.14);
- i) procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen;
- j) het beheer van informatie uit audittrajecten en systeemlogbestanden (zie 8.15 en 8.17) en videobewakingssystemen (zie 7.4);
- k) monitoringprocedures zoals capaciteit, prestaties en beveiliging (zie 8.6 en 8.16);
- l) onderhoudsinstructies.

Gedocumenteerde bedieningsprocedures behoren te worden beoordeeld en zo nodig bijgewerkt. Wijzigingen in gedocumenteerde bedieningsprocedures behoren te worden geautoriseerd. Indien technisch haalbaar behoren informatiesystemen consistent te worden beheerd, met gebruikmaking van dezelfde procedures, instrumenten en hulpmiddelen.

## **Overige informatie**

Geen overige informatie.

## 6 Mensgerichte beheersmaatregelen

### 6.1 Screening

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem

#### Beheersmaatregel

De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie behoort te worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving, voorschriften en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.

#### Doel

Bewerkstelligen dat al het personeel in aanmerking komt en geschikt is voor de functies waarvoor zij worden overwogen en dat zij hiervoor gedurende hun dienstverband in aanmerking blijven komen en geschikt blijven.

#### Richtlijn

Al het personeel, met inbegrip van voltijd-, deeltijd- en tijdelijk personeel, behoort te worden gescreend. Indien deze personen via dienstverleners worden ingehuurd, behoren screeningseisen te worden opgenomen in de contractuele afspraken tussen de organisatie en de dienstverleners.

Informatie over alle kandidaten die in aanmerking komen voor posities binnen de organisatie, behoort te worden verzameld en verwerkt met inachtneming van de relevante wetgeving in het relevante rechtsgebied. In bepaalde rechtsgebieden kan het wettelijk vereist zijn dat de organisatie de kandidaten vooraf op de hoogte stelt van de screeningsactiviteiten.

Bij deze controle behoort alle relevante wetgeving op het gebied van privacy, bescherming van persoonsgegevens en arbeidswetgeving in acht te worden genomen, en de controle behoort, voor zover toegestaan, het volgende te omvatten:

- de beschikbaarheid van positieve referenties (bijv. zakelijke en persoonlijke referenties);
- een controle (op volledigheid en nauwkeurigheid) van het curriculum vitae van de sollicitant;
- bevestiging van de geclaimde academische en beroepskwalificaties;
- onafhankelijke identiteitscontrole (bijv. een paspoort of ander aanvaardbaar document dat is afgegeven door een passende instantie);
- meer gedetailleerde controle, zoals controle op kredietwaardigheid of strafblad indien de kandidaat een essentiële rol krijgt.

Als een persoon wordt ingehuurd voor een specifieke informatiebeveiligingsrol, behoort de organisatie zich ervan te vergewissen dat:

- a) de kandidaat over de nodige competentie beschikt om de beveiligingsrol te vervullen;
- b) de kandidaat de rol kan worden toevertrouwd, in het bijzonder als de rol cruciaal is voor de organisatie.

Als een functie, hetzij bij een eerste aanstelling, hetzij bij promotie, met zich meebrengt dat de persoon toegang heeft tot faciliteiten die informatie verwerken, en, in het bijzonder, indien het hierbij gaat om vertrouwelijke informatie (bijv. financiële, persoonlijke of medische informatie of zeer vertrouwelijke informatie), behoort de organisatie ook verdere, meer gedetailleerde verificaties te overwegen.

In procedures behoren criteria en beperkingen voor controleonderzoeken te worden gedefinieerd (bijv. wie is competent om personen te screenen, en hoe, wanneer en waarom worden controleonderzoeken uitgevoerd).

In situaties waarin de controle niet tijdig kan worden voltooid, behoren beperkende beheersmaatregelen te worden geïmplementeerd totdat de beoordeling is voltooid, bijvoorbeeld:

- a) uitgestelde 'onboarding';
- b) uitgestelde inzet van bedrijfsmiddelen van het bedrijf;
- c) 'onboarding' met beperkte toegang;
- d) beëindiging van het dienstverband.

Deze controles behoren op gezette tijden te worden herhaald om te bevestigen dat personeel nog altijd geschikt is, afhankelijk van hoe essentieel de rol van een persoon is.

#### **Overige informatie**

Geen overige informatie.

## **6.2 Arbeidsovereenkomst**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_ecosysteem

#### **Beheersmaatregel**

In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.

#### **Doel**

Bewerkstelligen dat personeel begrijpt wat hun verantwoordelijkheden zijn op het gebied van informatiebeveiliging voor de rollen waarvoor zij mogelijk in aanmerking komen.

## Richtlijn

In de contractuele verplichtingen voor personeel behoren het informatiebeveiligingsbeleid en relevante onderwerpspecifieke beleidsregels van de organisatie in aanmerking te worden genomen. Bovendien kunnen de volgende punten worden opgehelderd en vermeld:

- a) vertrouwelijkheids- of geheimhoudingsovereenkomsten die door personeel dat toegang krijgt tot vertrouwelijke informatie, behoren te worden ondertekend alvorens aan personeel toegang wordt verleend tot informatie en andere gerelateerde bedrijfsmiddelen (zie 6.6);
- b) wettelijke verantwoordelijkheden en rechten [bijv. betreffende auteursrechtwetgeving of wetgeving inzake gegevensbescherming (zie 5.32 en 5.34)];
- c) verantwoordelijkheden met betrekking tot de classificatie van informatie en het beheer van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, informatieverwerkende faciliteiten en informatiediensten waarmee het personeel omgaat (zie 5.9 t/m 5.13);
- d) verantwoordelijkheden voor het omgaan met van belanghebbenden ontvangen informatie;
- e) te treffen maatregelen indien personeel de beveiligingseisen van de organisatie veronachtzaamt (zie 6.4).

De informatiebeveiligingsrollen en de verantwoordelijkheden behoren tijdens het voortraject van het aanstellingsproces aan kandidaten te worden gecommuniceerd.

De organisatie behoort ervoor te zorgen dat personeel en contractanten instemmen met voorwaarden betreffende informatiebeveiliging. Deze voorwaarden behoren te passen bij de aard en de mate van toegang die ze zullen krijgen tot de bedrijfsmiddelen van de organisatie die samenhangen met informatiesystemen en -diensten. De voorwaarden inzake informatiebeveiliging behoren te worden beoordeeld wanneer wetten, regelgeving, het informatiebeveiligingsbeleid of onderwerpspecifieke beleidsregels veranderen.

Waar van toepassing behoren de verantwoordelijkheden die in de arbeidsovereenkomst staan, voor een vastgestelde periode na het einde van het dienstverband van kracht te blijven (zie 6.5).

## Overige informatie

Er kan een gedragscode worden gebruikt die de verantwoordelijkheden van het personeel in het kader van informatiebeveiliging aangeeft ten aanzien van vertrouwelijkheid, bescherming van persoonsgegevens, ethiek, passend gebruik van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, alsmede ten aanzien van door de organisatie verwacht moreel verantwoord handelen.

Een externe partij waarmee personeel van leveranciers is verbonden, kan ertoe zijn verplicht namens de gecontracteerde persoon contractuele afspraken te maken.

Indien de organisatie geen rechtspersoon is en geen werknemers heeft, kan het equivalent van een contractuele overeenkomst en van contractuele voorwaarden in aanmerking worden genomen, overeenkomstig de richtlijnen van deze beheersmaatregel.

### 6.3 Bewustwording van, opleiding en training in informatiebeveiliging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem

#### Beheersmaatregel

Personeel van de organisatie en relevante belanghebbenden behoren een passend(e) bewustwording van, opleiding, training en bijscholing in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.

#### Doel

Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.

#### Richtlijn

##### Algemeen

Een bewustwordingsprogramma, -opleiding en -training voor informatiebeveiliging behoren te worden vastgesteld in overeenstemming met het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de te beschermen informatie van de organisatie en de beheersmaatregelen voor informatiebeveiliging die zijn geïmplementeerd om de informatie te beschermen.

Opleiding en training voor bewustwording van informatiebeveiliging behoort periodiek plaats te vinden. Een basisbewustwordingsprogramma, -opleiding en -training kunnen van toepassing zijn op nieuw personeel en op personeel dat naar nieuwe functies of rollen met substantieel andere informatiebeveiligingseisen overstapt.

Om de kennisoverdracht en doeltreffendheid van het bewustwordings-, opleidings- of trainingsprogramma te testen behoort aan het eind van een bewustwordings-, opleidings- of trainingsactiviteit een beoordeling van het inzicht van het personeel te worden uitgevoerd.

##### Bewustwording

Een bewustwordingsprogramma voor informatiebeveiliging behoort erop gericht te zijn om personeel bewust te maken van hun verantwoordelijkheden voor informatiebeveiliging en de manieren waarop personeel zich van deze verantwoordelijkheden kan kwijten.

Bij het plannen van het bewustwordingsprogramma behoort rekening te worden gehouden met de rollen van het personeel binnen de organisatie, met inbegrip van intern en extern personeel (bijv. externe consultants, personeel van leveranciers). De activiteiten in het bewustwordingsprogramma behoren op zo'n manier te worden gespreid en bij voorkeur regelmatig te worden uitgevoerd dat de activiteiten worden herhaald en nieuw personeel deze ook meemaken. Er behoort te worden voortgebouwd op lering die is getrokken uit informatiebeveiligingsincidenten.

Het bewustwordingsprogramma behoort een aantal bewustwordingsactiviteiten te bevatten via passende fysieke of virtuele kanalen, zoals campagnes, boekjes, posters, nieuwsbrieven, websites, informatiesessies, briefings, e-learningmodules en e-mails.

Bewustwording van informatiebeveiliging behoort algemene aspecten te omvatten zoals:

- a) de betrokkenheid van het management bij informatiebeveiliging in de gehele organisatie;
- b) de noodzaak van bekend zijn met en het voldoen aan de van toepassing zijnde regels en verplichtingen met betrekking tot informatiebeveiliging, rekening houdend met informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels, normen, wetten, statuten, regelgeving, contracten en overeenkomsten;
- c) persoonlijke verantwoordelijkheid voor eigen doen en laten, en algemene verantwoordelijkheden ten opzichte van het beveiligen of beschermen van informatie die eigendom is van de organisatie en belanghebbenden;
- d) basisprocedures op informatiebeveiliging [zoals het melden van informatiebeveiligingsgebeurtenissen (6.8)] en basisbeheersmaatregelen [zoals wachtwoordbeveiliging (5.17)];
- e) contactpunten en bronnen voor aanvullende informatie en advies over informatiebeveiligingsaangelegenheden, met inbegrip van aanvullende materialen voor het verhogen van bewustwording van informatiebeveiliging.

### Opleiding en training

De organisatie behoort een passend trainingsplan vast te stellen, voor te bereiden en te implementeren voor technische teams met rollen die specifieke vaardigheden en deskundigheid vereisen. Technische teams behoren te beschikken over de vaardigheden voor het configureren en in stand houden van het vereiste beveiligingsniveau voor apparaten, systemen, toepassingen en diensten. Indien er vaardigheden ontbreken, behoort de organisatie actie te ondernemen om deze vaardigheden te verwerven.

Voor het opleidings- en trainingsprogramma behoren verschillende vormen te worden overwogen [bijv. lessen of zelfstudie, begeleiding door deskundig personeel of consultants (training in de praktijk), het rouleren van personeelsleden om verschillende activiteiten te volgen, mensen met de juiste vaardigheden werven en consultants inhuren]. Dit kan via verschillende middelen worden geleverd, bijv. klassikaal, via afstandsonderwijs, via internet, in eigen tempo. Technisch personeel behoort zijn kennis op peil te houden door zich te abonneren op nieuwsbrieven en tijdschriften of door conferenties en evenementen te bezoeken die zich richten op technische en professionele verbetering.

### **Overige informatie**

Bij het opstellen van een bewustwordingsprogramma is het belangrijk niet alleen de aandacht te richten op het 'wat' en 'hoe', maar ook op het 'waarom', indien mogelijk. Het is belangrijk dat personeel het doel van informatiebeveiliging en de mogelijke uitwerking, positief en negatief, van het eigen gedrag op de organisatie begrijpt.

Bewustwording van, opleiding en training in informatiebeveiliging kunnen onderdeel zijn van, of worden gegeven in combinatie met andere activiteiten, bijvoorbeeld algemene informatiemanagement-, ICT-, beveiligings-, privacy- of veiligheidstraining.

## 6.4 Disciplinaire procedure

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Personeelsbeveiliging	#Governance_en_Ecosysteem

### Beheersmaatregel

Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.

### Doel

Bewerkstelligen dat personeel en andere relevante belanghebbenden de gevolgen begrijpen van schending van het informatiebeveiligingsbeleid, personeel en andere relevante belanghebbenden ervan weerhouden zich schuldig te maken aan een schending, en personeel en andere relevante belanghebbenden die zich schuldig hebben gemaakt aan een schending op de juiste manier aanpakken.

### Richtlijn

De disciplinaire procedure behoort niet te worden geïnitieerd voordat is geverifieerd dat er zich een schending van het informatiebeveiligingsbeleid heeft voorgedaan (zie 5.28).

De formele disciplinaire procedure behoort te voorzien in een geleidelijke getrapte respons waarbij rekening wordt gehouden met factoren zoals:

- a) de aard (wie, wat, wanneer, hoe) en ernst van de inbreuk en de gevolgen ervan;
- b) of de overtreding opzettelijk (kwaadwillig) of onopzettelijk (per ongeluk) was;
- c) of het al dan niet een eerste overtreding betreft;
- d) of de overtreder al dan niet naar behoren was opgeleid.

Bij de reactie behoort rekening te worden gehouden met relevante eisen van wet- en regelgeving, statutaire, contractuele en bedrijfseisen evenals andere factoren voor zover vereist. De disciplinaire procedure behoort ook te worden gebruikt als een afschrikmiddel om te voorkomen dat personeel en andere relevante belanghebbenden het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures voor informatiebeveiliging overtreden. Opzettelijke schendingen van het informatiebeveiligingsbeleid kunnen onmiddellijke maatregelen vereisen.

### Overige informatie

Indien mogelijk behoort de identiteit van personen tegen wie disciplinaire actie wordt ondernomen overeenkomstig de toepasselijke eisen te worden beschermd.

Wanneer personen blijken hebben gegeven van uitstekend gedrag met betrekking tot informatiebeveiliging, kunnen ze worden beloond om de informatiebeveiliging te bevorderen en goed gedrag te stimuleren.

## 6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging #Beheer_van_bedrijfsmiddelen	#Governance_en_Ecosysteem

### Beheersmaatregel

Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.

### Doel

De belangen van de organisatie beschermen als onderdeel van de wijzigings- of beëindigingsprocedure van dienstverband of contracten.

### Richtlijn

Het proces voor het beheer van een beëindiging of verandering van dienstverband behoort te definiëren welke verantwoordelijkheden en plichten op het gebied van informatiebeveiliging na de beëindiging of verandering behoren te blijven gelden. Dit kan onder meer betrekking hebben op de vertrouwelijkheid van informatie, intellectuele eigendom en andere kennis die wordt verkregen, alsmede op de verantwoordelijkheden die deel uitmaken van andere geheimhoudingsovereenkomsten (zie 6.6). Verantwoordelijkheden en taken die na beëindiging van het dienstverband of contract nog altijd van kracht zijn, behoren te worden opgenomen in de arbeidsovereenkomst, het contract of de overeenkomst van de persoon (zie 6.2). Andere contracten of overeenkomsten die na het einde van het dienstverband van de persoon nog een bepaalde tijd doorlopen, kunnen ook verantwoordelijkheden op het gebied van informatiebeveiliging bevatten.

Wijzigingen in verantwoordelijkheid of dienstverband behoren te worden beheerst als het beëindigen van de desbetreffende verantwoordelijkheid of het desbetreffende dienstverband behoort te worden gecombineerd met het initiëren van de nieuwe verantwoordelijkheid of het nieuwe dienstverband.

De informatiebeveiligingsrollen en -verantwoordelijkheden van een persoon die een rol of functie neerlegt of van rol of functie verandert, behoren te worden geïdentificeerd en op een andere persoon te worden overgedragen.

Er behoort een proces te worden opgesteld om de wijzigingen en operationele procedures te communiceren naar het personeel, andere belanghebbenden en relevante contactpersonen (bijv. klanten en leveranciers).

Het proces voor het beëindigen of wijzigen van een dienstverband behoort ook te worden toegepast op extern personeel (d.w.z. leveranciers) wanneer een dienstverband van personeel, het contract of de functie bij de organisatie wordt beëindigd of wanneer er een verandering van functie binnen de organisatie is.

### Overige informatie

In veel organisaties is de afdeling personeelszaken doorgaans verantwoordelijk voor de totale beëindigingsprocedure en werkt deze afdeling samen met de direct leidinggevende van de persoon die

overstapt om de informatiebeveiligingsaspecten van de relevante procedures af te handelen. Als het gaat om personeel dat is ingehuurd via een externe partij (bijv. via een leverancier), dan wordt deze beëindigingsprocedure uitgevoerd door de externe partij in overeenstemming met het contract tussen de organisatie en de externe partij.

## 6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid	#Beschermen	#Personeelsbeveiliging #Informatiebescherming #Leveranciersrelaties	#Governance_en_ Ecosysteem

### Beheersmaatregel

Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.

### Doel

De vertrouwelijkheid van informatie waartoe personeel of externe partijen toegang hebben handhaven.

### Richtlijn

Vertrouwelijkheids- of geheimhoudingsovereenkomsten behoren de eis van bescherming van vertrouwelijke informatie te behandelen binnen juridisch afdwingbare voorwaarden.

Vertrouwelijkheids- of geheimhoudingsovereenkomsten zijn van toepassing op belanghebbenden en personeel van de organisatie. Op basis van de informatiebeveiligingseisen van een organisatie behoren de voorwaarden in de overeenkomsten te worden vastgesteld door te kijken naar de soort informatie waarmee de belanghebbenden of het personeel zullen omgaan, het classificatieniveau en het gebruik ervan en de toegestane toegang door de andere partij. Bij het vaststellen van eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten, behoren de volgende elementen in overweging te worden genomen:

- a) een definitie van de te beschermen informatie (bijv. vertrouwelijke informatie);
- b) de verwachte looptijd van een overeenkomst, met inbegrip van gevallen waarin het nodig kan zijn de vertrouwelijkheid onbeperkt te handhaven of tot de informatie openbaar beschikbaar wordt;
- c) de vereiste acties als een overeenkomst is beëindigd;
- d) de verantwoordelijkheden en acties van de ondertekenaars betreffende het vermijden van onbevoegd openbaar maken van informatie;
- e) de eigendom van informatie, handelsgeheimen en intellectuele eigendom, en hoe dit zich verhoudt tot de bescherming van vertrouwelijke informatie;
- f) het toegelaten gebruik van vertrouwelijke informatie en de rechten van de ondertekenaar om de informatie te gebruiken;

- g) het recht om activiteiten waar vertrouwelijke informatie voor uiterst gevoelige omstandigheden bij is betrokken, te auditen en te monitoren;
- h) de procedure voor het notificeren en melden van ongeoorloofde openbaarmaking of lekken van vertrouwelijke informatie;
- i) de voorwaarden voor retourneren of vernietigen van informatie na beëindiging van de overeenkomst;
- j) de verwachte te treffen maatregelen indien niet wordt voldaan aan de overeenkomst.

De organisatie behoort het voldoen aan vertrouwelijkheids- en geheimhoudingsovereenkomsten in aanmerking te nemen voor het rechtsgebied waarop deze van toepassing zijn (zie 5.31, 5.32, 5.33, 5.34).

Eisen voor vertrouwelijkheids- en geheimhoudingsovereenkomsten behoren periodiek te worden beoordeeld, en als zich veranderingen voordoen die van invloed zijn op deze eisen.

### Overige informatie

Vertrouwelijkheids- en geheimhoudingsovereenkomsten beschermen informatie van de organisatie en informeren de ondertekenaars over hun verantwoordelijkheid om informatie op een verantwoordelijke en bevoegde manier te beschermen, te gebruiken en openbaar te maken.

## 6.7 Werken op afstand

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfs-middelen #Informatiebescher-ming #Fysieke_beveiliging #Systeem-en_net-werkbeveiliging	#Bescherming

### Beheersmaatregel

Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.

### Doel

De beveiliging van informatie waarborgen wanneer personeel op afstand werkt.

### Richtlijn

Er is sprake van werken op afstand telkens wanneer personeel van de organisatie vanaf een locatie buiten het gebouw en/of terrein van de organisatie werkt en toegang maakt tot informatie, hetzij in gedrukte vorm of elektronisch via ICT-apparatuur. Omgevingen voor werken op afstand zijn onder andere omgevingen die worden aangeduid als 'telewerken', 'teleforenzen', 'flexibele werkplek', 'virtuele werkomgevingen' en 'onderhoud op afstand'.

**OPMERKING** Het is mogelijk dat niet alle aanbevelingen in deze richtlijn kunnen worden toegepast als gevolg van lokale wet- en regelgeving in verschillende rechtsgebieden.

Organisaties die activiteiten voor werken op afstand toestaan, behoren onderwerpspecifiek beleid inzake werken op afstand uit te vaardigen waarin de desbetreffende voorwaarden en beperkingen worden gedefinieerd. Waar van toepassing geacht, behoort rekening te worden gehouden met de volgende zaken:

- a) de bestaande of voorgestelde fysieke beveiliging van de locatie vanwaaraf op afstand wordt gewerkt, waarbij rekening wordt gehouden met de fysieke beveiliging van de locatie en de lokale omgeving, met inbegrip van de verschillende rechtsgebieden waar personeel zich bevindt;
- b) regels en beveiligingsmechanismen voor de fysieke werkomgeving op afstand, zoals afsluitbare archiefkasten, beveiligd transport tussen locaties en regels voor toegang op afstand, 'clear desk', het printen en verwijderen van informatie en andere gerelateerde bedrijfsmiddelen, en het melden van informatiebeveiligingsgebeurtenissen (zie 6.8);
- c) de verwachte fysieke werkomgevingen op afstand;
- d) de beveiligingseisen die voor communicatie gelden, waarbij rekening wordt gehouden met de behoefte aan toegang op afstand tot de systemen van de organisatie, de gevoeligheid van de informatie die wordt ingezien en via de communicatiekoppeling wordt doorgegeven, en de gevoeligheid van de systemen en toepassingen;
- e) het gebruik van toegang op afstand zoals virtuele desktoptoeegang die verwerking en opslag van informatie op privéapparatuur ondersteunt;
- f) de dreiging van onbevoegde toegang tot informatie of middelen van andere gebruikers op de locatie vanwaaraf op afstand wordt gewerkt (bijv. familie en vrienden);
- g) de dreiging van onbevoegde toegang tot informatie of middelen door andere personen op openbare plekken;
- h) het gebruik van thuisnetwerken en openbare netwerken en de eisen of beperkingen van de configuratie van draadloze netwerkdiensten;
- i) het gebruik van beveiligingsmaatregelen, zoals firewalls en bescherming tegen malware;
- j) beveiligde mechanismen voor het op afstand inzetten en initialiseren van systemen;
- k) beveiligde mechanismen voor het authenticeren en inschakelen van speciale toegangsrechten, rekening houdend met de kwetsbaarheid van eenfactorauthenticatiemechanismen waarbij toegang tot het netwerk van de organisatie vanaf een externe locatie is toegestaan.

De in acht te nemen richtlijnen en maatregelen behoren te omvatten:

- a) het beschikbaar stellen van passende apparatuur en opbergmeubelen voor de activiteiten van het werken op afstand, waarbij het gebruik van privéapparatuur die niet onder het beheer van de organisatie staat, niet is toegelaten;
- b) een definitie van geoorloofde werkzaamheden, de classificatie van informatie waarover men kan beschikken en de interne systemen en diensten waartoe de persoon die werkt op afstand, bevoegde toegang heeft;

- c) het voorzien in training voor personeel dat werkt op afstand en personeel dat ondersteuning biedt. Dit behoort ook in te gaan op hoe men veilig kan zakendoen tijdens het werken op afstand;
- d) het voorzien in passende communicatieapparatuur, met inbegrip van methoden voor het beveiligen van toegang op afstand, zoals eisen inzake schermvergrendeling en inactiviteitstimers; de mogelijkheid om de locatie van apparaten te traceren; de installatie van mogelijkheden om apparaten op afstand schoon te vegen;
- e) fysieke beveiliging;
- f) regels en richtlijnen voor toegang voor familie en bezoekers tot apparatuur en informatie;
- g) het beschikbaar stellen van ondersteuning en onderhoud van hardware en software;
- h) het regelen van de verzekering;
- i) de procedures voor de back-up en de bedrijfscontinuïteit;
- j) audit en monitoren van de beveiliging;
- k) intrekking van bevoegdheid en toegangsrechten en het inleveren van apparatuur na beëindiging van de werkactiviteiten op afstand.

### Overige informatie

Geen overige informatie.

## 6.8 Melden van informatiebeveiligingsgebeurtenissen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging

### Beheersmaatregel

De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.

### Doel

Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen die door personeel kunnen worden geïdentificeerd.

### Richtlijn

Al het personeel en alle gebruikers behoren bewust te worden gemaakt van hun verantwoordelijkheid om informatiebeveiligingsgebeurtenissen zo snel mogelijk te melden om het effect van informatiebeveiligingsincidenten te voorkomen of tot het minimum te beperken. Zij behoren ook te worden geïnformeerd over de procedure voor het melden van informatiebeveiligingsgebeurtenissen en het contactpunt waar de gebeurtenissen behoren te worden gemeld. Het meldmechanisme behoort zo eenvoudig, toegankelijk en beschikbaar mogelijk te zijn. Informatiebeveiligingsgebeurtenissen zijn onder andere incidenten, inbreuken en kwetsbaarheden.

Wat betreft het melden van informatiebeveiligingsgebeurtenissen, behoort rekening te worden gehouden met de volgende situaties:

- a) ondoeltreffende informatiebeveiligingsbeheersmaatregelen;
- b) schending van informatievertrouwelijkheid, -integriteit of aanwezige verwachtingen;
- c) menselijke fouten;
- d) het niet naleven van het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels of toepasselijke normen;
- e) schending van fysieke beveiligingsmaatregelen;
- f) wijzigingen aan systemen die niet het proces voor wijzigingsbeheer hebben doorlopen;
- g) storingen of ander afwijkend systeemgedrag van software of hardware;
- h) overtredingen van de toegangsregeling;
- i) kwetsbaarheden;
- j) vermoedelijke besmetting door malware.

Personeel en gebruikers behoort te worden geadviseerd niet te proberen om de vermeende aanwezigheid van kwetsbaarheden op het gebied van informatiebeveiliging aan te tonen. Het testen op kwetsbaarheden kan worden uitgelegd als potentieel misbruik van het systeem en kan ook schade veroorzaken aan het informatiesysteem en het kan digitaal bewijs corrumperen of aan het oog onttrekken. Uiteindelijk kan dit leiden tot wettelijke aansprakelijkheid voor de persoon die de tests uitvoert.

### Overige informatie

Zie de ISO/IEC 27035-reeks voor aanvullende informatie.

## 7 Fysieke beheersmaatregelen

### 7.1 Fysieke beveiligingszones

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming

### Beheersmaatregel

Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.

**Doel**

Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie voorkomen.

**Richtlijn**

Voor zover van toepassing behoren de volgende richtlijnen voor fysieke beveiligingszones te worden overwogen:

- a) beveiligingszones en de locatie en sterkte van elk van de buitengrenzen definiëren overeenkomstig de informatiebeveiligingseisen met betrekking tot bedrijfsmiddelen binnen de beveiligingszone;
- b) beschikken over fysiek solide buitengrenzen voor een gebouw of locatie met informatieverwerkende faciliteiten (d.w.z. dat er geen zwakke plekken mogen zitten in de buitengrenzen of beveiligingszones waardoor men gemakkelijk kan inbreken). De constructie van de buitendaken, -muren, -plafonds en -vloeren van de locatie behoort gedegen te zijn en alle buitendeuren behoren op passende wijze met toegangsbeveiligingsmechanismen (bijv. stangen, alarmen, sloten) te worden beschermd tegen toegang door onbevoegden. Deuren en ramen behoren afgesloten te zijn als er geen toezicht is en er behoort externe bescherming te worden overwogen voor ramen, met name op de begane grond; ook aan ventilatiepunten behoort aandacht te worden besteed;
- c) alle branddeuren die deel uitmaken van een beveiligingszone, van alarmsystemen voorzien en ze in combinatie met de muren monitoren en testen om vast te stellen of ze het vereiste weerstandsniveau, overeenkomstig geschikte normen, bieden. Ze behoren faalveilig te werken.

**Overige informatie**

Fysieke bescherming kan worden verkregen door een of meer fysieke barrières rond het gebouw en/of terrein en de informatieverwerkende faciliteiten van de organisatie aan te brengen.

Een beveiligd gebied kan een afsluitbaar kantoor zijn of diverse ruimten omgeven door een ononderbroken interne fysieke beveiligingsbarrière. Tussen zones met verschillende beveiligingseisen binnen de beveiligingszone kunnen extra barrières en buitengrenzen nodig zijn om fysieke toegang te beheersen. De organisatie behoort te overwegen fysieke beveiligingsmaatregelen in te voeren die tijdens situaties waar er sprake is van een verhoogd dreigingsniveau kunnen worden versterkt.

**7.2 Fysieke toegangsbeveiliging**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Identiteits-en_toegangsbeheer	#Bescherming

**Beheersmaatregel**

Beveiligde zones behoren te worden beschermd door passende toegangscontroles en toegangspunten.

**Doel**

Bewerkstelligen dat er alleen bevoegde fysieke toegang tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie plaatsvindt.

## Richtlijn

### Algemeen

Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het gebouw en/of terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) uitsluitend bevoegd personeel toegang verlenen tot locaties en gebouwen. Het proces voor het beheer van toegangsrechten tot fysieke zones behoort het toekennen, periodiek herzien, bijwerken en intrekken van autorisaties te omvatten (zie 5.18);
- b) veilig een fysiek logboek of elektronisch audittraject van alle toegang onderhouden en monitoren en alle logbestanden (zie 5.33) en gevoelige authenticatie-informatie beschermen;
- c) een proces en technische mechanismen voor het beheer van de toegang tot zones waar informatie wordt verwerkt of opgeslagen, opstellen en implementeren. Authenticatiemechanismen omvatten het gebruik van toegangspassen, biometrische authenticatie of tweefactorauthenticatie, zoals een toegangspas en een geheime pincode. Dubbele veiligheidsdeuren behoren te worden overwogen voor toegang tot gevoelige zones;
- d) een ontvangstgebied dat door personeel wordt gemonitord, opzetten of andere middelen om de fysieke toegang tot de locatie of het gebouw te beheersen;
- e) de persoonlijke bezittingen van personeel en belanghebbenden bij het binnenkomen en weggaan inspecteren en onderzoeken;  
  
OPMERKING Er kan lokale wet- en regelgeving bestaan inzake de mogelijkheid persoonlijke bezittingen te inspecteren.
- f) van al het personeel en alle belanghebbenden verlangen dat zij een bepaalde vorm van zichtbare identificatie dragen en dat zij onmiddellijk beveiligingspersoneel op de hoogte stellen als zij bezoekers zonder begeleiding en personen die geen zichtbare identificatie dragen, tegenkomen. Gemakkelijk te herkennen badges behoren te worden overwogen om vaste werknemers, leveranciers en bezoekers beter te kunnen identificeren;
- g) personeel van leveranciers alleen wanneer toegang vereist is, beperkte toegang verlenen tot beveiligde zones of informatieverwerkende faciliteiten. Deze toegang behoort gebaseerd te zijn op autorisatie en te worden gemonitord;
- h) speciale aandacht geven aan de fysieke toegangsbeveiliging van gebouwen die bedrijfsmiddelen voor meerdere organisaties bevatten;
- i) fysieke beveiligingsmaatregelen dusdanig ontwerpen dat ze kunnen worden versterkt indien het meer aannemelijk wordt dat er zich fysieke incidenten gaan voordoen;
- j) andere toegangspunten zoals nooduitgangen tegen onbevoegde toegang beveiligen;
- k) een sleutelbeheerproces opzetten om ervoor te zorgen dat de fysieke sleutels of authenticatie-informatie (bijv. slotcodes, combinatiesloten voor kantoren, ruimten en faciliteiten zoals sleutelkasten) worden beheerd en om een logboek of jaarlijkse sleutelaudit te bewerkstelligen en ervoor te zorgen dat de toegang tot fysieke sleutels of authenticatie-informatie wordt beveiligd (zie 5.17 voor verdere richtlijnen over authenticatie-informatie).

Bezoekers

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) met passende middelen de identiteit van bezoekers vaststellen;
- b) de datum en het tijdstip van binnenkomst en vertrek van bezoekers registreren;
- c) bezoekers alleen toegang verlenen voor specifieke, toegestane doeleinden en ze instructies geven over de veiligheidseisen voor de zone en over noodprocedures;
- d) toezicht houden op alle bezoekers, tenzij er een uitdrukkelijke uitzondering is verleend.

Laad- en loslocaties en inkomend materiaal

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) uitsluitend geïdentificeerd en bevoegd personeel toegang verlenen tot laad- en loslocaties van buiten het gebouw;
- b) de laad- en loslocaties dusdanig ontwerpen dat leveringen kunnen worden geladen en gelost zonder dat de leverancier onbevoegde toegang heeft tot andere zones van het gebouw;
- c) de buitendeuren van laad- en loslocaties beveiligen als deuren naar beperkt toegankelijke zones open zijn;
- d) inkomende leveringen controleren en onderzoeken op explosieven, chemicaliën of andere gevaarlijke materialen voordat ze vanaf laad- en loslocaties worden overgebracht;
- e) inkomende leveringen bij binnenkomst op de zone in overeenstemming met de procedures voor bedrijfsmiddelenbeheer registreren (zie 5.9 en 7.10);
- f) waar mogelijk, inkomende en uitgaande zendingen fysiek scheiden;
- g) inkomende leveringen inspecteren op bewijs van manipulatie onderweg. Indien vervalsing wordt ontdekt, behoort dit direct aan beveiligingspersoneel te worden gemeld.

**Overige informatie**

Geen overige informatie.

**7.3 Beveiligen van kantoren, ruimten en faciliteiten**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming

**Beheersmaatregel**

Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.

## Doel

Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie in kantoren, ruimten en faciliteiten voorkomen.

## Richtlijn

Bij het beveiligen van kantoren, ruimten en faciliteiten behoren de volgende richtlijnen in aanmerking te worden genomen:

- a) essentiële faciliteiten dusdanig positioneren dat wordt vermeden dat het publiek er toegang toe heeft;
- b) indien van toepassing, bewerkstelligen dat gebouwen onopvallend zijn en zo min mogelijk aanwijzingen geven over het gebruiksdoel ervan, zonder duidelijke tekenen binnen of buiten het gebouw die op de aanwezigheid van informatieverwerkende activiteiten duiden;
- c) faciliteiten zo configureren dat wordt voorkomen dat vertrouwelijke informatie of activiteiten van buitenaf zichtbaar en hoorbaar zijn. Voor zover van toepassing behoort elektromagnetische afscherming ook te worden overwogen;
- d) ervoor zorgen dat adreslijsten, interne telefoongidsen en online toegankelijke plattegronden met daarop de locaties van faciliteiten waar vertrouwelijke informatie wordt verwerkt, niet gemakkelijk beschikbaar zijn voor onbevoegden.

## Overige informatie

Geen overige informatie.

## 7.4 Monitoren van de fysieke beveiliging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Fysieke_beveiliging	#Bescherming #Verdediging

## Beheersmaatregel

Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.

## Doel

Onbevoegde fysieke toegang detecteren en ontmoedigen.

## Richtlijn

Fysieke terreinen en gebouwen behoren te worden bewaakt door bewakingssystemen die kunnen bestaan uit bewakers, inbraakalarmen, videobewakingssystemen zoals gesloten televisiecircuits en software voor het beheer van informatie over fysieke beveiliging die intern of door een aanbieder van bewakingsdiensten wordt beheerd.

De toegang tot gebouwen waarin kritieke systemen zijn ondergebracht, behoort voortdurend te worden gemonitord om toegang door onbevoegden of verdacht gedrag te detecteren door:

- a) videomonitoringssystemen, zoals gesloten televisiecircuits, te installeren om de toegang tot gevoelige zones binnen en buiten het terrein en de gebouwen van een organisatie te bekijken en te registreren;
- b) contact-, geluids- of bewegingsmelders die een inbraakalarm in werking stellen, volgens de desbetreffende toepasselijke normen te installeren en periodiek te testen, bijvoorbeeld:
  - 1) op elke plaats waar contact kan worden gemaakt of verbroken (zoals ramen en deuren en onder voorwerpen), contactmelders die een alarm geven wanneer een contact wordt gemaakt of verbroken, voor gebruik als paniekalarm installeren;
  - 2) bewegingsmelders op basis van infraroodtechnologie installeren die een alarm veroorzaken wanneer een voorwerp hun gezichtsveld passeert;
  - 3) sensoren installeren die gevoelig zijn voor het geluid van brekend glas en die een alarm in werking kunnen stellen dat de beveiligingsmedewerkers alarmeert.
- c) met de alarmsystemen alle buitendeuren en toegankelijke ramen af te dekken. Leegstaande ruimten behoren te allen tijde met een alarm beveiligd te zijn; er behoort ook te worden voorzien in dekking voor andere ruimten (bijv. computer- of communicatieruimten).

Het ontwerp van monitoringsystemen behoort geheim te worden gehouden omdat openbaarmaking ervan onopgemerkte inbraken mogelijk kan maken.

Om te voorkomen dat onbevoegden toegang hebben tot bewakingsinformatie, zoals videobeelden, of dat systemen op afstand worden uitgeschakeld, behoren monitoringsystemen te worden beschermd tegen toegang door onbevoegden.

Het bedieningspaneel van het alarmsysteem behoort in een met een alarm beveiligde zone te worden geplaatst en, in het geval van veiligheidsalarmen, op een plek die het voor de persoon die het alarm instelt, gemakkelijk maakt om de zone te verlaten. Het bedieningspaneel en de detectoren behoren te zijn voorzien van manipulatiebestendige mechanismen. Het systeem behoort regelmatig te worden getest om te garanderen dat het naar behoren werkt, met name als de onderdelen ervan op batterijen werken.

Elk monitoring- en opnamemechanisme behoort te worden gebruikt met inachtneming van de plaatselijke wet- en regelgeving, met inbegrip van de wetgeving inzake gegevensbescherming en de bescherming van persoonsgegevens, met name wat betreft het monitoren van werknemers en de bewaringstermijnen voor video-opnamen.

### **Overige informatie**

Geen overige informatie.

## 7.5 Beschermen tegen fysieke en omgevingsdreigingen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke beveiliging	#Bescherming

### Beheersmaatregel

Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, te worden ontworpen en geïmplementeerd.

### Doel

De gevolgen van gebeurtenissen die voortvloeien uit fysieke en omgevingsdreigingen, voorkomen of beperken.

### Richtlijn

Risicobeoordelingen om de potentiële gevolgen van fysieke en omgevingsdreigingen te identificeren, behoren voorafgaand aan kritische activiteiten op een fysieke locatie en met regelmatige tussenpozen te worden uitgevoerd. De nodige voorzorgsmaatregelen behoren te worden getroffen en veranderingen in de dreigingen behoren te worden gemonitord. Specialistisch advies behoort te worden ingewonnen over het beheren van risico's die voortvloeien uit fysieke en omgevingsdreigingen, zoals brand, overstroming, aardbeving, explosie, oproer, toxisch afval, uitstoot van milieubelastende stoffen en andere vormen van natuurrampen of door personen veroorzaakte rampen.

Bij het bepalen van de locatie en het aanleggen en bouwen van fysieke terreinen en gebouwen behoort rekening te worden gehouden met:

- de topografie ter plaatse, zoals de juiste hoogteligging, watermassa's en breuklijnen langs tektonische platen;
- dreigingen die inherent zijn aan stedelijke omgevingen, zoals locaties met een hoog risicoprofiel wat betreft het aantrekken van politieke onrust, criminele activiteiten of terrorisme.

Op basis van de resultaten van de risicobeoordelingen behoren de relevante fysieke en omgevingsdreigingen te worden geïdentificeerd en behoort te worden nagedacht over passende beheersmaatregelen in de volgende contexten, bij wijze van voorbeeld:

- brand: systemen die vroegtijdig brand kunnen detecteren, installeren en configureren zodat deze brandmeldingen doen of blussystemen in werking stellen, om brandschade aan opslagmedia en gerelateerde informatieverwerkende systemen te voorkomen. Brand behoort te worden geblust met de meest passende stof voor wat betreft de omgeving (bijv. gas in besloten ruimten);
- overstroming: systemen die overstroming in een vroeg stadium kunnen detecteren, installeren onder de vloeren van ruimten met opslagmedia of informatieverwerkende systemen. Waterpompen of gelijkwaardige middelen behoren onmiddellijk beschikbaar te zijn voor het geval er zich een overstroming voordoet;

- c) stroompieken: systemen die zowel server- als clientinformatiesystemen tegen stroompieken of soortgelijke gebeurtenissen kunnen beschermen, implementeren om de gevolgen van dergelijke gebeurtenissen tot een minimum te beperken;
- d) explosieven en wapens: steekproefsgewijze inspecties verrichten naar de aanwezigheid van explosieven of wapens bij personeel, in voertuigen of in goederen die faciliteiten binnenkomen waar gevoelige informatie wordt verwerkt.

### Overige informatie

Kluizen en andere vormen van beveiligde opslagvoorzieningen kunnen de daarin opgeslagen informatie beschermen tegen rampen zoals brand, aardbeving, overstroming of explosie.

Organisaties kunnen de concepten van criminaliteitspreventie door het ontwerp van de omgeving in overweging nemen bij het ontwerpen van de beheersmaatregelen om hun omgeving te beveiligen en dreigingen die inherent zijn aan stedelijke omgevingen, te beperken. In plaats van verkeerspalen te gebruiken, kunnen bijvoorbeeld standbeelden of waterpartijen als decoratie en als fysieke barrière fungeren.

## 7.6 Werken in beveiligde zones

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke beveiliging	#Bescherming

### Beheersmaatregel

Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.

### Doel

Informatie en andere gerelateerde bedrijfsmiddelen in beveiligde zones beschermen tegen schade en onbevoegde verstoring door personeel dat in deze zones aan het werk is.

### Richtlijn

De beveiligingsmaatregelen voor het werken in beveiligde gebieden behoren van toepassing te zijn op al het personeel en behoren alle activiteiten te bestrijken die in de beveiligde zone plaatsvinden.

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) het personeel op grond van 'need-to-know' alleen bekend maken met het bestaan van de activiteiten in een beveiligde zone.
- b) zonder toezicht werken in beveiligde gebieden vermijden, zowel om veiligheidsredenen als om de kansen op kwaadaardige activiteiten te beperken;
- c) leegstaande beveiligde gebieden fysiek afsluiten en regelmatig inspecteren;
- d) foto-, video-, audio- of andere opnameapparatuur, zoals camera's in 'endpoint devices' van gebruikers, alleen toelaten als hiervoor autorisatie is verleend;

- e) het in beveiligde gebieden meenemen en gebruiken van 'endpoint devices' van gebruikers naar behoren beheersen;
- f) noodprocedures duidelijk zichtbaar en toegankelijk ophangen.

#### Overige informatie

Geen overige informatie.

### 7.7 'Clear desk' en 'clear screen'

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke beveiliging	#Bescherming

#### Beheersmaatregel

Er behoren 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten te worden gedefinieerd en op passende wijze ten uitvoer worden gebracht.

#### Doel

De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.

#### Richtlijn

De organisatie behoort een onderwerpspecifiek beleid inzake 'clear desk' en 'clear screen' vast te stellen en aan alle relevante belanghebbenden mee te delen.

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) gevoelige of essentiële bedrijfsinformatie (bijv. op papier of op elektronische opslagmedia) in een afgesloten ruimte bewaren (idealiter in een kluis, een kast of een andere vorm van beveiligd meubilair) wanneer deze informatie niet vereist is, met name als er niemand in het kantoor is.
- b) 'endpoint devices' van gebruikers beschermen met sleutelsloten of andere beveiligingsmiddelen wanneer deze onbeheerd of niet in gebruik zijn;
- c) ervoor zorgen dat onbeheerde 'endpoint devices' van gebruikers uitgelogd zijn of beschermd zijn met een scherm- en toetsenbordvergrendeling met gebruikersauthenticatie. Alle computers en systemen behoren te worden geconfigureerd met een time-out of automatische afmeldfunctie;
- d) ervoor zorgen dat de persoon die een printopdracht geeft, de uitdraaien onmiddellijk uit de printer of het multifunctionele apparaat verwijdert. Gebruik printers met een authenticatiefunctie, waardoor alleen degene die de code invoert en naast de printer staat, de afdrucken ontvangt;
- e) documenten en verwijderbare opslagmedia met gevoelige informatie veilig opslaan en ze, wanneer ze niet meer nodig zijn, met behulp van beveiligde verwijderingsmechanismen verwijderen;

- f) regels en richtlijnen voor het configureren van pop-ups op schermen vaststellen en communiceren (bijv. de pop-ups voor nieuwe e-mail en berichten zo mogelijk uitschakelen tijdens presentaties, bij het delen van schermen of in een openbare ruimte);
- g) gevoelige of essentiële informatie van whiteboards en andere schermen of borden wissen als deze niet meer nodig is.

De organisatie behoort te beschikken over procedures voor het ontruimen van faciliteiten, waaronder een laatste doorzoeking voorafgaand aan vertrek om te garanderen dat er geen bedrijfsmiddelen van de organisatie worden achtergelaten (bijv. documenten die achter laden of meubilair zijn gevallen).

### Overige informatie

Geen overige informatie.

## 7.8 Plaatsen en beschermen van apparatuur

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming

### Beheersmaatregel

Apparatuur behoort veilig te worden geplaatst en beschermd.

### Doel

De risico's op fysieke en omgevingsdreigingen en op toegang door onbevoegden en schade beperken.

### Richtlijn

Om apparatuur te beschermen behoren de volgende richtlijnen in overweging te worden genomen:

- a) apparatuur op een dusdanige locatie plaatsen dat onnodige toegang tot werkgebieden tot het minimum wordt beperkt en toegang door onbevoegden wordt vermeden;
- b) de plaats van informatieverwerkende faciliteiten die gevoelige gegevens verwerken, zorgvuldig bepalen om het risico te beperken dat informatie tijdens het gebruik van die faciliteiten wordt bekeken door onbevoegden;
- c) beheersmaatregelen invoeren om het risico op potentiële fysieke en omgevingsdreigingen [bijv. diefstal, brand, explosie, rook, wateroverlast (of uitval van watervoorziening), stof, trilling, chemische reacties, storing in de elektriciteitsvoorziening of in communicatievoorzieningen, elektromagnetische straling en vandalisme] zo laag mogelijk te houden;
- d) richtlijnen voor eten, drinken en roken in de nabijheid van informatieverwerkende faciliteiten vaststellen;
- e) omgevingsomstandigheden zoals temperatuur en vochtigheid monitoren en controleren op omstandigheden die de werking van informatieverwerkende faciliteiten negatief kunnen beïnvloeden;

- f) bliksembeveiliging toepassen op alle gebouwen en bliksembeveiligingsfilters installeren op alle inkomende stroom- en communicatieleidingen;
- g) de toepassing van speciale beschermingsmiddelen zoals toetsenbordfolie overwegen voor apparatuur in industriële omgevingen;
- h) apparatuur die vertrouwelijke informatie verwerkt beschermen om het risico op weglekken van informatie door elektromagnetische emanatie zo laag mogelijk te houden;
- i) informatieverwerkende faciliteiten die worden beheerd door de organisatie fysiek scheiden van informatieverwerkende faciliteiten die niet door de organisatie worden beheerd.

#### Overige informatie

Geen overige informatie.

### 7.9 Beveiligen van bedrijfsmiddelen buiten het terrein

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming

#### Beheersmaatregel

Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.

#### Doel

Verlies, schade, diefstal of compromittering van bedrijfsmiddelen buiten het gebouw en/of terrein en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

#### Richtlijn

Het is nodig apparatuur die buiten het gebouw en/of terrein van de organisatie wordt gebruikt en waarop informatie wordt opgeslagen of verwerkt (bijv. een mobiel apparaat), met inbegrip van apparaten die eigendom zijn van de organisatie en apparaten die particulier eigendom zijn en gebruikt worden namens de organisatie ['bring your own device (BYOD)'], te beschermen. Het gebruik van deze apparaten behoort door het management te worden goedgekeurd.

Met de volgende richtlijnen behoort rekening te worden gehouden voor het beschermen van apparatuur die buiten het gebouw en/of terrein van de organisatie wordt gebruikt en waarop informatie wordt opgeslagen of verwerkt:

- a) apparatuur en opslagmedia die buiten het gebouw en/of terrein worden gebracht niet onbewaakt op openbare en niet-beveiligde plekken achterlaten;
- b) voorschriften van de fabrikant voor het beschermen van de apparatuur te allen tijde in acht nemen (bijv. bescherming tegen blootstelling aan sterke elektromagnetische velden, water, hitte, vocht, stof);
- c) als apparatuur buiten het gebouw en/of terrein tussen verschillende personen of belanghebbenden wordt overgedragen, een overzicht bijhouden dat de bewakingsketen voor de apparatuur

definieert, met daarin opgenomen ten minste de namen en organisaties die voor de apparatuur verantwoordelijk zijn. Informatie die niet samen met het bedrijfsmiddel hoeft te worden overgedragen, behoort op beveiligde wijze te worden gewist voorafgaand aan de overdracht;

- d) indien nodig en haalbaar, goedkeuring vereisen om apparatuur en media buiten het gebouw en/of terrein van de organisatie te brengen en een registratie van dergelijke verplaatsingen bijhouden om een audittraject te onderhouden (zie 5.14);
- e) bescherming bieden tegen het bekijken van informatie op een apparaat (bijv. een mobiele telefoon of laptop in het openbaar vervoer, en de risico's die verbonden zijn aan meekijken);
- f) locatiebepaling voor apparaten en de mogelijkheid om apparaten op afstand schoon te vegen implementeren.

Voor permanent buiten het gebouw of terrein van de organisatie geïnstalleerde apparatuur (zoals antennes of geldautomaten) kan het risico op schade, diefstal of afluisteren groter zijn. Deze risico's kunnen van locatie tot locatie sterk variëren en behoren bij het vaststellen van de meest geschikte maatregelen in overweging te worden genomen. Met de volgende richtlijnen behoort rekening te worden gehouden bij het bepalen van de locaties van deze apparatuur buiten het gebouw en/of terrein van de organisatie:

- a) fysiek monitoren van de beveiliging (zie 7.4);
- b) beschermen tegen fysieke dreigingen en dreigingen van buitenaf (zie 7.5);
- c) fysieke toegangsbeveiligingsmaatregelen en beheersmaatregelen om manipuleren tegen te gaan;
- d) logische toegangsbeveiligingsmaatregelen.

### Overige informatie

Meer informatie over andere aspecten van de bescherming van apparatuur waarop informatie wordt opgeslagen en verwerkt, en 'endpoint devices' van gebruikers is te vinden in 8.1 en 6.7.

## 7.10 Opslagmedia

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_be-drijfsmiddelen	#Bescherming

### Beheersmaatregel

Opslagmedia behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.

### Doel

Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.

## Richtlijn

### Verwijderbare opslagmedia

Voor het beheren van verwijderbare opslagmedia behoren de volgende richtlijnen te worden overwogen:

- a) onderwerpspecifiek beleid inzake het beheer van verwijderbare opslagmedia vaststellen en dit onderwerpspecifieke beleid communiceren aan iedereen die verwijderbare opslagmedia gebruikt of hanteert;
- b) indien nodig en haalbaar, goedkeuring vereisen om opslagmedia uit de organisatie te verwijderen en een registratie van dergelijke verwijderingen bijhouden om een audittraject te onderhouden;
- c) alle opslagmedia opslaan in een veilige, beveiligde omgeving overeenkomstig de desbetreffende informatieclassificatie en beschermen tegen dreigingen van buitenaf (zoals warmte, vocht, luchtvochtigheid, elektronische velden of veroudering), overeenkomstig de specificaties van de fabrikant;
- d) indien vertrouwelijkheid of integriteit van informatie belangrijke overwegingen zijn, cryptografische technieken gebruiken om informatie op verwijderbare media te beschermen;
- e) om het risico te verkleinen dat opslagmedia in kwaliteit achteruitgaan terwijl de opgeslagen informatie nog nodig is, de informatie op nieuwe opslagmedia overbrengen voordat deze onleesbaar wordt;
- f) van waardevolle informatie meerdere kopieën op afzonderlijke opslagmedia opslaan om het risico op toevallige beschadiging of verlies van informatie verder te beperken;
- g) verwijderbare opslagmedia registreren om de kans dat informatie verloren gaat, te beperken;
- h) poorten voor verwijderbare opslagmedia (bijv. SD-kaartsleuven en USB-poorten) alleen inschakelen indien er vanuit de organisatie een reden voor het gebruik ervan is;
- i) als er behoefte is om verwijderbare opslagmedia te gebruiken, de overdracht van informatie op dergelijke opslagmedia monitoren;
- j) informatie kan tijdens fysiek transport gevoelig zijn voor onbevoegde toegang, misbruik of beschadiging, bijvoorbeeld wanneer opslagmedia per post- of koeriersdienst worden verzonden.

In deze beheersmaatregel worden onder media ook papieren documenten verstaan. Pas bij het transport van fysieke opslagmedia de beveiligingsmaatregelen van 5.14 toe.

### Beveiligd hergebruiken of verwijderen

Voor het beveiligd hergebruiken of verwijderen van opslagmedia behoren procedures te worden vastgesteld om het risico zo klein mogelijk te houden dat vertrouwelijke informatie bij onbevoegde personen terechtkomt. De procedures voor het beveiligd hergebruiken of verwijderen van opslagmedia die vertrouwelijke informatie bevatten, behoren in verhouding te staan tot de gevoeligheid van die informatie. Met de volgende aspecten behoort rekening te worden gehouden:

- a) indien het nodig is opslagmedia met vertrouwelijke informatie te hergebruiken binnen de organisatie: op beveiligde wijze voorafgaand aan het hergebruik gegevens wissen of opslagmedia formatteren (zie 8.10);
- b) opslagmedia met vertrouwelijke informatie op beveiligde wijze verwijderen als ze niet meer nodig zijn (bijv. door ze te vernietigen, versnipperen of de inhoud ervan op beveiligde wijze te wissen);

- c) procedures instellen om media te identificeren waarvan het nodig kan zijn ze veilig te verwijderen;
- d) veel organisaties bieden inzamelings- en verwijderingsdiensten aan voor opslagmedia. Een geschikte externe leverancier met toereikende beheersmaatregelen en ervaring behoort met zorg te worden gekozen;
- e) de verwijdering van gevoelige zaken in een logbestand bijhouden om een audittraject te onderhouden;
- f) bij het accumuleren van opslagmedia voor verwijdering rekening houden met het aggregatie-effect, waardoor een grote hoeveelheid niet-gevoelige informatie gevoelig kan worden.

Er behoort een risicobeoordeling te worden uitgevoerd van beschadigde apparatuur die gevoelige gegevens bevat om vast te stellen of de media fysiek behoren te worden vernietigd in plaats van te worden gerepareerd of verwijderd (zie 7.14).

### Overige informatie

Als vertrouwelijke informatie op opslagmedia niet versleuteld is, behoort aanvullende fysieke bescherming van de opslagmedia te worden overwogen.

## 7.11 Nutsvoorzieningen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief	#Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Fysieke beveiliging	#Bescherming

### Beheersmaatregel

Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.

### Doel

Verlies, schade of compromittering van informatie en andere gerelateerde bedrijfsmiddelen of onderbreking van de bedrijfsvoering van de organisatie vanwege verstoring en ontregeling van ondersteunende nutsvoorzieningen voorkomen.

### Richtlijn

Organisaties zijn afhankelijk van nutsvoorzieningen (bijv. elektriciteit, telecommunicatie, water, gas, riolering, ventilatie en airconditioning) om hun informatieverwerkende faciliteiten te ondersteunen. Daarom behoort de organisatie:

- a) te bewerkstelligen dat apparatuur die de nutsvoorzieningen ondersteunt, geconfigureerd, bediend en onderhouden wordt volgens de specificaties van de desbetreffende fabrikant;
- b) te bewerkstelligen dat nutsvoorzieningen regelmatig worden onderzocht om te beoordelen of hun capaciteit toereikend is voor de groei van het bedrijf en de interactie met andere nutsvoorzieningen;
- c) te bewerkstelligen dat apparatuur die de nutsvoorzieningen ondersteunt, regelmatig wordt geïnspecteerd en getest om te garanderen dat deze naar behoren functioneert;

- d) zo nodig te voorzien in alarmmeldingen om disfunctioneren van nutsvoorzieningen te detecteren;
- e) voor zover nodig, te bewerkstelligen dat nutsvoorzieningen over meervoudige aanvoer of voeding via verschillende fysieke routes beschikken;
- f) te bewerkstelligen dat apparatuur die de nutsvoorzieningen ondersteunt en met een netwerk is verbonden, met een ander netwerk is verbonden dan de informatieverwerkende faciliteiten;
- g) te bewerkstelligen dat apparatuur die de nutsvoorzieningen ondersteunt, uitsluitend op beveiligde wijze en slechts wanneer dat nodig is met het internet wordt verbonden.

Noodverlichting en communicatiemiddelen behoren aanwezig te zijn. Nabij nooduitgangen of ruimten waar apparatuur aanwezig is, behoren noodschakelaars en knoppen te zijn waarmee stroom, water, gas of andere voorzieningen kunnen worden uitgeschakeld. Contactgegevens voor noodgevallen behoren te worden geregistreerd en bij uitval ter beschikking van het personeel te staan.

### Overige informatie

Redundantie voor netwerkverbinding kan worden verkregen via meerdere routes vanaf meer dan één aanbieder.

## 7.12 Beveiligen van bekabeling

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Beschikbaarheid	#Beschermen	#Fysieke beveiliging	#Bescherming

### Beheersmaatregel

Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.

### Doel

Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie in verband met voedings- en communicatiekabels voorkomen.

### Richtlijn

Met de volgende richtlijnen voor beveiligen van bekabeling behoort rekening te worden gehouden:

- a) voedings- en telecommunicatieleidingen naar informatieverwerkende faciliteiten: waar mogelijk onder de grond of op een andere passende wijze beschermd, zoals met een vloerkabelgoot en een nutspaal; ondergrondse kabels: beschermd tegen onopzettelijk doorsteken (bijv. met een mantel of detectiesignalen);
- b) voedingskabels van communicatiekabels scheiden om interferentie te voorkomen;

c) voor gevoelige of essentiële systemen kunnen de volgende aanvullende beheersmaatregelen worden overwogen:

- 1) de installatie van gewapende kabelgoten en afgesloten kamers of dozen en alarmen bij inspectie- en afsluitpunten;
- 2) het gebruik van elektromagnetische afscherming ter bescherming van de kabels;
- 3) periodieke technische schoonmaakbeurten en fysieke controles om aansluiting van niet-goedgekeurde apparaten op de kabels op te sporen;
- 4) beveiligde toegang tot schakelpanelen en kabelruimten (bijv. met mechanische sleutels of pincodes);
- 5) het gebruik van glasvezelkabels;

d) kabels aan elk uiteinde voorzien van labels met voldoende informatie over de bron en de bestemming om fysieke identificatie en inspectie van de kabel mogelijk te maken.

Specialistisch advies behoort te worden ingewonnen over het beheeren van risico's die voortvloeien uit incidenten met of disfunctioneren van kabels.

### Overige informatie

Soms worden voedings- en telecommunicatiekabels door meer dan één organisatie op één locatie gedeeld.

## 7.13 Onderhoud van apparatuur

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke beveiliging #Beheer van bedrijfsmiddelen	#Bescherming #Veerkracht

### Beheersmaatregel

Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.

### Doel

Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie door gebrekkig onderhoud voorkomen.

### Richtlijn

De volgende richtlijnen voor onderhoud van apparatuur behoren in aanmerking te worden genomen:

- a) apparatuur in overeenstemming met de door de leverancier aanbevolen frequentie voor servicebeurten en voorschriften onderhouden;
- b) het door de organisatie implementeren en monitoren van een onderhoudsprogramma;

- c) alleen bevoegd onderhoudspersoneel reparaties en onderhoud aan apparatuur laten uitvoeren;
- d) registraties bijhouden van alle vermeende en daadwerkelijke fouten, en van al het preventieve en corrigerende onderhoud;
- e) passende beheersmaatregelen implementeren wanneer onderhoud van apparatuur is gepland, rekening houdend met of dit onderhoud wordt uitgevoerd door personeel ter plaatse of door extern personeel, waarbij het onderhoudspersoneel gehouden is aan een passende geheimhoudingsovereenkomst;
- f) toezicht houden op onderhoudspersoneel tijdens het uitvoeren van onderhoud ter plaatse;
- g) toegang voor onderhoud op afstand op basis van autorisatie toestaan en beveiligen;
- h) beveiligingsmaatregelen voor bedrijfsmiddelen buiten het gebouw en/of terrein (zie 7.9) toepassen indien apparatuur die informatie bevat, voor onderhoud buiten het gebouw en/of terrein wordt gebracht;
- i) voldoen aan alle door de verzekering opgelegde onderhoudseisen;
- j) voordat apparatuur na onderhoud weer in bedrijf wordt gesteld, een inspectie uitvoeren om te waarborgen dat er niet is geknoeid met de apparatuur en dat deze naar behoren functioneert;
- k) maatregelen toepassen voor het veilig verwijderen of hergebruiken van apparatuur (zie 7.14) indien wordt vastgesteld dat het nodig is apparatuur te verwijderen.

### Overige informatie

Apparatuur omvat technische componenten van informatieverwerkende faciliteiten, UPS, batterijen en accu's, stroomgeneratoren, wisselstroomgeneratoren en vermogensomzetters, fysieke inbraakdetectiesystemen en -alarmen, rookmelders, brandblussers, airconditioning en liften.

## 7.14 Veilig verwijderen of hergebruiken van apparatuur

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming

### Beheersmaatregel

Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.

### Doel

Het lekken van informatie via af te voeren of te hergebruiken apparatuur voorkomen.

### Richtlijn

Voorafgaand aan verwijdering of hergebruik behoort te worden gecontroleerd of apparatuur opslagmedia bevat.

Opslagmedia die vertrouwelijke of door auteursrecht beschermde informatie bevatten, behoren, in plaats van met de standaard 'delete'-functie te worden gewist, fysiek te worden vernietigd of de informatie behoort te worden vernietigd, verwijderd of overschreven met gebruikmaking van technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen. Zie 7.10 voor gedetailleerde richtlijnen over het veilig verwijderen van opslagmedia en 8.10 voor richtlijnen over het wissen van informatie.

Labels en markeringen waarmee de organisatie wordt geïdentificeerd of die de classificatie, de eigenaar, het systeem of het netwerk aangeven, behoren voorafgaand aan het verwijderen, waaronder begrepen doorverkopen of aan een goed doel schenken, van de opslagmedia te worden verwijderd.

De organisatie behoort te overwegen beveiligingsbeheersmaatregelen zoals toegangsbeveiligingsmaatregelen of bewakingsapparatuur aan het einde van de huurovereenkomst of bij verhuizing uit het gebouw te verwijderen. Dit is afhankelijk van factoren zoals:

- a) de huurovereenkomst om de faciliteit in de oorspronkelijke staat terug te brengen;
- b) het minimaliseren van het risico dat systemen met gevoelige informatie erop worden achtergelaten voor de volgende huurder (bijv. lijsten van welke gebruikers toegang hebben gehad, video- of beeldbestanden);
- c) de mogelijkheid om de beheersmaatregelen in de volgende faciliteit opnieuw te gebruiken.

### **Overige informatie**

Voor beschadigde apparatuur die opslagmedia bevat, kan een risicobeoordeling nodig zijn om vast te stellen of het desbetreffende onderdeel van de apparatuur fysiek behoort te worden vernietigd in plaats van te worden gerepareerd of verwijderd. Informatie kan worden gecompromitteerd door onzorgvuldige verwijdering of door hergebruik van apparatuur.

Naast zorgvuldig wissen van de schijf vermindert codering van de volledige schijf het risico op openbaarmaking van vertrouwelijke informatie als de apparatuur van de hand wordt gedaan of opnieuw wordt ingezet, mits:

- a) de codering voldoende sterk is en de gehele schijf omvat (met inbegrip van 'slack space', swap-bestanden);
- b) de cryptografische sleutels lang genoeg zijn om met grove middelen uitgevoerde aanvallen te weerstaan;
- c) de cryptografische sleutels vertrouwelijk worden behandeld (bijv. nooit op dezelfde schijf worden bewaard).

Zie voor verder advies over cryptografie 8.24.

De technieken voor het op beveiligde wijze overschrijven van opslagmedia verschillen afhankelijk van de opslagmediatechnologie en het classificatieniveau van de informatie op de opslagmedia. Overschrijvingsinstrumenten behoren te worden beoordeeld om er zeker van te zijn dat ze geschikt zijn voor de technologie van het opslagmedium.

Zie ISO/IEC 27040 voor nadere informatie over methoden om opslagmedia leeg te maken.

## 8 Technologische beheersmaatregelen

### 8.1 'User endpoint devices'

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfs-middelen #Informatiebescherming	#Bescherming

#### Beheersmaatregel

Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.

#### Doel

Informatie beschermen tegen de risico's als gevolg van het gebruik van 'user endpoint devices'.

#### Richtlijn

##### Algemeen

De organisatie behoort onderwerpspecifiek beleid vast te stellen inzake beveiligde configuratie en beveiligd gebruik van 'user endpoint devices'. Het onderwerpspecifieke beleid behoort aan al het relevante personeel te worden gecommuniceerd en het volgende in aanmerking te nemen:

- het soort informatie en het classificatieniveau waarmee de 'user endpoint devices' kunnen omgaan of dat ze kunnen verwerken, opslaan of ondersteunen;
- registratie van 'user endpoint devices';
- eisen voor fysieke bescherming;
- beperking van de installatie van software (bijv. op afstand beheerst door systeembeheerders);
- eisen voor software (met inbegrip van softwareversies) van de 'user endpoint devices' en voor het toepassen van updates (bijv. actief automatisch updaten);
- regels voor de verbinding met informatiediensten, publieke netwerken of andere netwerken buiten het gebouw of terrein (bijv. het gebruik van een persoonlijke firewall vereisen);
- toegangsbeveiliging;
- versleuteling van opslagapparaten;
- bescherming tegen malware;
- het op afstand onbruikbaar maken, wissen, uitsluiten;
- back-ups;
- het gebruik van internetdiensten en -toepassingen;

- m) analyse van het gedrag van de eindgebruiker (zie 8.16);
- n) het gebruik van verwijderbare apparaten, met inbegrip van verwijderbare geheugenapparaten, en de mogelijkheid om fysieke poorten (bijv. USB-poorten) uit te schakelen;
- o) het gebruik van partitioneringsmogelijkheden, indien ondersteund door de 'user endpoint devices', waarmee de informatie en andere gerelateerde bedrijfsmiddelen (bijv. software) van de organisatie veilig kunnen worden gesegmenteerd van andere informatie en andere gerelateerde bedrijfsmiddelen op het apparaat.

Er behoort te worden overwogen of bepaalde informatie zo gevoelig is dat er via 'user endpoint devices' slechts toegang toe kan worden gemaakt, maar de informatie niet op die apparaten mag worden opgeslagen. In dergelijke gevallen kunnen aanvullende technische beveiligingen op het apparaat vereist zijn. Bijvoorbeeld, ervoor zorgen dat het downloaden van bestanden voor offline werken is uitgeschakeld en dat lokale opslag zoals SD-kaarten is uitgeschakeld.

De aanbevelingen met betrekking tot deze beheersmaatregel behoren voor zover mogelijk te worden afgedwongen via configuratiebeheer (zie 8.9) of geautomatiseerde instrumenten.

#### Gebruikersverantwoordelijkheid

Alle gebruikers behoren op de hoogte te worden gebracht van de beveiligingseisen en de procedures voor het beschermen van 'user endpoint devices' en van hun verantwoordelijkheden voor het implementeren van dergelijke beschermingsmaatregelen. Gebruikers behoren het advies te krijgen:

- a) uit te loggen uit actieve sessies en diensten afsluiten die niet langer nodig zijn;
- b) 'user endpoint devices' terwijl deze niet in gebruik zijn met een fysieke beheersmaatregel (bijv. een sleutelslot of speciale sloten) en logische beheersmaatregel (bijv. toegang met wachtwoorden) te beschermen tegen gebruik door onbevoegden; geen apparaten met belangrijke, gevoelige of essentiële bedrijfsinformatie onbewaakt achter te laten;
- c) apparaten extra zorgvuldig te gebruiken in openbare ruimten, open kantoren, vergaderruimten en andere onbeschermd gebieden (bijv. bij voorkeur geen vertrouwelijke informatie lezen als mensen van achteren kunnen meelezen, schermfilters gebruiken met het oog op privacy);
- d) 'user endpoint devices' fysiek te beveiligen tegen diefstal (bijv. in een auto of andere vervoermiddelen, in hotelkamers, conferentie- en ontmoetingscentra).

Er behoort een speciale procedure te worden vastgesteld voor diefstal of verlies van 'user endpoint devices' waarin rekening is gehouden met wettelijke, statutaire, regelgevende, contractuele (met inbegrip van verzekerings-) en andere veiligheidseisen die in de organisatie gelden.

#### Het gebruik van persoonlijke apparaten

Indien de organisatie het gebruik van persoonlijke apparaten toestaat (dit wordt soms aangeduid als BYOD), behoort, in aanvulling op de richtlijnen die in deze beheersmaatregel worden gegeven, ook het volgende te worden overwogen:

- a) scheiding van persoonlijk en zakelijk gebruik van de apparatuur, met inbegrip van het gebruik van software ter ondersteuning van een dergelijke scheiding en ter bescherming van bedrijfsgegevens op een privéapparaat;
- b) verschaffen van toegang tot bedrijfsinformatie alleen nadat gebruikers hun verplichtingen hebben bevestigd (fysieke beveiliging, updaten van software enz.), afstand doen van eigendom van bedrijfsgegevens, toestaan dat de organisatie op afstand gegevens wist in geval van diefstal of

verlies van het apparaat of indien zij niet langer bevoegd zijn. In dergelijke gevallen behoort rekening te worden gehouden met wetgeving inzake de bescherming van persoonsgegevens;

- c) onderwerpspecifieke beleidsregels en procedures ter voorkoming van geschillen over rechten van intellectuele eigendom die is ontwikkeld op privéapparatuur;
- d) toegang tot privéapparatuur (om de veiligheid van het apparaat vast te stellen of tijdens een onderzoek), wat wetgeving kan verhinderen;
- e) softwarelicentiecontracten waardoor de organisatie aansprakelijk kan worden gesteld voor de licenties van clientsoftware op 'user endpoint devices' die privébezit zijn van personeel of van externe gebruikers.

#### Draadloze verbindingen

De organisatie behoort procedures vast te stellen voor:

- a) het configureren van draadloze verbindingen op apparaten (bijv. kwetsbare protocollen uitschakelen);
- b) het gebruik van draadloze of bedrade verbindingen met passende bandbreedte overeenkomstig relevante onderwerpspecifieke beleidsregels (bijv. omdat back-ups of software-updates nodig zijn).

#### **Overige informatie**

Beheersmaatregelen voor het beschermen van informatie op 'user endpoint devices' zijn afhankelijk van of het 'endpoint device' van de gebruiker alleen binnen het beveiligde gebouw en terrein en de beveiligde netwerkverbindingen van de organisatie wordt gebruikt of dat het wordt blootgesteld aan meer fysieke en netwerkgerelateerde dreigingen buiten de organisatie.

De draadloze verbindingen van 'user endpoint devices' zijn gelijksoortig aan andere vormen van netwerkverbindingen, maar hebben belangrijke verschillen waar rekening mee behoort te worden gehouden bij het identificeren van beheersmaatregelen. Er kan met name soms iets fout gaan bij het maken van back-ups van informatie die op 'user endpoint devices' is opgeslagen indien de bandbreedte van het netwerk beperkt is of 'user endpoint devices' niet zijn aangesloten op de tijden waarop de back-ups zijn gepland.

Voor bepaalde USB-poorten, zoals USB-C, is het niet mogelijk de USB-poort uit te schakelen, omdat deze voor andere doelen (bijv. voeding of als uitgang voor een weergavescherm) in gebruik is.

## **8.2 Speciale toegangsrechten**

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer	#Bescherming

#### **Beheersmaatregel**

Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd.

**Doel**

Bewerkstelligen dat alleen bevoegde gebruikers, softwarecomponenten en diensten speciale toegangsrechten krijgen.

**Richtlijn**

Het toewijzen van speciale toegangsrechten behoort te worden beheerst door een autorisatieprocedure die in overeenstemming is met het relevante onderwerpspecifieke beleid inzake toegangsbeveiliging (zie 5.15). Het volgende behoort te worden overwogen:

- a) het identificeren van gebruikers die speciale toegangsrechten nodig hebben voor elk systeem of proces (bijv. besturingssystemen, databasebeheersystemen en toepassingen);
- b) het toekennen van speciale toegangsrechten aan gebruikers waar nodig en van gebeurtenis tot gebeurtenis, overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging (zie 5.15) (d.w.z. alleen aan personen met de nodige competentie om de activiteiten uit te voeren die speciale toegang vereisen en op basis van de minimumeisen voor hun functionele rol);
- c) een autorisatieproces in stand houden (d.w.z. bepalen wie speciale toegangsrechten kan goedkeuren, of speciale toegangsrechten pas toekennen als het autorisatieproces is afgerond) en een registratie van alle toegewezen rechten bijhouden;
- d) het definiëren en implementeren van eisen voor het vervallen van speciale toegangsrechten;
- e) het treffen van maatregelen om te bewerkstelligen dat de gebruikers zich bewust zijn van hun speciale toegangsrechten en wanneer zij zich in de speciale toegangsmodus bevinden. Mogelijke maatregelen zijn onder andere het gebruik van specifieke gebruikersidentiteiten, gebruikersinterface-instellingen of zelfs specifieke apparatuur;
- f) de authenticatie-eisen voor speciale toegangsrechten kunnen hoger zijn dan de eisen voor normale toegangsrechten. Herauthenticeren of het aanscherpen van het authenticeren kan nodig zijn voordat er werk met speciale toegangsrechten kan worden uitgevoerd;
- g) het regelmatig en na elke organisatiewijziging beoordelen van de gebruikers die met speciale toegangsrechten werken om te verifiëren of ze op grond van hun taken, rollen, verantwoordelijkheden en competentie nog altijd in aanmerking komen voor het werken met speciale toegangsrechten (zie 5.18);
- h) het vaststellen van specifieke regels om het gebruik van generieke gebruikersidentificaties voor beheer (zoals 'root') te vermijden, afhankelijk van de configuratiemogelijkheden van de systemen. Het beheren en beschermen van de authenticatie-informatie van dergelijke identiteiten (zie 5.17);
- i) tijdelijke speciale toegangsrechten slechts verlenen voor het tijdsvenster dat nodig is om goedgekeurde veranderingen of activiteiten te implementeren (bijv. voor onderhoudsactiviteiten of bepaalde essentiële veranderingen), in plaats van speciale toegangsrechten permanent te verlenen. Dit wordt vaak aangeduid als een procedure voor noodtoegang, en wordt vaak geautomatiseerd door technologieën voor het beheer van speciale toegangsrechten;
- j) het registreren van alle speciale toegang tot systemen voor auditdoeleinden;

- k) identiteiten met speciale toegangsrechten niet met meerdere personen delen of aan meerdere personen koppelen, maar aan elke persoon een afzonderlijke identiteit toekennen waarmee specifieke speciale toegangsrechten kunnen worden toegekend. Identiteiten kunnen worden gegroepeerd (bijv. door een beheerdersgroep te definiëren) om het beheer van speciale toegangsrechten te vereenvoudigen;
- l) het gebruik van identiteiten met speciale toegangsrechten beperken tot het uitvoeren van beheerfuncties en deze identiteiten niet gebruiken voor de dagelijkse algemene taken [d.w.z. e-mail bekijken, toegang tot internet (gebruikers behoren voor deze activiteiten een afzonderlijke normale netwerkidentiteit te hebben)].

### Overige informatie

Speciale toegangsrechten zijn toegangsrechten die aan een identiteit, rol of proces worden verleend om activiteiten te kunnen uitvoeren die gewone gebruikers of processen niet kunnen uitvoeren. Systeembeheerdersrollen vereisen meestal speciale toegangsrechten.

Ongepast gebruik van speciale systeembeheerdersrechten (elke functie of faciliteit van een informatiesysteem die de gebruiker in staat stelt systeem- of toepassingsbeheersmaatregelen op te heffen) is een factor die in grote mate bijdraagt aan storingen van of inbreuken op het systeem.

Meer informatie over toegangsbeheer en het beveiligde beheer van de toegang tot informatie en informatie- en communicatietechnologiemiddelen is te vinden in ISO/IEC 29146.

## 8.3 Beperking toegang tot informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer	#Bescherming

### Beheersmaatregel

De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.

### Doel

Uitsluitend bevoegde toegang bewerkstelligen en onbevoegde toegang tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.

### Richtlijn

De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig de vastgestelde onderwerpspecifieke beleidsregels. De volgende aspecten behoren in aanmerking te worden genomen om de eisen voor toegangsbeperking te ondersteunen:

- a) toegang tot gevoelige informatie niet anoniem of aan onbekende gebruikersidentiteiten toestaan. Openbare of anonieme toegang behoort uitsluitend te worden verleend tot opslaglocaties waar zich geen gevoelige informatie bevindt;
- b) voorzien in configuratiemechanismen voor toegangsbeveiliging van informatie in systemen, toepassingen en diensten;

- c) beheersen welke gegevens voor een bepaalde gebruiker toegankelijk zijn;
- d) beheersen welke identiteiten of groep identiteiten bepaalde toegangsrechten hebben, zoals lezen, schrijven, wissen en uitvoeren;
- e) zorgen voor fysieke of logische toegangsbeveiligingsmaatregelen voor het isoleren van gevoelige toepassingen, toepassingsgegevens of systemen;

Verder behoren dynamische technieken en processen voor het beschermen van gevoelige informatie die van hoge waarde is voor de organisatie, in overweging te worden genomen als de organisatie:

- a) granulaire beveiliging nodig heeft met betrekking tot wie, gedurende welke periode en volgens welke wijze toegang kan krijgen tot dergelijke informatie;
- b) zulke informatie wil delen met mensen buiten de organisatie en de controle wil behouden over wie er toegang toe heeft;
- c) het gebruik en de verspreiding van die informatie dynamisch en in real time wil beheren;
- d) dergelijke informatie wil beschermen tegen ongeautoriseerde wijzigingen, kopiëren en verspreiding (met inbegrip van afdrukken);
- e) het gebruik van de informatie wil monitoren;
- f) wijzigingen aan deze informatie wil registreren voor het geval onderzoek in de toekomst vereist is.

Technieken voor het beheer van dynamische toegang behoren informatie gedurende de hele levenscyclus ervan te beschermen (d.w.z. het aanmaken, verwerken, opslaan, overdragen en verwijderen), met inbegrip van:

- a) het vaststellen van regels voor het beheer van dynamische toegang op basis van specifieke usecases, waarbij het volgende in overweging wordt genomen:
  - 1) toegangsrechten verlenen op basis van identiteit, apparaat, locatie of toepassing;
  - 2) het classificatieschema inzetten om vast te stellen welke informatie met technieken voor het beheer van dynamische toegang moet worden beschermd;
- b) operationele, monitoring- en meldingsprocessen opstellen en ondersteunende technische infrastructuur inrichten.

Systemen voor het beheer van dynamische toegang behoren informatie te beschermen door:

- a) authenticatie, passende toegangsgegevens of een certificaat te vereisen voor toegang tot informatie;
- b) de toegang te beperken, bijvoorbeeld tot een bepaald tijdsbestek (bijvoorbeeld na een bepaalde datum of tot een bepaalde datum);
- c) versleuteling te gebruiken om informatie te beschermen;
- d) de afdrukrechten voor de informatie te definiëren;
- e) te registreren wie zich toegang verschaft tot de informatie en hoe de informatie wordt gebruikt;
- f) waarschuwingen te geven indien er pogingen om de informatie te misbruiken worden waargenomen.

## Overige informatie

Indien traditionele toegangscontroles niet kunnen worden afgedwongen, kunnen technieken voor het beheer van dynamische toegang en andere technieken voor dynamische informatiebeveiliging de bescherming van informatie ondersteunen, zelfs wanneer gegevens buiten de organisatie van herkomst worden gedeeld. Dit kan worden toegepast op documenten, e-mails of andere bestanden met informatie, om te beperken wie er toegang kan krijgen tot de inhoud en hoe men deze kan krijgen. Dit kan op granulair niveau zijn en worden aangepast gedurende de levenscyclus van de informatie.

Technieken voor het beheer van dynamische toegang zijn geen vervangers van klassiek toegangsbeheer [bijv. het gebruik van lijsten voor toegangsbeheer (ACL's)], maar ze kunnen meer factoren toevoegen voor conditionaliteit, realtime-evaluatie, just-in-timedatabeperking en andere verbeteringen die nuttig kunnen zijn voor de meest gevoelige informatie. Dit biedt een manier om toegang buiten de omgeving van de organisatie te beveiligen. Incidentrespons kan worden ondersteund door technieken voor het beheer van dynamische toegang aangezien rechten te allen tijde kunnen worden gewijzigd of ingetrokken.

Aanvullende informatie over een kader voor toegangsbeheer wordt gegeven in ISO/IEC 29146.

## 8.4 Toegangsbeveiliging op broncode

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer #Toepassingsbeveiliging #Veilige_configuratie	#Bescherming

### Beheersmaatregel

Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd.

### Doel

Voorkomen dat er ongeoorloofde functionaliteit wordt geïntroduceerd, vermijden dat onbedoelde of kwaadwillige wijzigingen plaatsvinden en de vertrouwelijkheid behouden van waardevol intellectueel eigendom.

### Richtlijn

Toegang tot broncode en gerelateerde zaken (zoals ontwerpen, specificaties, verificatieplannen en validatieplannen) en ontwikkelinstrumenten (bijv. compilers, builders, integratie-instrumenten, testplatformen en -omgevingen) behoort streng te worden beheerst.

Met betrekking tot broncode kan dit worden bereikt door de code gecontroleerd centraal op te slaan, bij voorkeur in een broncodebeheersysteem.

Lees- en schrijftoegang tot broncode kan verschillen op basis van de rol van het personeel. Zo kan leestoegang tot broncode binnen de organisatie breed worden aangeboden, maar schrijftoegang tot broncode worden voorbehouden aan speciaal personeel of aangewezen eigenaren. Indien codecomponenten door verschillende ontwikkelaars binnen een organisatie worden hergebruikt, behoort leestoegang tot een gecentraliseerde broncodebibliotheek te worden geïmplementeerd.

Bovendien kan, indien binnen een organisatie open broncode of codecomponenten van derden worden gebruikt, de leestoegang tot dergelijke externe broncodebibliotheken ook breed worden aangeboden. De schrijftoegang behoort echter nog steeds te worden beperkt.

De volgende richtlijnen behoren te worden overwogen om de toegang tot broncodebibliotheken te beheersen en zo de kans op corruptie van computerprogramma's te verkleinen:

- a) de toegang tot programmabroncode en de programmabronbibliotheken volgens vastgestelde procedures beheren;
- b) lees- en schrijftoegang tot broncode op basis van de bedrijfsbehoeften verlenen, dusdanig beheerd dat de risico's op wijziging of misbruik worden opgepakt en volgens vastgestelde procedures;
- c) de procedures voor wijzigingsbeheer (zie 8.32) toepassen op het bijwerken van broncode en gerelateerde zaken en het verlenen van toegang tot broncode en dit pas uitvoeren nadat de passende autorisatie is ontvangen;
- d) ontwikkelaars geen rechtstreekse toegang tot de broncodebibliotheek verlenen, maar via ontwikkelinstrumenten die activiteiten en autorisaties met betrekking tot de broncode beheersen;
- e) lijsten van programma's in een beveiligde omgeving bewaren waar lees- en schrijftoegang op passende wijze behoort te worden beheerd en toegewezen;
- f) een auditlogbestand bijhouden van alle toegangsinstanties en van alle wijzigingen aan de broncode.

Indien het de bedoeling is dat de programmabroncode wordt gepubliceerd, behoren aanvullende beheersmaatregelen die de integriteit ervan waarborgen (bijv. een digitale handtekening), te worden overwogen.

### Overige informatie

Indien de toegang tot broncode niet naar behoren wordt beveiligd, kunnen onbevoegden broncode aanpassen of bepaalde gegevens in de ontwikkelomgeving (bijv. kopieën van productiegegevens, configuratiedetails) opvragen.

## 8.5 Beveiligde authenticatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits- _en_toegangsbeheer	#Bescherming

### Beheersmaatregel

Er behoren beveiligde authenticatietechnologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.

### Doel

Bewerkstelligen dat een gebruiker of een entiteit veilig wordt geauthenticeerd wanneer toegang tot systemen, toepassingen en diensten wordt verleend.

## **Richtlijn**

Om de geclaimde identiteit van een gebruiker, software, berichten en andere entiteiten te bewijzen behoort een passende authenticatietechniek te worden gekozen.

De sterkte van authenticatie behoort passend te zijn voor de classificatie van de informatie waartoe toegang wordt verleend. Ingeval krachtige verificatie en authenticatie van de identiteit is vereist, behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals digitale certificaten, chipkaarten, tokens of biometrische middelen.

Authenticatie-informatie behoort vergezeld te gaan van aanvullende authenticatiefactoren voor toegang tot essentiële informatiesystemen (ook bekend als multifactorauthenticatie). Het gebruik van een combinatie van meerdere authenticatiefactoren, zoals wat je weet, wat je hebt en wat je bent, beperkt de mogelijkheid van onbevoegde toegang. Multifactorauthenticatie kan worden gecombineerd met andere technieken die aanvullende factoren onder specifieke omstandigheden vereisen, op basis van vooraf gedefinieerde regels en patronen, zoals toegang vanaf een ongebruikelijke locatie, een ongebruikelijk apparaat of op een ongebruikelijk tijdstip.

Biometrische authenticatie-informatie behoort ongeldig te worden gemaakt als deze ooit wordt gecompromitteerd. Het is mogelijk dat biometrische authenticatie niet beschikbaar is, afhankelijk van de gebruiksomstandigheden (bijv. vocht of veroudering). Om hierop voorbereid te zijn, behoort biometrische authenticatie van ten minste één alternatieve authenticatietechniek vergezeld te gaan.

De procedure om in een systeem in te loggen, behoort zo te worden ontworpen dat het risico op onbevoegde toegang zo klein mogelijk wordt gemaakt. Er behoren inlogprocedures en -technologieën te worden geïmplementeerd waarbij het volgende in overweging wordt genomen:

- a) gevoelige systeem- of toepassingsinformatie pas tonen nadat het inlogproces op geslaagde wijze is afgerond om zo te vermijden dat een onbevoegde onnodig wordt geholpen;
- b) een algemene waarschuwing tonen dat het systeem of de toepassing of dienst alleen toegankelijk is voor bevoegde gebruikers;
- c) geen hulpmeldingen geven tijdens de aanmeldprocedure die een onbevoegde gebruiker zouden helpen (bijv. als er zich een fout voordoet, behoort het systeem niet aan te geven welk gedeelte van de gegevens correct of niet correct is);
- d) de inloginformatie pas na invoer van alle gegevens valideren;
- e) bescherming bieden tegen bruto geweld bij aanmeldpogingen met gebruikersnamen en wachtwoorden (bijv. door gebruik te maken van CAPTCHA, te eisen dat een wachtwoord opnieuw wordt ingesteld na een vooraf bepaald aantal mislukte pogingen of de gebruiker na een maximumaantal fouten te blokkeren);
- f) niet-succesvolle en succesvolle pogingen registreren;
- g) een beveiligingsgebeurtenis genereren wanneer een potentiële poging tot of succesvolle inbreuk op aanmeldbeheersmaatregelen wordt gedetecteerd (bijv. een waarschuwing naar de gebruiker en de systeembeheerders van de organisatie sturen wanneer een bepaald aantal verkeerde wachtwoordpogingen is bereikt);

- h) de volgende informatie op een apart kanaal tonen of verzenden nadat het inloggen met succes is voltooid:
- 1) datum en tijdstip waarop de vorige keer met succes is ingelogd;
  - 2) details van niet-succesvolle pogingen om in te loggen sinds de vorige succesvolle poging om in te loggen;
- i) een wachtwoord terwijl het wordt ingevoerd niet als leesbare tekst tonen; in bepaalde gevallen kan het nodig zijn deze functionaliteit uit te schakelen om de gebruiker te laten inloggen (bijv. vanwege toegankelijkheidsredenen of om te vermijden dat gebruikers worden geblokkeerd doordat ze meermaals fouten hebben gemaakt);
- j) wachtwoorden niet als onversleutelde tekst via een netwerk verzenden om zo te voorkomen dat zij door een snifferprogramma op het netwerk worden onderschept;
- k) inactieve sessies na een bepaalde tijd van inactiviteit beëindigen, vooral op locaties met een hoog risico, zoals openbare of externe locaties die buiten het beveiligingsbeheer van de organisatie vallen, of op 'endpoint devices' van gebruikers;
- l) de verbindingduur beperken om extra beveiliging te bieden voor toepassingen met een hoog risico en de mogelijkheden voor onbevoegde toegang te verkleinen.

### Overige informatie

Aanvullende informatie over de borging van de authenticatie van entiteiten is te vinden in ISO/IEC 29115.

## 8.6 Capaciteitsbeheer

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief	#Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Detecteren	#Continuïteit	#Governance_en_ Ecosysteem #Bescherming

### Beheersmaatregel

Het gebruik van middelen behoort te worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.

### Doel

De vereiste capaciteit van informatieverwerkende faciliteiten, personeel, kantoren en andere faciliteiten waarborgen.

### Richtlijn

Capaciteitseisen voor informatieverwerkende faciliteiten, personeel, kantoren en andere faciliteiten behoren te worden gedefinieerd, rekening houdend met het belang van de betrokken systemen en processen voor de organisatie.

Het systeem behoort te worden afgestemd en gemonitord om de beschikbaarheid en doelmatigheid van systemen te waarborgen en zo nodig te verbeteren.

De organisatie behoort stresstests van systemen en diensten uit te voeren om te bevestigen dat er voldoende systeemcapaciteit beschikbaar is om aan eisen voor piekprestaties te voldoen.

Om problemen vroegtijdig vast te stellen behoren detectiemaatregelen te worden genomen.

Prognoses voor toekomstige capaciteitseisen behoren rekening te houden met nieuwe bedrijfs- en systeemeisen en de huidige en verwachte trends in de informatieverwerkende capaciteiten van de organisatie.

Er behoort met name aandacht te worden besteed aan middelen met lange verwervingsdoorlooptijden of hoge kosten. Daarom behoren managers en de eigenaren van een dienst of product het gebruik van belangrijke systeemmiddelen te monitoren.

Beheerders behoren deze capaciteitsinformatie te gebruiken voor het signaleren en vermijden van potentiële beperkingen aan middelen en afhankelijkheid van belangrijk personeel, wat een dreiging kan vormen voor de systeembeveiliging en diensten, en behoren passende actie te plannen.

Voldoende capaciteit kan worden verkregen door de capaciteit te verhogen of door de vraag te verlagen. Om de capaciteit te verhogen behoort het volgende in overweging te worden genomen:

- a) nieuw personeel aantrekken;
- b) nieuwe faciliteiten of ruimte verkrijgen;
- c) krachtigere verwerkingssystemen, geheugen en opslag verkrijgen;
- d) gebruikmaken van cloudcomputing, hetgeen inherente kenmerken heeft die rechtstreeks capaciteitskwesties oppakken. Cloudcomputing heeft elasticiteit en schaalbaarheid waardoor snelle uitbreiding en inkrimping van middelen op vraag beschikbaar is voor specifieke toepassingen en diensten.

Om het beslag op de middelen van de organisatie te verminderen, behoort het volgende te worden overwogen:

- a) verouderde gegevens verwijderen (schijfruimte);
- b) registraties op papier waarvan de bewaartermijn is verstreken, verwijderen (schapruimte vrijmaken);
- c) toepassingen, systemen, databases of omgevingen buiten gebruik stellen;
- d) batchprocessen en -schema's optimaliseren;
- e) toepassingscode of databasevragen optimaliseren;
- f) de bandbreedte voor diensten die veel energie verbruiken, weigeren of beperken als deze niet van overwegend belang zijn (bijv. videostreaming).

Voor systemen die belangrijk zijn voor de missie, behoort voor de capaciteit een gedocumenteerd beheersplan te worden overwogen.

### **Overige informatie**

Meer informatie over de elasticiteit en schaalbaarheid van cloudcomputing is te vinden in ISO/IEC TS 23167.

## 8.7 Bescherming tegen malware

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem- _en_netwerk- beveiliging #Informatiebe- scherming	#Bescherming #Verdediging

### Beheersmaatregel

Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn

### Doel

Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.

### Richtlijn

Bescherming tegen malware behoort te zijn gebaseerd op software die malware detecteert en op herstelsoftware, bewustwording ten aanzien van informatiebeveiliging, passende beheersmaatregelen met betrekking tot systeemtoegang en wijzigingsbeheer. Het gebruik van software voor het detecteren en herstellen van malware op zich is meestal niet afdoende. De volgende richtlijnen behoren te worden overwogen:

- a) regels en beheersmaatregelen implementeren die het gebruik van niet-geautoriseerde software voorkomen of detecteren [bijv. een lijst maken van toegestane toepassingen ('allowlisting')] (zie 8.19 en 8.32);
- b) beheersmaatregelen implementeren die het gebruik van bekende of verdachte kwaadaardige websites voorkomen of detecteren (bijv. een blokkeerlijst opstellen ('blocklisting'));
- c) kwetsbaarheden verminderen die kunnen worden geëxploiteerd door malware [bijv. via beheer van technische kwetsbaarheden (zie 8.8 en 8.19)];
- d) regelmatig geautomatiseerde validatie uitvoeren van de software en gegevensinhoud van systemen, met name voor systemen die kritische bedrijfsprocessen ondersteunen; de aanwezigheid van niet-goedgekeurde bestanden of ongeautoriseerde wijzigingen onderzoeken;
- e) beschermende maatregelen vaststellen tegen de risico's die verbonden zijn met het verkrijgen van bestanden en software van of via externe netwerken of op een ander medium;
- f) software voor het detecteren en herstellen van malware installeren en regelmatig bijwerken om computers en elektronische opslagmedia te scannen; reguliere scans uitvoeren die het volgende omvatten:
  - 1) alle gegevens die via netwerken of via welke vorm van elektronische opslagmedia dan ook worden ontvangen, vóór gebruik op malware scannen;
  - 2) bijlagen bij e-mail en instantmessagingsystemen en downloads voorafgaand aan gebruik op malware scannen. Deze scan op verschillende plekken (bijv. op mailservers, pc's) en bij binnenkomst in het netwerk van de organisatie uitvoeren;
  - 3) webpagina's op malware scannen wanneer er toegang toe wordt gemaakt;

- g) de plaatsing en configuratie van hulpmiddelen voor het detecteren van malware en het herstel naar aanleiding daarvan vaststellen, op basis van de resultaten van de risicobeoordeling en rekening houdend met:
- 1) principes voor 'defence in depth' waar deze het doeltreffendst zouden zijn. Dit kan bijvoorbeeld leiden tot de detectie van malware in een netwerkgateway (in verschillende toepassingsprotocollen zoals e-mail, bestandsoverdracht en internet) en in 'endpoint devices' van gebruikers en servers;
  - 2) de ontwijkstechnieken van aanvallers (bijv. het gebruik van versleutelde bestanden) om malware af te leveren of het gebruik van versleutelingsprotocollen om malware te verzenden;
- h) ervoor zorgen dat er bescherming is tegen het introduceren van malware tijdens onderhouds- en noodprocedures, die de normale beheersmaatregelen tegen malware kan omzeilen;
- i) een proces implementeren om tijdelijk of permanent autorisatie te verlenen om bepaalde of alle maatregelen tegen malware uit te schakelen, waaronder bevoegdheden om in uitzonderingsgevallen goedkeuring te verlenen, gedocumenteerde onderbouwing en de beoordelingsdatum. Dit kan nodig zijn wanneer de bescherming tegen malware een verstoring van de normale bedrijfsvoering veroorzaakt;
- j) passende bedrijfscontinuïteitsplannen voorbereiden voor het herstel na malwareaanvallen, met inbegrip van alle nodige maatregelen voor het back-uppen van gegevens en software (waaronder zowel online als offline back-up) en het herstellen ervan (zie 8.13);
- k) omgevingen isoleren waar zich catastrofale gevolgen kunnen voordoen;
- l) procedures en verantwoordelijkheden vaststellen voor hoe om te gaan met bescherming tegen malware op systemen, met inbegrip van training in het gebruik ervan, het melden en herstellen van malwareaanvallen;
- m) alle gebruikers bewustmaken of trainen (zie 6.3) hoe zij de ontvangst, verzending of installatie van met malware geïnfecteerde e-mails, bestanden of programma's kunnen herkennen en mogelijk kunnen tegengaan [de onder n) en o) verzamelde informatie kan worden gebruikt om te bewerkstelligen dat bewustwording en training actueel blijven];
- n) procedures toepassen om regelmatig informatie over nieuwe malware te verzamelen, zoals abonnementen nemen op mailinglijsten of relevante websites bekijken;
- o) verifiëren dat informatie met betrekking tot malware, zoals waarschuwingbulletins, afkomstig is van gekwalificeerde en gerenommeerde bronnen (bijv. betrouwbare internetsites of leveranciers van malwaredetectiesoftware), juist is en informatie biedt.

### **Overige informatie**

Het is niet altijd mogelijk om op bepaalde systemen (bijv. bepaalde industriële besturingssystemen) software te installeren die tegen malware beschermt. Bepaalde vormen van malware infecteren computerbesturingssystemen en computerfirmware dusdanig dat gewone malwarebeheersmaatregelen het systeem niet kunnen opschonen en het nodig is de software voor het besturingssysteem en soms de computerfirmware vanaf een imagebestand volledig te herstellen om weer een veilige situatie te bereiken.

## 8.8 Beheer van technische kwetsbaarheden

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_ dreigingen_en_ kwetsbaarheden	#Governance_en_Ecosysteem #Bescherming #Verdediging

### Beheersmaatregel

Er behoort informatie te worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behorende passende maatregelen te worden getroffen.

### Doel

Misbruik van technische kwetsbaarheden voorkomen.

### Richtlijn

#### Technische kwetsbaarheden identificeren

De organisatie behoort te beschikken over een nauwkeurige inventarislijst van bedrijfsmiddelen (zie 5.9 t/m 5.14) als voorwaarde voor een doeltreffend beheer van technische kwetsbaarheden; in de inventarislijst behoren de leverancier en naam van de software, versienummers, de huidige toepassingsstatus (bijv. welke software is geïnstalleerd op welke systemen) en de binnen de organisatie voor de software verantwoordelijke persoon of personen te worden opgenomen.

Om technische kwetsbaarheden te identificeren behoort de organisatie het volgende in aanmerking te nemen:

- het definiëren en vaststellen van de rollen en verantwoordelijkheden in samenhang met het beheer van technische kwetsbaarheden, met inbegrip van het monitoren van de kwetsbaarheden, een risicobeoordeling van de kwetsbaarheden, updaten, het traceren van bedrijfsmiddelen en de vereiste coördinatieverantwoordelijkheden;
- voor software en andere technologieën (op basis van de inventarislijst van bedrijfsmiddelen, zie 5.9), informatiemiddelen identificeren die worden gebruikt om relevante technische kwetsbaarheden te identificeren en de bewustwording ervan in stand te houden. De lijst met informatiemiddelen bijwerken op basis van veranderingen in de inventarislijst of wanneer er andere nieuwe of nuttige middelen worden gevonden;
- verlangen dat leveranciers van informatiesystemen (met inbegrip van hun componenten) het melden, afhandelen en bekendmaken van kwetsbaarheden garanderen; met inbegrip van de eisen in desbetreffende contracten (zie 5.20);
- gebruikmaken van instrumenten om op kwetsbaarheden te scannen die geschikt zijn voor de gebruikte technologieën om kwetsbaarheden te identificeren en nagaan of het patchen van kwetsbaarheden geslaagd is;

- e) competente en bevoegde personen geplande, gedocumenteerde en herhaalbare penetratietests of kwetsbaarheidsbeoordelingen laten uitvoeren ter ondersteuning van het identificeren van kwetsbaarheden. Zorg betrachten aangezien zulke activiteiten de beveiliging van het systeem in het gedrang kunnen brengen;
- f) het gebruik van bibliotheken en broncode van derden met het oog op kwetsbaarheden traceren. Dit behoort te worden opgenomen in beveiligde codering (zie 8.28).

De organisatie behoort procedures en capaciteiten te ontwikkelen om:

- a) het bestaan te detecteren van kwetsbaarheden in haar producten en diensten, met inbegrip van alle externe componenten die in deze producten en diensten worden gebruikt;
- b) meldingen over kwetsbaarheden van interne of externe bronnen te ontvangen;

De organisatie behoort te voorzien in een openbaar contactpunt als onderdeel van onderwerpspecifiek beleid inzake het bekendmaken van kwetsbaarheden, zodat onderzoekers en anderen in staat zijn problemen te melden. De organisatie behoort procedures voor het melden van kwetsbaarheden op te stellen, online meldformulieren in te richten en gebruik te maken van passende fora voor het delen van informatie en analyses over dreigingen of andere informatie. De organisatie behoort ook na te denken over bug bounty-programma's, waarbij beloningen worden aangeboden als stimulans om organisaties te helpen kwetsbaarheden te identificeren om deze naar behoren te verhelpen. De organisatie behoort ook informatie met bevoegde vertegenwoordigers van het bedrijfsleven of andere belanghebbenden te delen.

#### Technische kwetsbaarheden evalueren

Om geïdentificeerde technische kwetsbaarheden te evalueren behoren de volgende richtlijnen te worden overwogen:

- a) meldingen analyseren en verifiëren om te bepalen welke respons- en herstelmaatregelen nodig zijn;
- b) als er een mogelijke technische kwetsbaarheid is geïdentificeerd, de gerelateerde risico's en te treffen maatregelen identificeren. Het bijwerken van kwetsbare systemen of het toepassen van andere beheersmaatregelen kan onderdeel zijn van die maatregelen.

#### Passende maatregelen treffen om technische kwetsbaarheden op te pakken

Er behoort een beheerprocedure voor het updaten van software te worden geïmplementeerd om te bewerkstelligen dat de meest recente goedgekeurde patches en toepassingsupdates bij alle goedgekeurde software zijn geïnstalleerd. Indien de veranderingen noodzakelijk zijn, behoort de originele software te worden bewaard en behoren de veranderingen aan een speciaal daarvoor bestemde kopie te worden aangebracht. Alle veranderingen behoren volledig te worden getest en gedocumenteerd zodat ze zo nodig opnieuw kunnen worden toegepast bij toekomstige software-upgrades. Indien vereist behoren de wijzigingen door een onafhankelijke beoordelingsinstantie te worden getest en gevalideerd.

De volgende richtlijnen behoren in overweging te worden genomen om technische kwetsbaarheden aan te pakken:

- a) tijdig passende maatregelen treffen als reactie op geïdentificeerde mogelijke technische kwetsbaarheden; een tijdsbestek definiëren waarin moet worden gereageerd op meldingen van mogelijk relevante technische kwetsbaarheden;
- b) afhankelijk van hoe urgent een technische kwetsbaarheid moet worden aangepakt, de actie ondernemen in overeenstemming met de beheersmaatregelen in verband met wijzigingsbeheer (zie 8.32) of door reactieprocedures voor informatiebeveiligingsincidenten te volgen (zie 5.26);

- c) alleen updates gebruiken die afkomstig zijn van legitieme bronnen (dit kunnen interne bronnen binnen de organisatie of externe bronnen buiten de organisatie zijn);
- d) updates testen en evalueren alvorens ze te installeren om te garanderen dat ze doeltreffend zijn en geen neveneffecten met zich meebrengen die niet kunnen worden getolereerd [d.w.z. indien een update beschikbaar is, de risico's in verband met het installeren van de update beoordelen (de risico's als gevolg van de kwetsbaarheid behoren te worden vergeleken met het risico dat het installeren van de update met zich meebrengt)];
- e) systemen met een hoog risico als eerste aanpakken;
- f) herstelmaatregelen ontwikkelen (meestal software-updates of patches);
- g) testen om te bevestigen dat de herstel- of beperkende maatregel doeltreffend is;
- h) voorzien in mechanismen om de authenticiteit van herstelmaatregelen te verifiëren;
- i) indien er geen update beschikbaar is of de update niet kan worden geïnstalleerd, andere beheersmaatregelen overwegen, zoals:
  - 1) een door de softwareleverancier of andere relevante bronnen voorgesteld alternatief toepassen;
  - 2) diensten of capaciteiten in verband met de kwetsbaarheid uitschakelen;
  - 3) toegangsbeveiligingsmaatregelen aanpassen of toevoegen (bijv. firewalls) rond de grenzen van netwerken (zie 8.20 t/m 8.22);
  - 4) kwetsbare systemen, apparaten of toepassingen afschermen tegen aanvallen door passende verkeersfilters toe te passen (soms aangeduid als virtueel patchen);
  - 5) intensiever monitoren om werkelijke aanvallen te detecteren;
  - 6) bewustwording omtrent de kwetsbaarheid kweken;

Voor aangekochte software geldt dat indien de leveranciers regelmatig informatie over beveiligingsupdates voor hun software vrijgeven en een faciliteit bieden om dergelijke updates automatisch te installeren, de organisatie behoort te beslissen of zij al dan niet gebruikmaakt van de automatische update.

#### Overige overwegingen

Over alle stappen die in het kader van het beheer van technische kwetsbaarheden zijn ondernomen, behoort een auditlogbestand te worden bijgehouden.

Het beheerproces met betrekking tot de technische kwetsbaarheid behoort regelmatig te worden gemonitord en geëvalueerd om de doeltreffendheid en doelmatigheid ervan te waarborgen.

Om gegevens over kwetsbaarheden te communiceren aan de functie die de verantwoordelijkheid heeft te reageren op het incident en om te voorzien in uit te voeren technische procedures indien zich een incident voordoet, behoort een doeltreffend beheerproces met betrekking tot de technische kwetsbaarheid te worden afgestemd op incidentbeheeractiviteiten.

Indien de organisatie gebruikmaakt van een door een derde aanbieder van clouddiensten beschikbaar gestelde clouddienst, behoort het beheer van de technische kwetsbaarheden van de middelen van de aanbieder van clouddiensten door deze aanbieder te worden gegarandeerd. De verantwoordelijkheden van de aanbieder van de clouddiensten voor het beheer van technische kwetsbaarheden behoort deel uit te maken van de clouddienstverleningsovereenkomst en dit behoort processen te

omvatten voor het melden van maatregelen van de aanbieder van de clouddiensten met betrekking tot technische kwetsbaarheden (zie 5.23). Voor bepaalde clouddiensten zijn er verantwoordelijkheden respectievelijk voor de aanbieder van de clouddienst en voor de afnemer van de clouddienst. Zo is de afnemer van de clouddienst bijvoorbeeld verantwoordelijk voor het beheer van kwetsbaarheden van de eigen bedrijfsmiddelen die voor de clouddiensten worden gebruikt.

### Overige informatie

Het beheer van technische kwetsbaarheid kan worden beschouwd als een subfunctie van wijzigingsbeheer en kan als zodanig profiteren van de processen en procedures van wijzigingsbeheer (zie 8.32).

Er is een mogelijkheid dat een update het probleem ontoereikend aanpakt en negatieve bijwerkingen heeft. Ook is het in bepaalde gevallen niet gemakkelijk een update na toepassing te de-installeren.

Indien het niet mogelijk is de updates in voldoende mate te testen (bijv. vanwege de kosten of door een gebrek aan middelen), kan worden overwogen het uitvoeren van een update uit te stellen om de samenhangende risico's te evalueren, op basis van de ervaringen die door andere gebruikers worden gemeld. Het kan nuttig zijn om ISO/IEC 27031 te raadplegen.

Indien er softwarepatches of -updates worden geproduceerd, kan de organisatie overwegen in een geautomatiseerd updateproces te voorzien waarbij deze updates op de betrokken systemen of producten worden geïnstalleerd zonder dat de klant of de gebruiker iets hoeft te doen. Indien een geautomatiseerd updateproces wordt aangeboden, kan dit de klant of gebruiker een optie bieden om de automatische update uit te schakelen of controle te hebben over het tijdstip waarop de update wordt geïnstalleerd.

Indien de verkoper een geautomatiseerd updateproces aanbiedt en de updates op getroffen systemen of producten kunnen worden geïnstalleerd zonder dat interventie nodig is, bepaalt de organisatie of zij het geautomatiseerde proces al dan niet toepast. Een reden om niet voor geautomatiseerde updates te kiezen is dat men zelf de controle wil behouden over wanneer de update wordt uitgevoerd. Een update van software die voor een bedrijfsactiviteit wordt gebruikt, kan bijvoorbeeld pas worden uitgevoerd als de activiteit is afgerond.

Een zwak punt van het scannen op kwetsbaarheden is dat het mogelijk is dat daarbij niet volledig rekening wordt gehouden met 'defence in depth': als tegenmaatregelen altijd na elkaar worden ingeroepen, kunnen kwetsbaarheden in de ene tegenmaatregel aan het oog worden onttrokken door sterke punten van de andere. De samengestelde tegenmaatregel is niet kwetsbaar, terwijl een instrument dat wordt gebruikt om op kwetsbaarheden te scannen kan melden dat beide componenten kwetsbaar zijn. De organisatie behoort derhalve zorgvuldig te werk te gaan bij het beoordelen van en het nemen van maatregelen naar aanleiding van gemelde kwetsbaarheden.

Veel organisaties leveren software, systemen, producten en diensten niet alleen binnen de organisatie, maar ook aan belanghebbenden zoals klanten, partners of andere gebruikers. Deze software, systemen, producten en diensten kunnen gepaard gaan met informatiebeveiligingskwetsbaarheden die van invloed zijn op de veiligheid van gebruikers.

Organisaties kunnen herstelmaatregelen vrijgeven en informatie over kwetsbaarheden bekendmaken aan gebruikers (doorgaans via een openbaar informatiebericht) en passende informatie verstrekken voor databasediensten voor softwarekwetsbaarheden.

Meer informatie over het beheer van technische kwetsbaarheden bij het gebruik van cloudcomputing is te vinden in de ISO/IEC 19086-reeks en ISO/IEC 27017.

ISO/IEC 29147 geeft gedetailleerde informatie over het ontvangen van meldingen van kwetsbaarheden en het publiceren van adviezen met betrekking tot kwetsbaarheden. ISO/IEC 30111 geeft gedetailleerde informatie over het omgaan met en oplossen van gemelde kwetsbaarheden.

## 8.9 Configuratiebeheer

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming

### Beheersmaatregel

Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.

### Doel

Garanderen dat hardware, software, diensten en netwerken correct met de vereiste beveiligingsinstellingen functioneren en de configuratie niet door ongeautoriseerde of onjuiste wijzigingen wordt gewijzigd.

### Richtlijn

#### Algemeen

De organisatie behoort processen en instrumenten te definiëren en te implementeren om de voor zowel nieuw geïnstalleerde systemen als bestaande operationele systemen gedefinieerde configuraties (met inbegrip van beveiligingsconfiguraties) voor hardware, software, diensten (bijv. clouddiensten) en netwerken gedurende de levensduur ervan af te dwingen.

Rollen, verantwoordelijkheden en procedures behoren te worden vastgelegd om afdoende beheersing van alle veranderingen aan configuraties te waarborgen.

#### Standardsjablonen

Er behoren standardsjablonen voor de beveiligde configuratie van hardware, software, diensten en netwerken te worden gedefinieerd:

- met behulp van openbaar beschikbare richtlijnen (bijv. vooraf gedefinieerde sjablonen van verkopers en van onafhankelijke beveiligingsorganisaties);
- met inachtneming van het beveiligingsniveau dat nodig is om een afdoende beveiligingsniveau vast te stellen;
- die het informatiebeveiligingsbeleid van de organisatie, onderwerpspecifieke beleidsregels, normen en andere beveiligingseisen van de organisatie ondersteunen;
- waarbij de haalbaarheid en toepasselijkheid van beveiligingsconfiguraties in de context van de organisatie in overweging worden genomen.

De sjablonen behoren regelmatig te worden beoordeeld en bijgewerkt wanneer nieuwe dreigingen of kwetsbaarheden moeten worden aangepakt, of wanneer er nieuwe software- of hardwareversies worden geïntroduceerd.

Voor het vaststellen van standaardsjablonen voor de beveiligde configuratie van hardware, software, diensten en netwerken behoort het volgende in overweging te worden genomen:

- a) het aantal identiteiten met toegangsrechten op speciaal of beheerdersniveau minimaliseren;
- b) onnodige, ongebruikte of onbeveiligde identiteiten uitschakelen;
- c) onnodige functies en diensten uitschakelen of beperken;
- d) de toegang tot krachtige systeemhulpmiddelen en hostparameterinstellingen beperken;
- e) klokken synchroniseren;
- f) de standaard authenticatie-informatie van de leverancier, zoals standaardwachtwoorden onmiddellijk na de installatie wijzigen en andere belangrijke standaardparameters in verband met de beveiliging beoordelen;
- g) time-outvoorzieningen in werking stellen die computerapparatuur na een vooraf vastgestelde inactiviteitsduur automatisch afmelden;
- h) verifiëren dat aan licentie-eisen is voldaan (zie 5.32).

### Configuraties beheren

Vastgestelde configuraties van hardware, software, diensten en netwerken behoren te worden geregistreerd en er behoort een logbestand te worden bijgehouden van alle configuratiewijzigingen. Deze registraties behoren veilig te worden opgeslagen. Dit kan op verschillende manieren worden bereikt, bijvoorbeeld met configuratiedatabases of configuratiesjablonen.

Wijzigingen aan configuraties behoren het wijzigingsbeheerproces te volgen (zie 8.32).

Configuratieregistraties kunnen het volgende, indien relevant, bevatten:

- a) up-to-date informatie over de eigenaar of het contactpunt voor het bedrijfsmiddel;
- b) de datum van de laatste wijziging van de configuratie;
- c) de versie van de configuratiesjabloon;
- d) de relatie tot configuraties van andere bedrijfsmiddelen.

### Configuraties monitoren

Configuraties behoren te worden gemonitord met een uitgebreide verzameling instrumenten voor systeembeheer (bijvoorbeeld onderhoudssysteemhulpmiddelen, ondersteuning op afstand, instrumenten voor bedrijfsbeheer en back-up- en herstelsoftware) en behoren regelmatig te worden beoordeeld om de configuratie-instellingen te verifiëren, de sterkte van wachtwoorden te evalueren en de uitgevoerde activiteiten te beoordelen. De daadwerkelijke configuraties kunnen worden vergeleken met de gedefinieerde doelsjablonen. Eventuele afwijkingen behoren te worden aangepakt, door middel van het automatisch afdwingen van de gedefinieerde doelconfiguratie of door handmatige analyse van de afwijking gevolgd door corrigerende maatregelen.

## Overige informatie

In documentatie voor systemen worden vaak details vastgelegd over de configuratie van zowel hardware als software.

Systeemhardening is een typisch onderdeel van configuratiebeheer.

Configuratiebeheer kan worden geïntegreerd met processen voor het beheer van bedrijfsmiddelen en de bijbehorende instrumenten.

Automatisering is meestal doeltreffender voor het beheren van de beveiligingsconfiguratie (bijv. door gebruik te maken van infrastructuur als code).

Configuratiesjablonen en -doelen kunnen vertrouwelijke informatie zijn en behoren dienovereenkomstig te worden beschermd tegen toegang door onbevoegden.

## 8.10 Wissen van informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid	#Beschermen	#Informatiebe-scherming #Juridisch_en_compliance	#Bescherming

### Beheersmaatregel

In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer nodig is.

### Doel

Onnodige openbaarmaking van gevoelige informatie voorkomen en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voor het wissen van informatie voldoen.

### Richtlijn

#### Algemeen

Om het risico op ongewenste openbaarmaking te beperken behoort gevoelige informatie niet langer te worden bewaard dan nodig is.

Bij het wissen van informatie van systemen, toepassingen en diensten behoort het volgende in overweging te worden genomen:

- a) een wismethode (bijv. elektronisch overschrijven of cryptografisch wissen) selecteren overeenkomstig de bedrijfseisen en met inachtneming van de relevante wet- en regelgeving;
- b) de resultaten van het wissen als bewijsmateriaal registreren;
- c) wanneer gebruik wordt gemaakt van dienstverleners voor het wissen van informatie, bewijs van het wissen van informatie van hen verkrijgen.

Indien derden de informatie van de organisatie namens de organisatie opslaan, behoort de organisatie te overwegen in de overeenkomsten met derden eisen inzake het wissen van informatie op te nemen, die tijdens en bij beëindiging van dergelijke diensten worden afgedwongen.

### Wismethoden

In overeenstemming met het onderwerpspecifieke beleid van de organisatie inzake het bewaren van gegevens en met inachtneming van de desbetreffende wet- en regelgeving, behoort gevoelige informatie te worden gewist wanneer zij niet langer nodig is, door:

- a) systemen dusdanig te configureren dat informatie op een beveiligde manier wordt vernietigd wanneer zij niet langer nodig is (bijv. na een gedefinieerde periode afhankelijk van het onderwerpspecifieke beleid inzake het bewaren van gegevens of op grond van een verzoek om toegang van een betrokkene);
- b) verouderde versies, kopieën en tijdelijke bestanden te wissen, ongeacht waar deze zich bevinden;
- c) gebruik te maken van goedgekeurde, veilige software voor het wissen waardoor informatie blijvend wordt gewist en wordt gegarandeerd dat de informatie niet met behulp van gespecialiseerde herstel- of forensische instrumenten kan worden hersteld;
- d) gebruik te maken van erkende, gecertificeerde aanbieders van beveiligde verwijderingsdiensten;
- e) gebruik te maken van verwijderingsmechanismen die geschikt zijn voor het type opslagmedia dat wordt verwijderd (bijv. door vaste schijven en andere magnetische opslagmedia te degaussen).

Indien gebruik wordt gemaakt van clouddiensten, behoort de organisatie na te gaan of de door de aanbieder van de clouddienst geboden wismethode aanvaardbaar is en indien dit het geval is, behoort de organisatie deze te gebruiken, of de aanbieder van de clouddienst te verzoeken de informatie te wissen. Deze wisprocessen behoren te worden geautomatiseerd overeenkomstig onderwerpspecifieke beleidsregels, indien die beschikbaar en van toepassing zijn. Afhankelijk van de gevoeligheid van de gewiste informatie kan met logbestanden worden getraceerd of geverifieerd dat deze wisprocessen hebben plaatsgevonden.

Om onbedoelde openbaarmaking van gevoelige informatie te voorkomen wanneer apparatuur naar leveranciers wordt teruggestuurd, behoort gevoelige informatie te worden beschermd door hulpopslagfaciliteiten (bijv. vaste schijven) en geheugen te verwijderen voordat de apparatuur het gebouw en/of terrein van de organisatie verlaat.

Aangezien bepaalde apparaten (bijv. smartphones) alleen veilig kunnen worden gewist door ze te vernietigen of door de in deze apparaten ingebouwde functies te gebruiken (bijv. 'fabrieksinstellingen herstellen'), behoort de organisatie de geschikte methode te kiezen op basis van de classificatie van de informatie die door dergelijke apparaten wordt verwerkt.

De in 7.14 beschreven beheersmaatregelen behoren te worden toegepast om het opslagapparaat fysiek te vernietigen en tegelijkertijd de informatie erop te wissen.

Een officiële registratie van het wissen van informatie is nuttig om de oorzaak van een mogelijk lek van informatie te analyseren.

### **Overige informatie**

Informatie over het wissen van gebruikersgegevens in clouddiensten is te vinden in ISO/IEC 27017.

Informatie over het wissen van persoonsgegevens is te vinden in ISO/IEC 27555.

## 8.11 Maskeren van gegevens

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid	#Beschermen	#Informatiebescherming	#Bescherming

### Beheersmaatregel

Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.

### Doel

De openbaarmaking van gevoelige informatie met inbegrip van persoonsgegevens beperken en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voldoen.

### Richtlijn

Indien de bescherming van gevoelige gegevens (bijv. persoonsgegevens) een punt van zorg is, behoort de organisatie te overwegen dergelijke gegevens te verbergen door gebruik te maken van technieken als het maskeren, pseudonimiseren of anonimiseren van gegevens.

Met pseudonimiserings- of anonimiseringstechnieken kunnen persoonsgegevens worden verborgen, de ware identiteit van de betrokkenen bij persoonsgegevens of andere gevoelige informatie worden verhuld, en het verband tussen persoonsgegevens en de identiteit van de betrokkene of het verband tussen andere gevoelige informatie worden verbroken.

Bij gebruik van pseudonimiserings- of anonimiseringstechnieken behoort te worden nagegaan of de gegevens afdoende zijn gepseudonimiseerd of geanonimiseerd. Om doeltreffend te zijn behoren bij het anonimiseren van gegevens alle elementen van de gevoelige informatie in aanmerking te worden genomen, anders kan bijvoorbeeld een persoon worden geïdentificeerd, zelfs als de gegevens waarmee die persoon direct kan worden geïdentificeerd zijn geanonimiseerd, doordat er andere gegevens aanwezig zijn aan de hand waarvan de persoon indirect kan worden geïdentificeerd.

Aanvullende technieken voor het maskeren van gegevens zijn onder andere:

- a) versleuteling (zodat bevoegde gebruikers alleen met een sleutel toegang hebben);
- b) tekens weghalen of wissen (waarmee wordt voorkomen dat onbevoegde gebruikers volledige berichten zien);
- c) wisselen van getallen en data;
- d) substitutie (een waarde door een andere vervangen om gevoelige gegevens te verbergen);
- e) waarden door de desbetreffende hash vervangen.

Het volgende behoort te worden overwogen bij het implementeren van technieken voor het maskeren van gegevens:

- a) niet alle gebruikers toegang tot alle gegevens geven, en daarom query's en maskers zo ontwerpen dat alleen de minimaal vereiste gegevens zichtbaar zijn voor de gebruiker;
- b) er zijn gevallen waarin bepaalde gegevens voor de gebruiker niet zichtbaar behoren te zijn voor sommige gegevenselementen in een verzameling gegevens; in dat geval een mechanisme ontwerpen en implementeren voor de versluiering van gegevens (bijv. indien een patiënt niet wil dat ziekenhuispersoneel, zelfs in geval van nood, alle gegevens over de patiënt kan zien; in dat geval krijgt het ziekenhuispersoneel gedeeltelijk versluierde gegevens te zien en hebben alleen personeelsleden met specifieke rollen toegang tot de gegevens als die nuttige informatie bevatten voor een passende behandeling);
- c) wanneer gegevens versluierd zijn, de betrokkene de mogelijkheid geven te eisen dat gebruikers niet kunnen zien of die gegevens versluierd zijn (versluiering van de versluiering; dit wordt gebruikt in gezondheidsinstellingen, bijvoorbeeld als de patiënt niet wil dat het personeel ziet dat gevoelige informatie zoals zwangerschappen of resultaten van bloedonderzoeken is versluierd);
- d) eventuele eisen van wet- en regelgeving (bijv. vereisen dat informatie van betaalkaarten tijdens de verwerking of opslag wordt gemaskeerd).

Het volgende behoort te worden overwogen bij het maskeren, pseudonimiseren of anonimiseren van gegevens:

- a) de mate van sterkte van gegevensmaskering, pseudonimisering of anonimisering gezien het gebruik van de verwerkte gegevens;
- b) beveiliging van de toegang tot de verwerkte gegevens;
- c) afspraken of beperkingen met betrekking tot het gebruik van de verwerkte gegevens;
- d) verbieden dat de verwerkte gegevens worden samengevoegd met andere informatie om de betrokkene te identificeren;
- e) de verstrekking en ontvangst van de verwerkte gegevens bijhouden.

### **Overige informatie**

Door anonimisering worden persoonsgegevens dusdanig onomkeerbaar gewijzigd dat de betrokkene niet langer rechtstreeks of indirect kan worden geïdentificeerd.

Bij pseudonimisering wordt de identificerende informatie door een alias vervangen. Kennis van het algoritme (soms 'aanvullende informatie' genoemd) dat wordt gebruikt om de pseudonimisering uit te voeren, maakt in ieder geval een bepaalde vorm van identificatie van de betrokkene mogelijk. Dergelijke 'aanvullende informatie' behoort daarom apart te worden gehouden en te worden beschermd.

Hoewel pseudonimisering dus zwakker is dan anonimisering, kunnen gepseudonimiseerde gegevensverzamelingen nuttiger zijn voor statistisch onderzoek.

Het maskeren van gegevens is een verzameling technieken waarmee gevoelige gegevens worden verborgen, vervangen of versluierd. Het maskeren van gegevens kan statisch zijn (als gegevens in de oorspronkelijke database worden gemaskeerd), dynamisch (waarbij automatisering en regels worden

gebruikt om gegevens in real time te beveiligen) of 'on-the-fly' (waarbij gegevens in het geheugen van een toepassing worden gemaskeerd).

Hashfuncties kunnen worden gebruikt om persoonsgegevens te anonimiseren. Om enumeratie-aanvallen te voorkomen, behoren ze altijd te worden gecombineerd met een 'salt'-functie, waarbij willekeurige gegevens worden toegevoegd.

Persoonsgegevens in identificatiecodes van middelen en de bijbehorende attributen [bijv. bestandsnamen, uniform resource locators (URL's)] behoren te worden vermeden of op passende wijze te worden geanonimiseerd.

Aanvullende beheersmaatregelen met betrekking tot de bescherming van persoonsgegevens in publieke clouds worden gegeven in ISO/IEC 27018.

Aanvullende informatie over de-identificatietechnieken is te vinden in ISO/IEC 20889.

## 8.12 Voorkomen van gegevenslekken (Data leakage prevention)

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief	#Vertrouwelijkheid	#Beschermen #Detecteren	#Informatiebe-scherming	#Bescherming #Verdediging

### Beheersmaatregel

Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.

### Doel

Om de ongeoorloofde openbaarmaking en extractie van informatie door personen of systemen te detecteren en te voorkomen.

### Richtlijn

De organisatie behoort het volgende te overwegen om het risico op gegevenslekken te beperken:

- informatie identificeren en classificeren als bescherming tegen lekken (bijv. persoonsinformatie, prijsbepalingsmodellen en productontwerpen);
- kanalen waarlangs gegevens kunnen lekken, monitoren (bijv. e-mail, bestandsoverdracht, mobiele apparaten en draagbare opslagapparatuur);
- actie ondernemen om te voorkomen dat informatie weglekt (bijv. e-mails met gevoelige informatie in quarantaine plaatsen).

Er behoren hulpmiddelen voor het voorkomen van gegevenslekken te worden gebruikt om:

- a) te identificeren welke gevoelige informatie blootstaat aan het risico op ongeoorloofde openbaarmaking (bijv. in niet-gestructureerde gegevens op het systeem van een gebruiker) en dit te monitoren;
- b) de openbaarmaking van gevoelige informatie te detecteren (bijv. wanneer informatie wordt geüpload naar niet-vertrouwde clouddiensten van derden of via e-mail wordt verzonden);
- c) handelingen van gebruikers of netwerktransmissies waardoor gevoelige informatie bekend wordt, te blokkeren (bijv. voorkomen dat databasegegevens naar een spreadsheet worden gekopieerd).

De organisatie behoort vast te stellen of het nodig is de mogelijkheid te beperken dat gebruikers gegevens kopiëren en plakken en deze naar diensten, apparaten en opslagmedia buiten de organisatie uploaden. In dat geval behoort de organisatie technologie te implementeren zoals instrumenten ter voorkoming van gegevenslekken of bestaande instrumenten dusdanig te configureren dat gebruikers gegevens op afstand kunnen bekijken en manipuleren, waarbij kopiëren en plakken waarop de organisatie geen controle heeft, wordt voorkomen.

Als het exporteren van gegevens vereist is, behoort de eigenaar van de gegevens in staat te zijn dit goed te keuren en gebruikers verantwoordelijk te stellen voor hun daden.

Voor het maken van schermafbeeldingen of foto's van het scherm behoren gebruiksvoorwaarden te worden opgesteld en hieraan behoort in trainingen en audits aandacht te worden besteed.

Indien er een back-up van gegevens wordt gemaakt, behoort ervoor te worden gezorgd dat gevoelige informatie wordt beschermd door maatregelen zoals encryptie, toegangsbeveiliging en fysieke bescherming van de opslagmedia waarop de back-up staat.

Het voorkomen van gegevenslekken behoort ook te worden beschouwd als een vorm van bescherming tegen de acties van tegenstanders om vertrouwelijke of geheime informatie (geopolitieke, menselijke, financiële, commerciële, wetenschappelijke of andere informatie) te verkrijgen die van belang kan zijn voor spionage of essentieel kan zijn voor de gemeenschap. De maatregelen ter voorkoming van het lekken van gegevens behoren erop gericht te zijn verwarring te zaaien wat betreft de beslissingen van de tegenstander, bijvoorbeeld door authentieke informatie te vervangen door valse informatie, hetzij als een eigen maatregel, hetzij als reactie op de acties van de tegenstander om informatie te verzamelen. Voorbeelden van dergelijke maatregelen zijn omgekeerde 'social engineering' of het gebruik van 'honeypots' om aanvallers te lokken.

### **Overige informatie**

Hulpmiddelen om gegevenslekken te voorkomen, zijn ervoor ontworpen om gegevens te identificeren, het gebruik en de verplaatsing van gegevens te monitoren, en maatregelen te nemen om gegevenslekken te voorkomen (bijv. gebruikers waarschuwen voor hun risicogedrag en de overdracht van gegevens naar draagbare opslagapparatuur blokkeren).

Een inherent element van het voorkomen van gegevenslekken is toezicht op de communicatie en de online activiteiten van het personeel en, in het verlengde daarvan, op de berichten van externe partijen, hetgeen aanleiding kan geven tot juridische aspecten die behoren te worden overwogen voordat instrumenten om gegevenslekken te voorkomen worden ingezet. Allerlei wetgeving op het gebied van privacy, gegevensbescherming, werkgelegenheid, het onderscheppen van gegevens en telecommunicatie is van toepassing op monitoren en gegevensverwerking in het kader van het voorkomen van gegevenslekken.

Het voorkomen van gegevenslekken kan worden ondersteund door standaardbeheersmaatregelen voor informatiebeveiliging, zoals onderwerpspecifiek beleid inzake toegangscontrole en veilig documentenbeheer (zie 5.12 en 5.15).

### 8.13 Back-up van informatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming

#### Beheersmaatregel

Back-ups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.

#### Doel

Herstel mogelijk maken na verlies van gegevens of systemen.

#### Richtlijn

Er behoort een onderwerpspecifiek beleid inzake back-ups te worden opgesteld met het oog op de eisen van de organisatie wat betreft het bewaren van gegevens en informatiebeveiliging.

Er behoort te worden voorzien in afdoende back-upfaciliteiten om te waarborgen dat alle essentiële informatie en software na een incident of na falen of verlies van opslagmedia kan worden hersteld.

Er behoren plannen te worden ontwikkeld en geïmplementeerd voor hoe de organisatie back-ups gaat maken van informatie, software en systemen, met het oog op het onderwerpspecifieke beleid inzake back-ups.

Bij het opstellen van een back-upplan, behoren de volgende punten in overweging te worden genomen:

- nauwkeurige en volledige registers van de back-upkopieën en gedocumenteerde herstelprocedures produceren;
- de bedrijfseisen van de organisatie (bijv. de RPO's, zie 5.30), de beveiligingseisen van de betrokken informatie en het belang van de informatie voor de voortzetting van de bedrijfsuitvoering van de organisatie behoren te worden weerspiegeld in de omvang (bijv. volledige of gedifferentieerde back-up) en de frequentie van back-ups;
- de back-ups in een veilige en beveiligde afgelegen locatie bewaren, op een voldoende afstand om niet te worden beschadigd door een calamiteit op de hoofdlocatie;
- aan back-upinformatie een passend niveau van fysieke en omgevingsbescherming geven (zie hoofdstuk 7 en 8.1), consistent met de normen die op de hoofdlocatie worden toegepast;
- back-upmedia regelmatig testen om te garanderen dat men er wanneer nodig voor gebruik in noodgevallen op kan vertrouwen. Op een testsysteem testen of de back-upgegevens kunnen worden hersteld en dit niet testen door de originele opslagmedia te overschrijven, aangezien het back-up- of herstelproces kan mislukken en onherstelbare schade aan of verlies van gegevens kan veroorzaken;

- f) back-ups door middel van encryptie beschermen, naargelang de geïdentificeerde risico's (bijv. in situaties waar vertrouwelijkheid van belang is);
- g) ervoor zorgen dat wordt gegarandeerd dat onopzettelijk gegevensverlies wordt opgespoord voordat een back-up wordt gemaakt.

Bedieningsprocedures behoren de uitvoering van back-ups te monitoren en fouten in geplande back-ups aan te pakken om de volledigheid van back-ups in overeenstemming met het onderwerpspecifieke beleid inzake back-ups te waarborgen.

Back-upmaatregelen voor individuele systemen en diensten behoren regelmatig te worden getest om te waarborgen dat ze voldoen aan de doelstellingen van incidentrespons- en bedrijfscontinuïteitsplannen (zie 5.30). Dit behoort te worden gecombineerd met een test van de herstelprocedures en te worden gecontroleerd aan de hand van de volgens het bedrijfscontinuïteitsplan vereiste hersteltijd. In het geval van kritische systemen en diensten behoren back-upmaatregelen betrekking te hebben op de informatie, toepassingen en gegevens van alle systemen die nodig zijn om het gehele systeem na een calamiteit te herstellen.

Wanneer de organisatie gebruikmaakt van een clouddienst, behoren er back-ups van de informatie, toepassingen en systemen van de organisatie in de clouddienstomgeving te worden gemaakt. De organisatie behoort vast te stellen of en hoe aan de eisen voor het back-uppen wordt voldaan bij het gebruik van de in het kader van de clouddienst aangeboden dienst voor het back-uppen van informatie.

Voor belangrijke bedrijfsinformatie behoort de bewaartermijn te worden vastgesteld, rekening houdend met eisen voor het bewaren van archiefkopieën. De organisatie behoort na te denken over het wissen van informatie (zie 8.10) in of op opslagmedia zodra de bewaartermijn van de informatie verstrijkt en behoort hierbij de wet- en regelgeving in aanmerking te nemen.

#### Overige informatie

Zie voor verdere informatie over beveiligde opslag, met inbegrip van bewaarspecifieke overwegingen, ISO/IEC 27040.

### 8.14 Redundantie van informatieverwerkende faciliteiten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Beschikbaarheid	#Beschermen	#Continuïteit #Beheer_van_be- drijfsmiddelen	#Bescherming #Veerkracht

#### Beheersmaatregel

Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

#### Doel

De ononderbroken werking van informatieverwerkende faciliteiten waarborgen.

## Richtlijn

De organisatie behoort eisen te identificeren voor de beschikbaarheid van zakelijke diensten en informatiesystemen. De organisatie behoort een systeemarchitectuur te ontwerpen en implementeren met passende redundantie om aan deze eisen te voldoen.

Redundantie kan worden geïntroduceerd door informatieverwerkende faciliteiten deels of geheel te dupliceren (d.w.z. reservecomponenten of twee van alles hebben). De organisatie behoort procedures te plannen en te implementeren voor het activeren van de redundante componenten en verwerkende faciliteiten. In de procedures behoort te worden vastgesteld of de redundante componenten en verwerkende activiteiten altijd zijn geactiveerd of, in een noodgeval, automatisch of handmatig worden geactiveerd. De redundante componenten en informatieverwerkende faciliteiten behoren hetzelfde beveiligingsniveau te garanderen als hun primaire tegenhangers.

Er behoren mechanismen te zijn om de organisatie te waarschuwen voor een storing in de informatieverwerkende faciliteiten, zodat de geplande procedure kan worden uitgevoerd en de beschikbaarheid in stand blijft terwijl de informatieverwerkende faciliteiten worden gerepareerd of vervangen.

De organisatie behoort het volgende te overwegen bij het implementeren van redundante systemen:

- a) overeenkomsten met twee of meer leveranciers van netwerkdiensten en diensten voor het verwerken van essentiële informatie, zoals aanbieders van internetdiensten, aangaan;
- b) gebruikmaken van redundante netwerken;
- c) gebruikmaken van twee geografisch gescheiden datacentra met gespiegelde systemen;
- d) gebruikmaken van fysiek redundante voedingen of stroombronnen;
- e) gebruikmaken van meerdere parallelle instanties van softwarecomponenten, met automatische onderlinge 'loadbalancing' (tussen instanties in hetzelfde datacentrum of in verschillende datacentra);
- f) beschikken over gedupliceerde componenten in systemen (bijv. CPU, vaste schijven, geheugens) of in netwerken (bijv. firewalls, routers, switches).

Indien van toepassing, bij voorkeur in productiebedrijf, behoren redundante informatiesystemen te worden getest om te waarborgen dat de automatische omschakeling van de ene op de andere component bij storing werkt zoals voorzien.

## Overige informatie

Er bestaat een sterk verband tussen redundantie en de gereedheid van ICT voor bedrijfscontinuïteit (zie 5.30), vooral indien korte hersteltijden vereist zijn. Veel van de redundantie maatregelen kunnen deel uitmaken van de strategieën en oplossingen voor ICT-continuïteit.

Het implementeren van redundantie kan risico's met zich meebrengen voor de integriteit (bijv. processen waarbij gegevens naar gedupliceerde componenten gekopieerd worden, kunnen fouten met zich meebrengen) of vertrouwelijkheid (bijv. een zwakke beveiligingsbeheersmaatregel voor gedupliceerde componenten kan tot compromittering leiden) van informatie en informatiesystemen. Het is nodig om dit in aanmerking te nemen bij het ontwerpen van informatiesystemen.

Redundantie in informatieverwerkende faciliteiten gaat meestal niet in op het niet-beschikbaar zijn van een toepassing als gevolg van fouten in de toepassing.

Met het gebruik van 'public cloud computing' is het mogelijk om meerdere liveversies van informatieverwerkende faciliteiten te hebben, die zich op meerdere afzonderlijke fysieke locaties bevinden met automatische omschakeling bij storingen en onderlinge loadbalancing.

Een aantal technologieën en technieken voor het voorzien in redundantie en automatische omschakeling bij storingen in de context van clouddiensten wordt besproken in ISO/IEC TS 23167.

## 8.15 Logging

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging

### Beheersmaatregel

Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.

### Doel

Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen leiden en onderzoeken ondersteunen.

### Richtlijn

#### Algemeen

De organisatie behoort het doel vast te stellen waarvoor logbestanden worden aangemaakt, welke gegevens worden verzameld en in het logbestand worden geregistreerd en welke logbestandspecifieke eisen er zijn voor het beschermen en behandelen van de gegevens in het logbestand. Dit behoort te worden gedocumenteerd in onderwerpspecifiek registratiebeleid.

Logbestanden van gebeurtenissen behoren het volgende voor elke gebeurtenis te bevatten, al naargelang van toepassing is:

- a) gebruikersidentificaties;
- b) systeemactiviteiten;
- c) data, tijdstippen en details van relevante gebeurtenissen (bijv. in- en uitloggen);
- d) de identiteit van apparaten, identificatie van systemen en hun locatie;
- e) netwerkadressen en -protocollen.

Het behoort te worden overwogen de volgende gebeurtenissen in logbestanden vast te leggen:

- a) geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem;
- b) goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie;
- c) systeemconfiguratieveranderingen;
- d) het gebruik van speciale bevoegdheden;
- e) het gebruik van systeemhulpmiddelen en -toepassingen;
- f) de bestanden waartoe toegang is gemaakt en de soort toegang, met inbegrip van het wissen van belangrijke gegevensbestanden;
- g) alarmen die worden afgegeven door het toegangsbeveiligingssysteem;
- h) activering en deactivering van beveiligingssystemen, zoals antivirussystemen en inbraakdetectiesystemen;
- i) het aanmaken, wijzigen of wissen van identiteiten;
- j) transacties die door gebruikers in toepassingen zijn uitgevoerd. In sommige gevallen zijn de toepassingen een door een derde verleend(e), geleverd(e) of verzorgd(e) dienst of product.

Het is belangrijk dat alle systemen gesynchroniseerde tijdsbronnen hebben (zie 8.17), aangezien dit het mogelijk maakt logbestanden van verschillende systemen met elkaar te correleren voor analyse, alarmering en voor het onderzoeken van incidenten.

#### Logbestanden beschermen

Gebruikers, ook die met speciale toegangsrechten, behoren geen toestemming te hebben om logbestanden van hun eigen activiteiten te verwijderen of te deactiveren. Zij kunnen mogelijk de logbestanden over informatieverwerkende faciliteiten waarover zij het directe bestuur hebben, manipuleren. Daarom is het nodig de logbestanden te beschermen en te beoordelen om de verantwoordelijkheid voor de gebruikers met speciale rechten in stand te houden.

Beheersmaatregelen behoren gericht te zijn op het beschermen van informatie in logbestanden tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, met inbegrip van:

- a) veranderingen aan de soorten berichten die worden vastgelegd;
- b) bewerken of verwijderen van logbestanden;
- c) het niet-registreren van gebeurtenissen of het overschrijven van eerder geregistreerde gebeurtenissen indien de capaciteit van opslagmedia met een logbestand wordt overschreden.

Ter bescherming van logbestanden behoort het gebruik van de volgende technieken te worden overwogen: cryptografisch hashen, registratie in een bestand waar alleen toevoegen of alleen lezen mogelijk is, registratie in een openbaar transparant bestand.

Voor bepaalde auditlogbestanden kan het vereist zijn dat ze worden gearhiveerd vanwege eisen met betrekking tot het bewaren van gegevens of eisen met betrekking tot het verzamelen en bewaren van bewijsmateriaal (zie 5.28).

Indien de organisatie logbestanden inzake systemen of toepassingen naar een leverancier moet sturen om te helpen bij het detecteren of oplossen van fouten of storingen, behoren de logbestanden waar mogelijk te worden gede-identificeerd door gebruik te maken van technieken voor het maskeren van gegevens (zie 8.11) voor informatie zoals gebruikersnamen, IP-adressen, hostnamen of de naam van de organisatie, alvorens ze naar de leverancier te sturen.

Logbestanden van gebeurtenissen kunnen gevoelige gegevens en persoonsgegevens bevatten. Ter bescherming van de privacy behoren passende maatregelen te worden genomen (zie 5.34).

#### Analyse van logbestanden

De analyse van logbestanden behoort te bestaan uit het analyseren en interpreteren van informatiebeveiligingsgebeurtenissen om ongebruikelijke activiteiten of afwijkend gedrag, hetgeen mogelijke indicatoren van compromittering zijn, te helpen identificeren.

Bij het analyseren van gebeurtenissen behoort rekening te worden gehouden met:

- a) de noodzakelijke vaardigheden van de deskundigen die de analyse uitvoeren;
- b) het vaststellen van de procedure voor het analyseren van logbestanden;
- c) de vereiste attributen van elke beveiligingsgerelateerde gebeurtenis;
- d) uitzonderingen die zijn geïdentificeerd door het gebruik van vooraf vastgestelde regels (bijv. SIEM- of firewallregels, en IDS- of malwarehandtekeningen);
- e) bekende gedragspatronen en standaardnetwerkverkeer in vergelijking met afwijkend(e) activiteiten en gedrag (analyse van het gedrag van gebruikers en entiteiten - UEBA);
- f) resultaten van de analyse van trends of patronen (bijv. als gevolg van het gebruik van gegevensanalyse, bigdatatechnieken en gespecialiseerde analyse-instrumenten);
- g) beschikbare informatie en analyses over dreigingen.

De analyse van logbestanden behoort te worden ondersteund door specifieke monitoringactiviteiten om afwijkend gedrag te helpen identificeren en analyseren, waaronder:

- a) het beoordelen van geslaagde en mislukte pogingen om toegang te krijgen tot beschermde bronnen (bijv. DNS-servers, webportals en bestandsshares);
- b) het controleren van DNS-logbestanden om uitgaande netwerkverbindingen met kwaadaardige servers te identificeren, zoals verbindingen die in verband worden gebracht met 'command-and-control' servers van botnets;
- c) het onderzoeken van gebruiksverslagen van dienstverleners (bijv. facturen of verslagen van de geleverde diensten) op ongebruikelijke activiteit binnen systemen en netwerken (bijvoorbeeld door activiteitenpatronen te beoordelen);
- d) het opnemen van gebeurtenislogbestanden van fysieke monitoring, zoals in- en uitgang, met het oog op een nauwkeurigere detectie en analyse van incidenten;
- e) het correleren van logbestanden om doelmatige en zeer nauwkeurige analyse mogelijk te maken.

Vermeende en daadwerkelijke informatiebeveiligingsincidenten behoren te worden geïdentificeerd (bijv. besmetting met malware of het uitpeilen van firewalls) en nader te worden onderzocht (bijv. in het kader van een proces voor het beheer van informatiebeveiligingsincidenten, zie 5.25).

## Overige informatie

Systeemlogbestanden bevatten vaak een grote hoeveelheid informatie, waarvan een groot deel irrelevant is voor het monitoren van informatiebeveiliging. Om belangrijke gebeurtenissen voor het monitoren in het kader van informatiebeveiliging te helpen identificeren, kan het gebruik van geschikte systeemhulpmiddelen of auditinstrumenten voor het bevragen van bestanden worden overwogen.

Logbestanden van gebeurtenissen vormen de basis van geautomatiseerde monitorsystemen (zie 8.16) die geconsolideerde rapporten en waarschuwingen over systeembeveiliging kunnen verzamelen.

Er kan een hulpmiddel voor het beheer van beveiligingsinformatie en -gebeurtenissen (SIEM) of een gelijkwaardige dienst worden gebruikt om loginformatie op te slaan, te correleren, normaliseren en analyseren en waarschuwingmeldingen te genereren. Meestal is het nodig SIEM-hulpmiddelen zorgvuldig te configureren om de voordelen ervan te optimaliseren. Configuraties die in aanmerking behoren te worden genomen, omvatten het identificeren en selecteren van passende bronnen voor logbestanden, het afstemmen en testen van regels, en het ontwikkelen van usecases.

Er worden openbaar transparante bestanden gebruikt voor het registreren van logbestanden, bijvoorbeeld in systemen voor de transparantie van certificaten. Dergelijke bestanden kunnen een extra detectiemechanisme bieden dat nuttig is ter bescherming tegen manipulatie van logbestanden.

In cloudomgevingen kunnen de afnemer en de leverancier van de clouddienst de verantwoordelijkheden voor het beheer van logbestanden met elkaar delen. De verantwoordelijkheden variëren afhankelijk van de soort clouddienst die wordt gebruikt. Verdere richtlijnen zijn te vinden in ISO/IEC 27017.

### 8.16 Monitoren van activiteiten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligings-gebeurtenissen	#Verdediging

#### Beheersmaatregel

Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.

#### Doel

Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.

#### Richtlijn

De reikwijdte en het niveau van de monitoring behoren te worden bepaald overeenkomstig de bedrijfs- en informatiebeveiligingseisen en met inachtneming van de relevante wet- en regelgeving. Er behoren registraties van de monitoring te worden bijgehouden gedurende gedefinieerde bewaartermijnen.

Het behoort te worden overwogen het volgende in het monitoringsysteem op te nemen:

- a) uitgaand en inkomend netwerk-, systeem- en toepassingsverkeer;
- b) toegang tot systemen, servers, netwerkapparatuur, monitoringsysteem, essentiële toepassingen enz.;
- c) systeem- en netwerkconfiguratiebestanden op essentieel of beheerdersniveau;
- d) logbestanden van beveiligingsinstrumenten [bijv. antivirus, IDS, inbraakpreventiesysteem (IPS), webfilters, firewalls, voorkoming van gegevenslekken];
- e) logbestanden van gebeurtenissen met betrekking tot systeem- en netwerkactiviteit;
- f) controle of de code die wordt uitgevoerd, in het systeem mag worden uitgevoerd en of deze niet is gemanipuleerd (bijv. door hercompileren om extra ongewenste code toe te voegen);
- g) gebruik van de middelen (bijvoorbeeld CPU, vaste schijven, geheugen, bandbreedte) en de prestaties daarvan.

De organisatie behoort een nullijn voor normaal gedrag vast te stellen en aan de hand van deze nullijn op afwijkingen te monitoren. Bij het vaststellen van de nullijn behoort het volgende te worden overwogen:

- a) het gebruik van de systemen in normale en piekperiodes beoordelen;
- b) het gebruikelijke tijdstip van toegang, de gebruikelijke plaats van toegang en de gebruikelijke frequentie van toegang voor elke gebruiker of gebruikersgroep.

Het monitoringsysteem behoort te worden geconfigureerd aan de hand van de vastgestelde nullijn om afwijkend gedrag te identificeren, zoals:

- a) ongeplande beëindiging van processen of toepassingen;
- b) activiteiten die meestal verband houden met malware of verkeer dat afkomstig is van bekende kwaadaardige IP-adressen of netwerkdomeinen (bijv. die verband houden met command-and-controlservers van botnets);
- c) bekende aanvalskennmerken (bijv. 'denial of service' en bufferoverflows);
- d) ongebruikelijk systeemgedrag (bijv. het registreren van toetsaanslagen, procesinjectie en afwijkingen in het gebruik van standaardprotocollen);
- e) knelpunten en overbelasting (bijv. netwerkwachtrijen, latentieniveaus en netwerkjitter);
- f) (daadwerkelijke of pogingen tot) toegang door onbevoegden tot systemen of informatie;
- g) het ongeoorloofd scannen van bedrijfstoepassingen, -systemen en -netwerken;
- h) geslaagde en mislukte pogingen om toegang te krijgen tot beschermde bronnen (bijv. DNS-servers, webportals en bestandssystemen);
- i) ongebruikelijk gebruikers- en systeemgedrag in vergelijking met het verwachte gedrag.

Er behoort gebruik te worden gemaakt van continue monitoring via een monitoringinstrument. Monitoring behoort realtime of met regelmatige tussenpozen te gebeuren, afhankelijk van de behoefte en mogelijkheden van de organisatie. Monitoringinstrumenten behoren geschikt te zijn voor grote hoeveelheden gegevens, zich aan te passen aan een voortdurend veranderend landschap van dreigingen en realtimemeldingen mogelijk te maken. De instrumenten behoren ook specifieke handtekeningen en gegevens of netwerk- of toepassingsgedragspatronen te kunnen herkennen.

Geautomatiseerde monitoringsoftware behoort dusdanig te worden geconfigureerd dat deze meldingen geeft (bijv. via beheerconsoles, e-mails of instantmessagingsystemen) op basis van vooraf gedefinieerde drempels. Het waarschuwingssysteem behoort op basis van de nullijn van de organisatie te worden afgestemd en getraind om valspositieven tot een minimum te beperken. Personeel behoort erop gericht te zijn om op waarschuwingen te reageren en naar behoren getraind te zijn om potentiële incidenten accuraat te interpreteren. Er behoren redundante systemen en processen aanwezig te zijn om waarschuwingsmeldingen te ontvangen en erop te reageren.

Abnormale gebeurtenissen behoren aan relevante partijen te worden meegedeeld, zodat de volgende activiteiten kunnen worden verbeterd: auditen, evaluatie van de beveiliging, scannen op kwetsbaarheden en monitoren (zie 5.25). Er behoren procedures te zijn ingevoerd om tijdig te reageren op positieve indicatoren van het monitoringsysteem teneinde het effect van nadelige gebeurtenissen op informatiebeveiliging tot het minimum te beperken (zie 5.26). Er behoren ook procedures te worden vastgesteld om valspositieven te identificeren en aan te pakken, waaronder het afstemmen van de monitoringsoftware om het toekomstige aantal valspositieven te beperken.

### Overige informatie

Beveiligingsmonitoring kan worden verbeterd door:

- a) gebruik te maken van systemen voor informatie en analyses over dreigingen (zie 5.7);
- b) gebruik te maken van de mogelijkheden van machinelearning en kunstmatige intelligentie;
- c) blokkeringslijsten of toestemmingslijsten te gebruiken;
- d) allerlei technische beveiligingsbeoordelingen (bijv. beoordelen op kwetsbaarheden, penetratietests, simulaties van cyberaanvallen en cyberresponsoefeningen) uit te voeren, en de resultaten van deze beoordelingen te gebruiken om de nullijnen of aanvaardbaar gedrag te helpen vaststellen;
- e) gebruik te maken van systemen voor het monitoren van prestaties om afwijkend gedrag te helpen vaststellen en detecteren;
- f) gebruik te maken van logbestanden in combinatie met monitoringsystemen.

Monitoringactiviteiten worden vaak uitgevoerd met behulp van gespecialiseerde software, zoals inbraakdetectiesystemen. Deze kunnen worden geconfigureerd aan de hand van een nullijn van normale, aanvaardbare en verwachte systeem- en netwerkactiviteiten.

Op afwijkende communicatie monitoren helpt bij het identificeren van botnets (d.w.z. een verzameling apparaten onder de kwaadwillige controle van de botneteigenaar, die meestal wordt gebruikt voor het uitvoeren van gedistribueerde denial-of-serviceaanvallen op andere computers van andere organisaties). Indien de computer door een extern apparaat wordt bestuurd, is er communicatie tussen het besmette en het besturende apparaat. De organisatie behoort daarom technologieën in te zetten om afwijkende communicatie te monitoren en zo nodig maatregelen te nemen.

## 8.17 Kloksynchronisatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Detectief	#Integriteit	#Beschermen #Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging

### Beheersmaatregel

De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.

### Doel

De correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere geregistreerde gegevens mogelijk maken en onderzoeken bij informatiebeveiligingsincidenten ondersteunen.

### Richtlijn

Externe en interne eisen voor weergave, betrouwbare synchronisatie en nauwkeurigheid van tijd behoren te worden gedocumenteerd en geïmplementeerd. Zulke eisen kunnen voortvloeien uit wet- en regelgeving, statuten, overeenkomsten, normen en uit interne monitoringbehoeften. Er behoort een standaardreferentietijd voor gebruik binnen de organisatie te worden gedefinieerd en in aanmerking te worden genomen voor alle systemen, met inbegrip van gebouwbeheersystemen, in- en uitgangssystemen en andere systemen die ter ondersteuning van onderzoeken kunnen worden gebruikt.

Een aan een nationale atoomklok die radiogolven uitzendt of aan gps (wereldwijd positioneringssysteem) gekoppelde klok behoort te worden gebruikt als referentieklok voor logsystemen; een consistente, vertrouwde bron voor de datum en tijd om nauwkeurige tijdstempels te garanderen. Protocollen zoals netwerkprotocol (NTP) of 'precision time protocol' (PTP) behoren te worden gebruikt om klokken in een computernetwerk gesynchroniseerd te houden met een referentieklok.

De organisatie kan twee externe tijdsbronnen tegelijk gebruiken om de betrouwbaarheid van externe klokken te verbeteren en naar behoren om te gaan met eventuele afwijkingen.

Klokken kunnen lastig te synchroniseren zijn wanneer meerdere clouddiensten worden gebruikt of wanneer zowel cloud- als op locatie gehoste diensten worden gebruikt. In dat geval behoort de klok van elke dienst te worden gecontroleerd en het verschil te worden geregistreerd om risico's als gevolg van verschillen te verkleinen.

### Overige informatie

De correcte instelling van computerklokken is belangrijk om de nauwkeurigheid van logbestanden van gebeurtenissen te waarborgen. Dit kan nodig zijn voor onderzoeken of als bewijs in juridische en disciplinaire zaken. Onnauwkeurige auditlogbestanden kunnen dergelijke onderzoeken belemmeren en de geloofwaardigheid van het bewijs schaden.

## 8.18 Gebruik van speciale systeemhulpmiddelen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem- _en_netwerkbeveiliging #Veilige_configuratie #Toepassingsbeveiliging	#Bescherming

### Beheersmaatregel

Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.

### Doel

Bewerkstelligen dat het gebruik van systeemhulpmiddelen geen schade toebrengt aan systeem- en toepassingsbeheersmaatregelen voor informatiebeveiliging.

### Richtlijn

Voor het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoren de volgende richtlijnen te worden overwogen:

- beperking van het gebruik van systeemhulpmiddelen tot het laagste aantal betrouwbare bevoegde gebruikers dat praktisch haalbaar is (zie 8.2);
- het gebruik van identificatie-, authenticatie- en autorisatieprocedures voor systeemhulpmiddelen, met inbegrip van de unieke identificatie van de persoon die het systeemhulpmiddel gebruikt;
- het definiëren en documenteren van autorisatieniveaus voor systeemhulpmiddelen;
- autorisatie voor ad-hocgebruik van systeemhulpmiddelen;
- het niet beschikbaar stellen van systeemhulpmiddelen aan gebruikers die toegang hebben tot toepassingen op systemen waarbij segmentatie van functies vereist is;
- het verwijderen of onbruikbaar maken van alle onnodige systeemhulpmiddelen;
- ten minste een logische segmentatie tussen systeemhulpmiddelen en toepassingssoftware. Indien mogelijk, de netwerkcommunicatie voor dergelijke systeemhulpmiddelen van het toepassingsverkeer scheiden;
- beperking van de beschikbaarheid van systeemhulpmiddelen (bijv. voor de duur van een geautoriseerde wijziging);
- registreren van alle gebruik van systeemhulpmiddelen.

### Overige informatie

De meeste informatiesystemen hebben een of meer systeemhulpmiddelen die systeem- en toepassingsbeheersmaatregelen kunnen omzeilen, bijvoorbeeld diagnose-, patching-, antivirus-, schijfdefragmentatie-, probleemdetectie- en probleemoplossings-, back-up- en netwerk hulpmiddelen.

## 8.19 Installeren van software op operationele systemen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie #Toepassingsbeveiliging	#Bescherming

### Beheersmaatregel

Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.

### Doel

De integriteit van operationele systemen garanderen en voorkomen dat misbruik wordt gemaakt van technische kwetsbaarheden.

### Richtlijn

De volgende richtlijnen behoren in overweging te worden genomen om wijzigingen en de installatie van software op operationele systemen op beveiligde wijze te beheren:

- a) updates van operationele software alleen laten uitvoeren door daartoe opgeleide beheerders met passende beheerdersrechten (zie 8.5);
- b) garanderen dat er alleen goedgekeurde uitvoerbare code, en geen ontwikkelcode of compilers, op operationele systemen wordt geïnstalleerd;
- c) software pas installeren en updaten na uitgebreide en geslaagde tests (zie 8.29 en 8.31);
- d) alle bijbehorende programmabronbibliotheken updaten;
- e) een configuratiebeheerssysteem gebruiken om alle operationele software en systeemdocumentatie te beheersen;
- f) een roll-backstrategie definiëren alvorens wijzigingen te implementeren;
- g) een auditlogbestand bijhouden van alle updates van operationele software;
- h) oude versies van software, samen met alle vereiste informatie en parameters, procedures, configuratiedetails archiveren en software als noodmaatregel ondersteunen zolang de software nodig is om gearchiveerde gegevens te lezen of te verwerken.

Bij beslissingen om te upgraden naar een nieuwe versie behoort rekening te worden gehouden met de bedrijfseisen die gelden voor de verandering en de veiligheid van de versie (bijv. de introductie van nieuwe informatiebeveiligingsfunctionaliteit of het aantal en de ernst van kwetsbaarheden in de informatiebeveiliging die zich bij de huidige versie voordoen). Softwarepatches behoren te worden toegepast als ze kunnen bijdragen aan het verwijderen of verminderen van kwetsbaarheden in de informatiebeveiliging (zie 8.8 en 8.19).

Computersoftware kan gebruikmaken van extern geleverde software en pakketten (bijv. softwareprogramma's met modules die op externe locaties worden gehost). Deze behoren te worden

gemonitord en beheerst om ongeautoriseerde wijzigingen te vermijden omdat ze tot kwetsbaarheden in de informatiebeveiliging kunnen leiden.

Software van leveranciers die in productiesystemen wordt gebruikt, behoort te worden onderhouden op een niveau dat door de leverancier wordt ondersteund. Na verloop van tijd zullen softwareleveranciers stoppen met het ondersteunen van oudere softwareversies. De organisatie behoort de risico's van het gebruiken van niet-ondersteunde software te overwegen. In operationele systemen toegepaste opensourcesoftware behoort op de stand van de meest recente geschikte uitgave van de software te worden onderhouden. Het is mogelijk dat opensourcecode na verloop van tijd niet meer wordt onderhouden, maar nog steeds beschikbaar is in een opensourcesoftwarebewaarplaats. De organisatie behoort ook rekening te houden met de risico's van het in operationele systemen gebruiken van opensourcesoftware die niet meer wordt onderhouden.

Wanneer leveranciers betrokken zijn bij het installeren of updaten van software, behoort fysieke of logische toegang alleen te worden verleend wanneer dat nodig is en met passende autorisatie. De activiteiten van de leverancier behoren te worden gemonitord (zie 5.22).

De organisatie behoort strikte regels te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers kunnen installeren.

Het beginsel van het 'least privilege' (minste voorrechten) behoort te worden toegepast op de installatie van software op operationele systemen. De organisatie behoort vast te leggen welke soorten software mogen worden geïnstalleerd (bijv. updates en beveiligingspatches voor bestaande software) en welke verboden zijn (bijv. software uitsluitend voor persoonlijk gebruik en software waarvan de herkomst met betrekking tot de potentiële kwaadaardigheid onbekend of verdacht is). Deze voorrechten behoren te worden verleend op basis van de rollen van de betrokken gebruikers.

#### Overige informatie

Geen overige informatie.

### 8.20 Beveiliging netwerkcomponenten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem- _en_netwerkbeveiliging	#Bescherming

#### Beheersmaatregel

Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.

#### Doel

Informatie in netwerken en de ondersteunende informatieverwerkingsfaciliteiten beschermen tegen compromittering via het netwerk.

## **Richtlijn**

Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en aangesloten diensten tegen onbevoegde toegang te beschermen. In het bijzonder behoort met de volgende aspecten rekening te worden gehouden:

- a) het soort informatie dat het netwerk kan ondersteunen en het classificatieniveau ervan;
- b) verantwoordelijkheden en procedures voor het beheer van netwerkapparatuur en apparaten vaststellen;
- c) actuele documentatie onderhouden, waaronder netwerkschema's en configuratiebestanden van apparatuur (bijv. routers, switches);
- d) de operationele verantwoordelijkheid voor netwerken scheiden van de operationele activiteiten met de ICT-systemen, al naargelang de situatie (zie 5.3);
- e) beheersmaatregelen vaststellen om de vertrouwelijkheid en integriteit van gegevens die via openbare netwerken of draadloze netwerken circuleren te waarborgen en om de aangesloten systemen en toepassingen te beschermen (zie 5.22, 8.24, 5.14 en 6.6). Er kunnen ook aanvullende beheersmaatregelen vereist zijn om de beschikbaarheid van de netwerkdiensten en aan het netwerk aangesloten computers in stand te houden;
- f) op passende wijze logbestanden bijhouden en monitoring uitvoeren om het registreren en detecteren van acties die van invloed kunnen zijn op of relevant zijn voor informatiebeveiliging, mogelijk te maken (zie 8.16 en 8.15);
- g) netwerkbeheeractiviteiten nauwgezet coördineren, zowel om de dienstverlening voor de organisatie te optimaliseren als om te waarborgen dat beheersmaatregelen consistent in de hele informatieverwerkende infrastructuur worden toegepast;
- h) systemen op het netwerk authenticeren;
- i) de verbinding van systemen met het netwerk beperken en filteren (bijv. door gebruik te maken van firewalls);
- j) de verbinding van apparatuur en apparaten met het netwerk detecteren, beperken en authenticeren;
- k) hardening van netwerkapparatuur;
- l) netwerkbeheerkanalen van ander netwerkverkeer scheiden;
- m) kritieke subnetwerken tijdelijk isoleren (bijv. met 'drawbridges' (ophaalbruggen)) als het netwerk wordt aangevallen;
- n) kwetsbare netwerkprotocollen uitschakelen.

De organisatie behoort te garanderen dat passende beveiligingsbeheersmaatregelen worden toegepast op het gebruik van gevirtualiseerde netwerken. Onder gevirtualiseerde netwerken vallen ook softwaregedefinieerde netwerken (SDN, SD-WAN). Vanuit beveiligingsoogpunt kunnen gevirtualiseerde netwerken wenselijk zijn, omdat ze een logische segmentatie mogelijk maken van de communicatie die over fysieke netwerken plaatsvindt, met name voor systemen en toepassingen die met behulp van 'distributed computing' (gedistribueerd rekenen) worden geïmplementeerd.

## Overige informatie

Aanvullende informatie over netwerkbeveiliging is te vinden in de ISO/IEC 27033-reeks.

Meer informatie over gevirtualiseerde netwerken is te vinden in ISO/IEC TS 23167.

## 8.21 Beveiliging van netwerkdiensten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming

### Beheersmaatregel

Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord.

### Doel

De beveiliging bij het gebruik van netwerkdiensten waarborgen.

### Richtlijn

De beveiligingsmaatregelen die nodig zijn voor bepaalde diensten, zoals beveiligingskenmerken, dienstverleningsniveaus en -eisen, behoren te worden vastgesteld en geïmplementeerd (door interne of externe aanbieders van netwerkdiensten). De organisatie behoort ervoor te zorgen dat aanbieders van netwerkdiensten deze maatregelen implementeren.

De kundigheid van de aanbieder van de netwerkdienst om de overeengekomen diensten veilig te beheren, behoort te worden vastgesteld en regelmatig te worden gemonitord. Het recht om een audit uit te voeren behoort te worden overeengekomen tussen de organisatie en de aanbieder. De organisatie behoort ook door dienstverleners verstrekte attesten van derden in aanmerking te nemen om aan te tonen dat zij passende beveiligingsmaatregelen handhaven.

Er behoren regels over het gebruik van netwerken en netwerkdiensten te worden opgesteld en geïmplementeerd. Deze behoren het volgende af te dekken:

- a) de netwerken en netwerkdiensten waartoe toegang wordt verleend;
- b) eisen voor authenticatie voor de toegang tot de verschillende netwerkdiensten;
- c) autorisatieprocedures om vast te stellen wie toegang krijgt tot welk netwerk en welke netwerkdiensten;
- d) netwerkbeheer- en technologische beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en -diensten te beschermen;
- e) de middelen die worden gebruikt om toegang te krijgen tot netwerken en netwerkdiensten [bijv. het gebruik van een virtueel privénetwerk (VPN) of draadloos netwerk];
- f) tijdstip, locatie en andere attributen van de gebruiker op het tijdstip van de toegang;
- g) monitoren van het gebruik van netwerkdiensten.

De volgende beveiligingskenmerken van netwerkdiensten behoren in overweging te worden genomen:

- a) technologie die wordt toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, codering en beheersmaatregelen voor netwerkverbinding;
- b) technische parameters die nodig zijn voor een veilige verbinding met de netwerkdiensten, in overeenstemming met de regels voor beveiliging en netwerkverbinding;
- c) 'caching' (bijv. in een 'content delivery network') en de parameters daarvan die gebruikers in staat stellen het gebruik van 'caching' te kiezen overeenkomstig de prestatie-, beschikbaarheids- en vertrouwelijkheidseisen;
- d) procedures voor het gebruik van netwerkdiensten ter beperking van toegang tot netwerkdiensten of, voor zover noodzakelijk, -toepassingen.

### Overige informatie

Tot netwerkdiensten behoren het leveren van aansluitingen, particuliere netwerkdiensten en beheerde netwerkbeveiligingsoplossingen zoals firewalls en inbraakdetectiesystemen. Deze diensten kunnen variëren van eenvoudige onbeheerde bandbreedte tot en met complexe aanbiedingen met toegevoegde waarde.

Verdere richtlijnen over een kader voor toegangsbeheer worden gegeven in ISO/IEC 29146.

## 8.22 Netwerksegmentatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming

### Beheersmaatregel

Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.

### Doel

Het netwerk opsplitsen met beveiligingsgrenzen en het verkeer ertussen op basis van de bedrijfsbehoeften beheersen.

### Richtlijn

De organisatie behoort te overwegen de beveiliging van grote netwerken te beheren door ze te verdelen in gesegmenteerde netwerkdomeinen en ze van het openbare netwerk (d.w.z. internet) te segmenteren. De domeinen kunnen worden gekozen op basis van betrouwbaarheids-, kritikaliteits- en gevoeligheidsniveaus (bijv. openbaar toegankelijk domein, bureaubladdomein, serverdomein, systemen met laag of hoog risico), op basis van organisatieafdelingen (bijv. personeelszaken, financiën, marketing) of een combinatie ervan (bijv. serverdomein verbonden met meerdere afdelingen van de organisatie). De segmentering kan tot stand worden gebracht door hetzij fysiek verschillende netwerken, hetzij verschillende logische netwerken te gebruiken.

De buitengrenzen van elk domein behoren goed te worden gedefinieerd. Indien toegang tussen netwerkdomeinen is toegelaten, behoort dit bij de buitengrenzen te worden beheerst door een gateway te gebruiken (bijv. een firewall, een filterende router). De criteria voor het segmenteren van netwerken in domeinen, en de toegang die via de gateways wordt toegestaan, behoren te worden gebaseerd op een beoordeling van de beveiligingseisen voor elk domein. De beoordeling behoort in overeenstemming te zijn met het onderwerpspecifieke toegangsbeveiligingsbeleid (zie 5.15), de toegangseisen, waarde en classificatie van verwerkte informatie en behoort rekening te houden met de relatieve kosten en de gevolgen voor de prestaties van het integreren van gatewaytechnologie.

Draadloze netwerken vereisen een speciale behandeling in verband met de slecht gedefinieerde buitengrenzen van het netwerk. Aanpassing van de radiodekking behoort te worden overwogen om draadloze netwerken te segmenteren. Voor gevoelige omgevingen behoort te worden overwogen om elke draadloze toegang te behandelen als externe verbinding en om deze toegang te segmenteren van interne netwerken totdat de toegang een gateway is gepasseerd, in overeenstemming met de netwerkbeheersmaatregelen (zie 8.20), alvorens toegang tot interne systemen wordt verleend. Draadloze toegangsnetwerken voor gasten behoren te worden gescheiden van die voor personeel, indien personeel alleen beheerste 'endpoint devices' gebruikt die voldoen aan de onderwerpspecifieke beleidsregels van de organisatie. Voor wifi voor gasten behoren ten minste dezelfde beperkingen te gelden als voor wifi voor personeel; zo wordt het gebruik van wifi voor gasten door het personeel ontmoedigd.

### Overige informatie

Netwerken strekken zich vaak uit tot buiten de muren van de organisatie omdat bedrijfsmatige partnerschappen worden gevormd waarvoor onderlinge verbinding of het delen van informatieverwerkende en netwerkfaciliteiten vereist is. Door dergelijke uitbreidingen kan het risico op onbevoegde toegang tot de informatiesystemen van de organisatie die gebruikmaken van het netwerk toenemen, waarbij sommige gevoelige en essentiële informatiesystemen bescherming tegen andere netwerkgebruikers nodig hebben.

## 8.23 Toepassen van webfilters

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem- en netwerkbeveiliging	#Bescherming

### Beheersmaatregel

De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.

### Doel

Systemen beschermen om te voorkomen dat ze door malware worden gecompromitteerd en om toegang tot ongeoorloofde internetbronnen te voorkomen.

### Richtlijn

De organisatie behoort de risico's te beperken dat haar personeel toegang krijgt tot websites die illegale informatie bevatten of waarvan bekend is dat ze virussen of phishingmateriaal bevatten. Een techniek om dit te bereiken is het IP-adres of het domein van de desbetreffende website(s) te

blokkeren. Bepaalde browsers en antimalwaretechnologieën doen dit automatisch of kunnen hiervoor worden geconfigureerd.

De organisatie behoort te identificeren tot welke soorten websites haar personeel wel of niet toegang behoort te hebben. De organisatie behoort te overwegen de toegang tot de volgende soorten websites te blokkeren:

- a) websites met een functie voor het uploaden van informatie, tenzij dit om geldige zakelijke redenen is toegestaan;
- b) websites waarvan bekend is of die ervan verdacht worden kwaadaardig te zijn (bijvoorbeeld websites die malware of phishinginhoud verspreiden);
- c) command-and-controlservers;
- d) websites die volgens informatie en analyses over dreigingen kwaadaardig zijn (zie 5.7);
- e) websites die illegale inhoud delen.

Alvorens deze beheersmaatregel in te zetten, behoort de organisatie regels op te stellen voor veilig en gepast gebruik van online bronnen, met inbegrip van een eventuele beperking van ongewenste of ongepaste websites en internetgebaseerde toepassingen. De regels behoren actueel te worden gehouden.

Het personeel behoort training te krijgen over het beveiligde en passende gebruik van online middelen, met inbegrip van toegang tot internet. De training behoort onder andere in te gaan op de regels van de organisatie, het contactpunt voor het melden van veiligheidskwesties en de uitzonderingsprocedure wanneer toegang tot online middelen waarvoor beperkingen gelden om legitieme zakelijke redenen nodig is. Er behoort ook training aan het personeel te worden gegeven om te garanderen dat ze browsermeldingen die aangeven dat een website niet veilig is, maar waarbij de gebruiker wel kan doorgaan, niet in de wind slaan.

### Overige informatie

Allerlei technieken kunnen worden gebruikt om webfilters toe te passen, zoals onder andere handtekeningen, heuristiek, een lijst van aanvaardbare websites of domeinen, een lijst van verboden websites of domeinen en configuratie op maat om te helpen voorkomen dat kwaadaardige software en andere kwaadaardige activiteiten het netwerk en de systemen van de organisatie aanvallen.

## 8.24 Gebruik van cryptografie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming

### Beheersmaatregel

Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.

## Doel

Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.

## Richtlijn

### Algemeen

Het volgende behoort te worden overwogen bij het gebruik van cryptografie:

- a) het door de organisatie gedefinieerde onderwerpspecifieke beleid inzake cryptografie, met inbegrip van de algemene principes voor de bescherming van informatie. Een onderwerpspecifiek beleid voor het gebruik van cryptografie is nodig om de voordelen van het gebruik van cryptografische technieken zo groot mogelijk en de risico's zo klein mogelijk te maken en om ongepast en onjuist gebruik te voorkomen;
- b) het vereiste beschermingsniveau en de classificatie van de informatie identificeren en vervolgens het vereiste type cryptografische algoritmen en de vereiste sterkte en kwaliteit ervan vaststellen;
- c) het gebruik van cryptografie voor het beschermen van informatie op mobiele 'endpoint devices' van gebruikers of opslagmedia en van informatie die via netwerken naar dergelijke apparaten of opslagmedia wordt verzonden;
- d) de aanpak van sleutelbeheer, waaronder methoden voor het genereren en beschermen van cryptografische sleutels en het herstel van versleutelde informatie in geval sleutels verloren gaan of gecompromitteerd of beschadigd raken;
- e) rollen en verantwoordelijkheden voor:
  - 1) het implementeren van de regels voor doeltreffend gebruik van cryptografie;
  - 2) het sleutelbeheer, waaronder het aanmaken van sleutels (zie 8.24);
- f) de toe te passen normen, evenals cryptografische algoritmen, de sterkte van code, cryptografische oplossingen en gebruikspraktijken die zijn goedgekeurd of vereist voor gebruik in de organisatie;
- g) de impact van het gebruik van versleutelde informatie op beheersmaatregelen die zijn gebaseerd op controle van de inhoud (bijv. detectie van malware of het filteren van inhoud).

Bij het implementeren van de regels van de organisatie voor het doeltreffende gebruik van cryptografie behoort rekening te worden gehouden met de regelgeving en nationale beperkingen die van toepassing kunnen zijn op het gebruik van cryptografische technieken in verschillende delen van de wereld, evenals met problemen met grensoverschrijdende stromen van versleutelde informatie (zie 5.31).

De inhoud van dienstverleningsovereenkomsten of contracten met externe leveranciers van cryptografische diensten (bijv. met een certificerende instantie) behoort aansprakelijkheid, betrouwbaarheid van dienstverlening en responstijden voor dienstverlening te omvatten (zie 5.22).

### Sleutelbeheer

Passend sleutelbeheer vereist nauwkeurige procedures voor het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van cryptografische sleutels.

Een sleutelbeheersysteem behoort te zijn gebaseerd op een overeengekomen pakket van normen, procedures en beveiligingsmethoden voor:

- a) het aanmaken van sleutels voor verschillende cryptografische systemen en verschillende toepassingen;
- b) het verstrekken en verkrijgen van openbare sleutelcertificaten;
- c) het verspreiden van sleutels onder de beoogde entiteiten en een instructie hoe de sleutels na ontvangst kunnen worden geactiveerd;
- d) het opslaan van sleutels en de wijze waarop bevoegde gebruikers toegang tot sleutels krijgen;
- e) het wijzigen of updaten van sleutels, met inbegrip van regels over wanneer en hoe sleutels behoren te worden gewijzigd;
- f) het omgaan met gecompromitteerde sleutels;
- g) het intrekken van sleutels, met inbegrip van hoe men sleutels kan terugtrekken of deactiveren [bijv. als sleutels zijn gecompromitteerd of als een gebruiker de organisatie verlaat (in welk geval sleutels ook behoren te worden gearchiveerd)];
- h) het herstellen van sleutels die verloren of gecorrumpeerd zijn;
- i) het back-uppen of archiveren van sleutels;
- j) het vernietigen van sleutels;
- k) het registreren en auditen van aan sleutelbeheer gerelateerde activiteiten;
- l) het instellen van activerings- en deactiveringstijdstippen voor sleutels zodat de sleutels alleen kunnen worden gebruikt voor de tijdsduur overeenkomstig de regels voor sleutelbeheer van de organisatie;
- m) het omgaan met rechtsverzoeken om toegang tot cryptografische sleutels (er kan bijvoorbeeld worden geëist dat versleutelde informatie in onversleutelde vorm beschikbaar wordt gesteld als bewijs in een rechtszaak).

Alle cryptografische sleutels behoren te worden beschermd tegen aanpassing en verlies. Bovendien hebben geheime en particuliere sleutels bescherming nodig tegen onbevoegd gebruik en tegen openbaarmaking. Apparatuur die wordt gebruikt om sleutels aan te maken, op te slaan en te archiveren, behoort fysiek te worden beschermd.

Naast integriteit behoort voor veel usecases aandacht te worden besteed aan de authenticiteit van openbare sleutels.

### **Overige informatie**

Voor de authenticiteit van openbare sleutels worden er meestal processen voor het beheer van openbare sleutels toegepast die gebruikmaken van certificaatinstanties en openbare-sleutelcertificaten, maar het is ook mogelijk om hiervoor gebruik te maken van technologieën zoals het toepassen van handmatige processen voor een klein aantal sleutels.

Cryptografie kan worden gebruikt voor verschillende informatiebeveiligingsdoelstellingen, bijvoorbeeld:

- a) vertrouwelijkheid: codering van informatie gebruiken om gevoelige of essentiële informatie, tijdens opslag of verzending, te beschermen;
- b) integriteit of authenticiteit: digitale handtekeningen of authenticatiecodes voor berichten gebruiken om de authenticiteit of integriteit van gevoelige of essentiële informatie tijdens opslag of verzending te verifiëren. Gebruikmaken van algoritmen om de integriteit van bestanden te controleren;
- c) onweerlegbaarheid: cryptografische technieken gebruiken om bewijs te verkrijgen van het al dan niet plaatsvinden van een gebeurtenis of actie;
- d) authenticatie: cryptografische technieken gebruiken ter authenticatie van gebruikers en andere systeemcomponenten die toegang vragen tot of die verrichtingen doen met systeemgebruikers, -entiteiten en -bronnen.

De ISO/IEC 11770-reeks geeft verdere informatie over sleutelbeheer.

## 8.25 Beveiligen tijdens de ontwikkelcyclus

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming

### Beheersmaatregel

Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.

### Doel

Bewerkstelligen dat informatiebeveiliging binnen de veilige ontwikkelcyclus van software en systemen wordt ontworpen en geïmplementeerd.

### Richtlijn

Beveiligd ontwikkelen is een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem. Om dit te bereiken behoort met de volgende aspecten rekening te worden gehouden:

- a) scheiding van ontwikkel-, test- en productieomgevingen (zie 8.31);
- b) richtlijnen betreffende beveiliging in de levenscyclus van systeemontwikkeling:
  - 1) beveiliging in de softwareontwikkelmethodiek (zie 8.28 en 8.27);
  - 2) richtlijnen voor beveiligde codering voor elke programmeertaal die wordt gebruikt (zie 8.28);
- c) beveiligingseisen tijdens de specificatie- en ontwerpfase (zie 5.8);

- d) beveiligingscontrolepunten in projecten (zie 5.8);
- e) het testen van de systemen en de beveiliging, zoals regressietests, codescan- en penetratietests (zie 8.29);
- f) beveiligde bewaarplaatsen voor broncode en configuratie (zie 8.4 en 8.9);
- g) beveiliging in het versiebeheer (zie 8.32);
- h) de vereiste kennis van en opleiding in de beveiliging van toepassingen (zie 8.28);
- i) het vermogen van de ontwikkelaar om kwetsbaarheden te voorkomen, te vinden en te repareren (zie 8.28);
- j) licentie-eisen en alternatieven om kosteneffectieve oplossingen te bewerkstelligen en tegelijkertijd toekomstige licentieproblemen te voorkomen (zie 5.32).

Indien ontwikkelactiviteiten worden uitbesteed, behoort de organisatie zich ervan te vergewissen dat de leverancier voldoet aan de regels van de organisatie voor veilig ontwikkelen (zie 8.30).

### Overige informatie

Ook binnen toepassingen kan ontwikkeling plaatsvinden, zoals binnen kantoortoepassingen, scripting, browsers en databases.

## 8.26 Toepassingsbeveiligingseisen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_net-werkbeveiliging	#Bescherming #Verdediging

### Beheersmaatregel

Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.

### Doel

Garanderen dat alle informatiebeveiligingseisen zijn geïdentificeerd en meegenomen bij het ontwikkelen of aanschaffen van toepassingen.

### Richtlijn

#### Algemeen

Beveiligingseisen voor toepassingen behoren te worden geïdentificeerd en gespecificeerd. Deze eisen worden gewoonlijk aan de hand van een risicobeoordeling vastgesteld. De eisen behoren met ondersteuning van informatiebeveiligingsspecialisten te worden ontwikkeld.

Toepassingsbeveiligingseisen kunnen allerlei onderwerpen betreffen, afhankelijk van het doel van de toepassing.

Toepassingsbeveiligingseisen behoren het volgende te omvatten, al naargelang de situatie:

- a) het niveau van vertrouwen in de identiteit van entiteiten [bijv. via authenticatie (zie 5.17, 8.2 en 8.5)];
- b) het identificeren van het door de toepassing te verwerken soort informatie en het classificatieniveau ervan;
- c) de noodzaak van segmentatie van toegang en het niveau van toegang tot gegevens en functies in de toepassing;
- d) weerstand tegen kwaadaardige aanvallen of onbedoelde verstoringen [bijv. bescherming tegen bufferoverflow of SQL-injecties];
- e) wettelijke, statutaire en regelgevende eisen in het rechtsgebied waar de transactie wordt gegenereerd, verwerkt, voltooid of opgeslagen;
- f) de noodzaak van privacy met betrekking tot alle betrokken partijen;
- g) de eisen ten aanzien van bescherming van vertrouwelijke informatie;
- h) bescherming van gegevens tijdens de verwerking, tijdens het transport en in ruste;
- i) de noodzaak om communicatie tussen alle betrokken partijen op beveiligde wijze te versleutelen;
- j) inputbeheersmaatregelen, waaronder integriteitscontroles en validatie van de invoer;
- k) geautomatiseerde beheersmaatregelen (bijv. goedkeuringslimieten of dubbele goedkeuring);
- l) outputbeheersmaatregelen, waarbij ook wordt nagedacht over wie er toegang kan hebben tot output en de autorisatie ervoor;
- m) beperkingen met betrekking tot de inhoud van 'vrije tekstvelden', aangezien deze kunnen leiden tot ongecontroleerde opslag van vertrouwelijke gegevens (bijv. persoonsgegevens);
- n) eisen die zijn afgeleid van het bedrijfsproces, zoals registreren en monitoren van transacties, eisen voor onweerlegbaarheid;
- o) eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging (bijv. interfaces voor het registreren en monitoren of systemen voor het detecteren van lekken van gegevens);
- p) het afhandelen van foutmeldingen.

#### Transactionele diensten

In aanvulling hierop behoort voor toepassingen die transactionele diensten tussen de organisatie en een partner aanbieden, het volgende in aanmerking te worden genomen bij het identificeren van informatiebeveiligingseisen:

- a) de mate van vertrouwen die beide partijen eisen van elkaars beweerde identiteit;
- b) de vereiste mate van vertrouwen in de integriteit van informatie die wordt uitgewisseld of verwerkt en de mechanismen voor het identificeren van integriteitsgebreken (bijv. cyclische redundantiecontrole, hashing, digitale handtekeningen);

- c) autorisatieprocedures voor wie de inhoud van belangrijke transactiedocumenten kan goedkeuren, belangrijke transactiedocumenten in circulatie kan brengen of kan ondertekenen;
- d) vertrouwelijkheid, integriteit, bewijs van verzending en ontvangst van belangrijke documenten en de onweerlegbaarheid (bijv. contracten in samenhang met inschrijvings- en contractprocedures);
- e) de vertrouwelijkheid en integriteit van transacties (bijv. orders, gegevens betreffende afleveringsadressen en ontvangstbevestigingen);
- f) eisen ten aanzien van hoelang een transactie vertrouwelijk moet blijven;
- g) verzekerings- en andere contractuele eisen.

#### Toepassingen voor elektronisch bestellen en betalen

In aanvulling hierop behoort het volgende in aanmerking te worden genomen voor toepassingen waarbij er sprake is van elektronisch bestellen en betalen:

- a) eisen om de vertrouwelijkheid en integriteit van orderinformatie in stand te houden;
- b) de mate van verificatie die passend is voor controle van betalingsinformatie die door een klant is verstrekt;
- c) verlies of vermenigvuldiging van transactie-informatie vermijden;
- d) transactiegegevens buiten een publiek toegankelijke omgeving opslaan (bijv. op een opslagplatform op het intranet van de organisatie, in plaats van deze te bewaren en te tonen op direct vanuit internet toegankelijke elektronische opslagmedia);
- e) als een vertrouwde instantie wordt gebruikt (bijv. voor het uitgeven en onderhouden van digitale handtekeningen of digitale certificaten), beveiliging integreren en inbedden in het gehele beheerproces van certificaten of handtekeningen.

Een aantal van de bovengenoemde aspecten kan worden opgepakt door toepassing van cryptografie (zie 8.24), waarbij wettelijke eisen in aanmerking worden genomen (zie 5.31 t/m 5.36, zie in het bijzonder 5.31 voor wetgeving betreffende cryptografie).

#### **Overige informatie**

Toepassingen die toegankelijk zijn via netwerken, staan bloot aan een reeks netwerkgerelateerde dreigingen zoals frauduleuze activiteiten, geschillen over contracten of openbaarmaking van informatie; onvolledige verzending, foutieve routing, ongeautoriseerd(e) wijziging, vermenigvuldiging of afspelen van berichten. Daarom zijn gedetailleerde risicobeoordelingen en zorgvuldige vaststelling van beheersmaatregelen onmisbaar. Vereiste beheersmaatregelen behelzen vaak cryptografische methoden voor het authenticeren en beveiligen van gegevensoverdracht.

Verdere informatie over de beveiliging van toepassingen is te vinden in de ISO/IEC 27034-reeks.

## 8.27 Veilige systeemarchitectuur en technische uitgangspunten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_net-werkbeveiliging	#Bescherming

### Beheersmaatregel

Uitgangspunten voor het ontwerpen van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.

### Doel

Waarborgen dat informatiesystemen veilig worden ontworpen, geïmplementeerd en beheerd binnen de ontwikkelingslevenscyclus.

### Richtlijn

Er behoren uitgangspunten voor het ontwerpen van beveiligde systemen te worden vastgesteld, gedocumenteerd en toegepast voor ontwerpactiviteiten voor informatiesystemen. Bij alle architectuurlagen (bedrijf, gegevens, toepassingen en technologie) behoort beveiliging deel uit te maken van het ontwerp. Nieuwe technologie behoort te worden geanalyseerd op veiligheidsrisico's en het ontwerp behoort te worden beoordeeld aan de hand van bekende aanvalspatronen.

Uitgangspunten voor veilig ontwerpen bieden richtlijnen voor manipulatietechnieken, beheer van beveiligde sessies en gegevensvalidatie en opschoning.

Uitgangspunten voor het ontwerpen van beveiligde systemen behoren een analyse te omvatten van:

- het volledige spectrum van beheersmaatregelen voor beveiliging dat vereist is om informatie en systemen tegen geïdentificeerde dreigingen te beschermen;
- de capaciteit van beveiligingsbeheersmaatregelen om beveiligingsgebeurtenissen te voorkomen, te detecteren of erop te reageren;
- specifieke beveiligingsbeheersmaatregelen die worden vereist door bepaalde bedrijfsprocessen (bijv. het versleutelen van gevoelige informatie, integriteitscontrole en digitale ondertekening van informatie);
- waar en hoe beveiligingsbeheersmaatregelen behoren te worden toegepast (bijv. door ze te integreren met een beveiligingsarchitectuur en de technische infrastructuur);
- hoe individuele beveiligingsbeheersmaatregelen (handmatige en geautomatiseerde) samenwerken om een geïntegreerde verzameling beheersmaatregelen tot stand te brengen.

In de uitgangspunten voor het ontwerpen van beveiligde systemen behoort rekening te worden gehouden met:

- a) de noodzaak van integratie met een beveiligingsarchitectuur;
- b) technische beveiligingsinfrastructuur [bijvoorbeeld openbaresleutelinfrastructuur (PKI), identiteits- en toegangsbeheer (IAM), voorkoming van het lekken van gegevens en dynamisch toegangsbeheer];
- c) de capaciteit van de organisatie om de gekozen technologie te ontwikkelen en te ondersteunen;
- d) de kosten, tijd en complexiteit van het voldoen aan de beveiligingseisen;
- e) 'best practices'.

Het ontwerp van beveiligde systemen behoort gepaard te gaan met:

- a) het gebruik van uitgangspunten voor beveiligingsarchitectuur zoals 'security by design' (beveiliging door ontwerp), 'defence in depth', 'security by default', 'default deny' (standaard weigeren), 'fail securely', 'distrust input from external applications' (input van externe toepassingen wantrouwen), 'security in deployment' (beveiliging tijdens implementatie), 'assume breach' (uitgaan van inbreuk), 'least privilege' (minimaal benodigde rechten), 'usability and manageability' (bruikbaarheid en beheerbaarheid) en 'least functionality' (minimale benodigde functionaliteit);
- b) een beveiligingsgerichte beoordeling van het ontwerp om kwetsbaarheden op het gebied van informatiebeveiliging te helpen detecteren, ervoor te zorgen dat beveiligingsbeheersmaatregelen zijn gespecificeerd en aan de beveiligingseisen te voldoen;
- c) documentatie en formele erkenning van beveiligingsbeheersmaatregelen die niet volledig aan de eisen voldoen (bijv. vanwege dwingende veiligheidseisen);
- d) hardening van systemen.

De organisatie behoort 'zero trust'-beginselen te overwegen zoals:

- a) ervan uitgaan dat er al sprake is van een inbreuk op de informatiesystemen van de organisatie en er daarom niet alleen kan worden vertrouwd op beveiliging van de buitengrenzen van netwerken;
- b) een benadering van 'nooit vertrouwen, altijd verifiëren' hanteren voor toegang tot informatiesystemen;
- c) bewerkstelligen dat verzoeken aan informatiesystemen van begin tot eind versleuteld zijn;
- d) elk verzoek aan een informatiesysteem controleren alsof dit afkomstig is van een open, extern netwerk, zelfs als deze verzoeken intern uit de organisatie afkomstig zijn (d.w.z. niets binnen of buiten de buitengrenzen van de organisatie automatisch vertrouwen);
- e) gebruikmaken van 'least privilege' (minste rechten) en dynamische toegangsbeveiligingstechnieken (zie 5.15, 5.18 en 8.2). Dit omvat het authenticeren en autoriseren van verzoeken om informatie of aan systemen op basis van contextuele informatie zoals authenticatie-informatie (zie 5.17), gebruikersidentiteiten (zie 5.16), gegevens over het 'endpoint device' van de gebruiker, en gegevensclassificatie (zie 5.12);
- f) personen die verzoeken indienen altijd authenticeren en autorisatieverzoeken aan informatiesystemen altijd valideren op basis van informatie, waaronder authenticatie-informatie

(zie 5.17) en gebruikersidentiteiten (5.16), gegevens over het 'endpoint device' van de gebruiker, en gegevensclassificatie (zie 5.12), bijvoorbeeld krachtige authenticatie (bijv. multifactor, zie 8.5) afdwingen.

De vastgestelde uitgangspunten voor het ontwerpen van beveiligde systemen en systeemarchitecturen behoren indien van toepassing te worden toegepast op de uitbestede ontwikkeling van informatiesystemen via de contracten en andere bindende overeenkomsten tussen de organisatie en de leverancier aan wie de organisatie uitbesteedt. De organisatie behoort ervoor te zorgen dat de praktijken van leveranciers voor het ontwerpen van beveiligde systemen aansluiten op de behoeften van de organisatie.

De uitgangspunten voor het ontwerpen van beveiligde systemen en de vastgestelde ontwerpprocedures behoren regelmatig te worden beoordeeld om te waarborgen dat ze doelmatig bijdragen aan verbeterde normen voor beveiliging binnen het ontwerpproces. Ze behoren ook regelmatig te worden beoordeeld om ervoor te zorgen dat ze actueel blijven in de zin dat ze nieuwe potentiële dreigingen afwenden en toepasbaar blijven bij verbeteringen die worden toegepast in de technologieën en oplossingen.

### Overige informatie

Uitgangspunten voor het ontwerpen van beveiligde systemen kunnen worden toegepast op het ontwerp of de configuratie van allerlei technieken, zoals:

- storingstolerantie en andere technieken met het oog op veerkracht;
- segmentatie (bijv. door virtualisatie of containerisatie);
- bestendigheid tegen manipulatie.

Er kunnen technieken voor beveiligde virtualisatie worden gebruikt om interferentie te voorkomen tussen toepassingen die op hetzelfde fysieke apparaat draaien. Als een virtuele instantie van een toepassing door een aanvaller wordt gecompromitteerd, wordt alleen die instantie getroffen. De aanval heeft geen effect op andere toepassingen of gegevens.

Technieken voor weerstand tegen manipulatie kunnen worden gebruikt om manipulatie van informatiecontainers te detecteren, hetzij fysiek (bijv. een inbraakalarm), hetzij logisch (bijv. een gegevensbestand). Een kenmerk van dergelijke technieken is dat de poging om de container te manipuleren, wordt geregistreerd. Bovendien kan de beheersmaatregel voorkomen dat gegevens met succes worden geëxtraheerd door ze te vernietigen (het geheugen van het apparaat kan bijvoorbeeld worden gewist).

## 8.28 Veilig coderen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem- en netwerkbeveiliging	#Bescherming

### Beheersmaatregel

Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling.

## Doel

Waarborgen dat veilige software wordt geschreven waardoor het aantal potentiële informatiebeveiligingskwetsbaarheden in de software wordt beperkt.

## Richtlijn

### Algemeen

De organisatie behoort organisatiebrede processen op te stellen om te voorzien in goede governance voor veilig coderen. Er behoort een minimale nullijn wat betreft beveiliging te worden vastgesteld en toegepast. In aanvulling hierop behoren dergelijke processen en governance te worden uitgebreid tot softwarecomponenten van derden en opensourcesoftware.

De organisatie behoort te monitoren op dreigingen in de echte wereld en actueel advies en actuele informatie over kwetsbaarheden in software als richtlijn om de principes voor veilig coderen van de organisatie door middel van continue verbetering en voortdurend leren te sturen. Dit kan bijdragen aan het garanderen dat er doeltreffende praktijken voor veilig coderen worden geïmplementeerd als tegenhanger tegen het snel veranderende dreigingslandschap.

### Planning en voorafgaand aan het coderen

Principes voor veilig coderen behoren zowel voor nieuwe ontwikkelingen als bij hergebruikscenario's te worden gebruikt. Deze principes behoren te worden toegepast op ontwikkelingsactiviteiten binnen de organisatie en voor producten en diensten die de organisatie aan anderen levert. De planning en de voorwaarden voorafgaand aan het coderen behoren het volgende te omvatten:

- a) organisatiespecifieke verwachtingen en goedgekeurde principes voor veilig coderen die zowel voor interne als voor uitbestede codeontwikkelingen behoren te worden gebruikt;
- b) gebruikelijke en historische codeerpraktijken en -gebreken die tot kwetsbaarheden in de informatiebeveiliging leiden;
- c) ontwikkelinstrumenten, zoals geïntegreerde ontwikkelomgevingen (IDE's), configureren om te helpen het maken van veilige code af te dwingen;
- d) richtlijnen volgen die door de aanbieders van ontwikkelinstrumenten en uitvoeringsomgevingen worden gegeven, al naargelang de situatie;
- e) onderhoud en gebruik van actuele ontwikkelinstrumenten (bijv. compilers);
- f) de kwalificatie van ontwikkelaars voor het schrijven van veilige code;
- g) veilig ontwerp en veilige architectuur, met inbegrip van het opstellen van dreigingsmodellen;
- h) normen voor veilig coderen en waar relevant het gebruik ervan verplicht stellen;
- i) het gebruik van beheerste omgevingen voor ontwikkeling.

Tijdens het coderen

Overwegingen tijdens het coderen behoren te zijn:

- a) veilige coderingspraktijken die specifiek zijn voor de programmeertalen en -technieken die worden gebruikt;
- b) veilige programmeertechnieken gebruiken zoals 'pair programming' (programmeren in duo's), 'refactoring' (code herstructureren), 'peer review' (beoordeling door collega's), beveiligingsiteraties en testgestuurde ontwikkeling;
- c) gestructureerde programmeertechnieken gebruiken;
- d) code documenteren en programmeerfouten verwijderen die anders misbruik van kwetsbaarheden in de informatiebeveiliging mogelijk kunnen maken;
- e) het gebruik van onveilige ontwerpstechnieken (bijvoorbeeld het gebruik van hardgecodeerde wachtwoorden, niet-goedgekeurde codesamples en niet-geauthenticeerde webdiensten) verbieden.

Er behoort tijdens en na het ontwikkelen te worden getest (zie 8.29). Met procedures voor het statisch testen van de beveiliging van toepassingen (SAST) kunnen beveiligingslekken in software worden geïdentificeerd.

Alvorens software operationeel te maken, behoort:

- a) het aanvalsoppervlak en het beginsel van het 'least privilege' (minste voorrechten) te worden geëvalueerd;
- b) een analyse te worden uitgevoerd op de meest voorkomende programmeerfouten en te worden gedocumenteerd dat deze zijn hersteld.

Beoordeling en onderhoud

Nadat de code operationeel is gemaakt:

- a) behoren updates op beveiligde wijze te worden verpakt en ingezet;
- b) behoren gemelde kwetsbaarheden in de informatiebeveiliging te worden opgepakt (zie 8.8);
- c) behoren logbestanden te worden bijgehouden van fouten en vermeende aanvallen en behoren de logbestanden regelmatig te worden beoordeeld om de code zo nodig aan te passen;
- d) behoort de broncode te worden beschermd tegen toegang en manipulatie door onbevoegden (bijv. door gebruik te maken van configuratiebeheerinstrumenten, die meestal functies als toegangsbeveiliging en versiebeheer bieden).

Als er gebruikgemaakt wordt van externe instrumenten en bibliotheken, behoort de organisatie na te denken over:

- a) het bewerkstelligen dat externe bibliotheken worden beheerd (bijv. door een inventarislijst bij te houden van bibliotheken die worden gebruikt en de desbetreffende versies) en regelmatig worden bijgewerkt met releasecycli;
- b) het selecteren, autoriseren en hergebruiken van goed gecontroleerde componenten, met name authenticatie- en cryptografische componenten;

- c) de licentie, beveiliging en historie van externe componenten;
- d) het bewerkstelligen dat software kan worden onderhouden, wordt getraceerd en afkomstig is van beproefde, gerenommeerde bronnen;
- e) het op voldoende lange termijn beschikbaar zijn van ontwikkelmiddelen en artefacten.

Als het nodig is een softwarepakket te wijzigen, behoren de volgende punten in overweging te worden genomen:

- a) het risico dat ingebouwde beheersmaatregelen en integriteitsprocessen gecompromitteerd raken;
- b) of het al dan niet nodig is toestemming van de leverancier te verkrijgen;
- c) de mogelijkheid om de vereiste wijzigingen van de aanbieder als standaard programma-updates te verkrijgen;
- d) de impact als de organisatie verantwoordelijk wordt gehouden voor het toekomstig onderhoud van de software als gevolg van de veranderingen;
- e) compatibiliteit met andere software die in gebruik is.

### **Overige informatie**

Een leidend principe is bewerkstelligen dat beveiligingsrelevante code wordt aangeroepen wanneer dat nodig is en deze bestand is tegen manipulatie. Programma's die worden geïnstalleerd op basis van gecompileerde binaire code hebben deze eigenschappen ook, maar alleen voor gegevens die binnen de toepassing worden bewaard. Voor geïnterpreteerde talen werkt het concept alleen wanneer de code wordt uitgevoerd op een server waartoe de gebruikers en de processen die er gebruik van maken verder geen toegang hebben en de gegevens ervan in een op vergelijkbare wijze beschermde database worden bewaard. De geïnterpreteerde code kan bijvoorbeeld worden uitgevoerd op een clouddienst waar beheerdersrechten vereist zijn voor toegang tot de code op zich. Dergelijke toegang door een beheerder behoort te worden beschermd door beveiligingsmechanismen zoals just-in-timebeheerprincipes en krachtige authenticatie. Indien de eigenaar van een toepassing op afstand via de server toegang kan maken tot scripts, kan een aanvalder dat in principe ook. Webservers behoren dusdanig te worden geconfigureerd dat het doorzoeken van directory's in dergelijke gevallen niet mogelijk is.

Het is het beste om er bij het ontwerpen van een toepassingscode vanuit te gaan dat deze code altijd het doelwit is van aanvallen, als gevolg van fouten of door kwaadwillige opzet. Bovendien kunnen kritische toepassingen zo worden ontworpen dat ze bestand zijn tegen interne fouten of storingen. Zo kan bijvoorbeeld de output van een complex algoritme worden gecontroleerd om te garanderen dat deze binnen veilige grenzen ligt voordat de gegevens worden gebruikt in een toepassing zoals een veiligheids- of financieel kritische toepassing. De code die de grenscontroles uitvoert, is eenvoudig en daarom veel gemakkelijker om de juistheid ermee aan te tonen.

Bepaalde internettoepassingen zijn gevoelig voor allerlei kwetsbaarheden die worden veroorzaakt door slecht ontwerp en slecht coderen, zoals injectieaanvallen op databases en 'cross-site scripting'-aanvallen. Bij deze aanvallen kunnen verzoeken worden gemanipuleerd om misbruik te maken van de webserverfunctionaliteit.

Meer informatie over het evalueren van ICT-beveiliging is te vinden in de ISO/IEC 15408-reeks.

## 8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Toepassingsbeveiliging #Borging_van_informatiebeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming

### Beheersmaatregel

Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.

### Doel

Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.

### Richtlijn

Nieuwe informatiesystemen, upgrades en nieuwe versies behoren tijdens de ontwikkelingsprocessen grondig te worden getest en geverifieerd. Het testen van de beveiliging behoort een integraal onderdeel te zijn van het testen voor systemen of componenten.

Het testen van de beveiliging behoort te worden uitgevoerd aan de hand van een verzameling eisen die als functioneel of niet-functioneel kunnen worden uitgedrukt. Het testen van de beveiliging behoort het testen te omvatten van:

- beveiligingsfuncties [bijv. authenticatie van gebruikers (zie 8.5), toegangsbeperking (zie 8.3) en het gebruik van cryptografie (zie 8.24)];
- veilig coderen (zie 8.28);
- beveiligde configuraties (zie 8.9, 8.20 en 8.22) waaronder die van besturingssystemen, firewalls en andere beveiligingscomponenten.

Testplannen behoren met behulp van een verzameling criteria te worden vastgesteld. De omvang van de tests behoort in verhouding te staan tot het belang, de aard van het systeem en de mogelijke impact van de verandering die wordt ingevoerd. Het testplan behoort het volgende te omvatten:

- een gedetailleerd schema van de activiteiten en tests;
- input en verwachte output onder allerlei omstandigheden;
- criteria om de resultaten te evalueren;
- een besluit over verdere acties naarmate nodig is.

De organisatie kan geautomatiseerde instrumenten inzetten zoals instrumenten om codes te analyseren of om op kwetsbaarheden te scannen, en behoort het herstel van beveiligingsgerelateerde tekortkomingen te verifiëren.

Voor interne ontwikkelactiviteiten behoren dergelijke tests in eerste instantie te worden uitgevoerd door het ontwikkelteam. Vervolgens behoren onafhankelijke tests te worden uitgevoerd om te bewerkstelligen dat het systeem uitsluitend werkt zoals voorzien (zie 5.8). Het volgende behoort te worden overwogen:

- a) het uitvoeren van activiteiten om code te beoordelen als relevant element voor het testen op zwakke plekken in de beveiliging, met inbegrip van onvoorziene inputs en omstandigheden;
- b) het scannen op kwetsbaarheden om onveilige configuraties en kwetsbaarheden in systemen te identificeren;
- c) het uitvoeren van penetratietests om onveilige code en ontwerpen te identificeren.

Voor uitbestede ontwikkeling en het inkopen van componenten behoort een verwervingsprocedure te worden gevolgd. In de contracten met de leverancier behoren de vastgestelde beveiligingseisen te zijn opgenomen (zie 5.20). Voordat producten en diensten worden gekocht, behoren ze te worden geëvalueerd tegen deze criteria.

Tests behoren te worden uitgevoerd in een testomgeving die zo nauwkeurig mogelijk overeenkomt met de doelproductieomgeving om te bewerkstelligen dat het systeem geen kwetsbaarheden introduceert in de omgeving van de organisatie en dat de tests betrouwbaar zijn (zie 8.31).

### Overige informatie

Er kunnen meer testomgevingen worden opgezet die gebruikt kunnen worden voor verschillende soorten tests (bijv. functionele en prestatietests). Deze verschillende omgevingen kunnen virtueel zijn, met individuele configuraties om allerlei verschillende bedrijfsomgevingen te simuleren.

Het testen en monitoren van testomgevingen, -instrumenten en -technologieën behoort ook te worden overwogen om doeltreffend testen te bewerkstelligen. Dezelfde overwegingen gelden voor het monitoren van de monitoringsystemen die worden ingezet in ontwikkel-, test- en productieomgevingen. Aan de hand van de gevoeligheid van de systemen en gegevens behoort te worden beoordeeld hoeveel lagen metatests zinvol zijn.

## 8.30 Uitbestede systeemontwikkeling

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Detecteren	#Systeem-_en_netwerk-beveiliging #Toepassingsbeveiliging #Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming

### Beheersmaatregel

De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.

### Doel

Garanderen dat de door de organisatie vereiste informatiebeveiligingsmaatregelen bij uitbestede systeemontwikkeling worden geïmplementeerd.

## Richtlijn

Als systeemontwikkeling wordt uitbesteed, behoort de organisatie eisen en verwachtingen te communiceren en overeen te komen en voortdurend te monitoren, en te beoordelen of de levering van uitbesteed werk aan deze verwachtingen voldoet. De volgende punten behoren in de gehele externe toeleveringsketen van de organisatie in overweging te worden genomen:

- a) licentieovereenkomsten, eigendom van de broncode en intellectuele-eigendomsrechten in verband met de uitbesteede inhoud (zie 5.32);
- b) contractuele eisen voor beveiligde ontwikkel-, coderings- en testpraktijken (zie 8.25 t/m 8.29);
- c) het door externe ontwikkelaars in aanmerking te nemen dreigingsmodel aanleveren;
- d) acceptatietests voor de kwaliteit en nauwkeurigheid van de leveringen (zie 8.29);
- e) bewijs leveren dat de beveiligings- en privacycapaciteiten aan een minimaal aanvaardbaar niveau voldoen (bijv. borgingsverslagen);
- f) bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de (zowel opzettelijke als onbedoelde) aanwezigheid van kwaadaardige inhoud op het tijdstip van levering;
- g) bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de aanwezigheid van bekende kwetsbaarheden;
- h) escrowovereenkomsten voor de broncode van het systeem (bijv. indien de leverancier failliet gaat);
- i) contractueel recht om ontwikkelprocessen en beheersmaatregelen te auditen;
- j) beveiligingseisen voor de ontwikkelomgeving (zie 8.31);
- k) rekening houden met toepasselijke wetgeving (bijv. inzake de bescherming van persoonsgegevens).

## Overige informatie

Verdere informatie over leveranciersrelaties is te vinden in de ISO/IEC 27036-reeks.

### 8.31 Scheiding van ontwikkel-, test- en productieomgevingen

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem_en_netwerkbeveiliging	#Bescherming

## Beheersmaatregel

Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.

## Doel

De productieomgeving en de gegevens beschermen tegen compromittering door ontwikkel- en testactiviteiten.

## **Richtlijn**

Het scheidingsniveau tussen productie-, test- en ontwikkelomgevingen dat nodig is om operationele problemen te voorkomen, behoort te worden geïdentificeerd en geïmplementeerd.

Met de volgende aspecten behoort rekening te worden gehouden:

- a) ontwikkel- en productiesystemen in afdoende mate van elkaar scheiden en ze in verschillende domeinen uitvoeren (bijv. in gescheiden virtuele of fysieke omgevingen);
- b) regels en autorisaties definiëren, documenteren en implementeren voor het inzetten van software vanuit de ontwikkel- naar de productiestatus;
- c) veranderingen aan productiesystemen en toepassingen in een test- of gefaseerde omgeving testen voordat ze in productiesystemen worden toegepast (zie 8.29);
- d) niet testen in productieomgevingen behalve in gedefinieerde en goedgekeurde omstandigheden;
- e) compilers, editors en andere ontwikkelinstrumenten of systeemhulpmiddelen behoren, indien ze niet nodig zijn, niet toegankelijk te zijn vanuit productiesystemen;
- f) passende milieu-identificatielabels in menu's tonen om het risico op fouten te beperken;
- g) geen gevoelige informatie naar de ontwikkel- en testsysteemomgevingen kopiëren tenzij er wordt voorzien in gelijkwaardige beheersmaatregelen voor de ontwikkel- en testsystemen.

In alle gevallen behoren de ontwikkel- en testomgevingen te worden beschermd, waarbij het volgende in aanmerking behoort te worden genomen:

- a) het patchen en bijwerken van alle ontwikkelings-, integratie- en testinstrumenten (met inbegrip van builders, integratie-instrumenten, compilers, configuratiesystemen en bibliotheken);
- b) beveiligde configuratie van systemen en software;
- c) toegangsbeveiliging voor de omgevingen;
- d) monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes;
- e) beveiligde monitoring van de omgevingen;
- f) back-ups maken van de omgevingen.

Het behoort niet mogelijk te zijn dat één persoon zonder voorafgaande beoordeling en goedkeuring veranderingen aan zowel de ontwikkeling als de productie kan doorvoeren. Dit kan bijvoorbeeld worden bereikt door toegangsrechten te scheiden of door middel van regels die worden gemonitord. In uitzonderingssituaties behoren aanvullende maatregelen zoals het bijhouden van gedetailleerde logbestanden en realltime monitoring te worden geïmplementeerd om veranderingen door onbevoegden te detecteren en er actie op te ondernemen.

## **Overige informatie**

Zonder afdoende maatregelen en procedures kunnen ontwikkelaars en testers die toegang hebben tot productiesystemen, aanmerkelijke risico's introduceren (bijv. ongewenste wijziging van bestanden of de systeemomgeving, systeemstoringen, niet-goedgekeurde en niet-geteste code in productiesystemen uitvoeren, openbaarmaking van vertrouwelijke gegevens, en problemen met de integriteit en beschikbaarheid van gegevens). Het is nodig een bekende en stabiele omgeving te onderhouden voor

het uitvoeren van zinvolle tests en om ongepaste toegang van de ontwikkelaar tot de productieomgeving te voorkomen.

Maatregelen en procedures omvatten zorgvuldig ontworpen rollen in combinatie met het implementeren van eisen met betrekking tot de segmentatie van functies en het beschikken over afdoende monitoringprocessen.

Medewerkers die worden ingezet voor ontwikkeling en testen, vormen ook een dreiging voor de vertrouwelijkheid van bedrijfsinformatie. Ontwikkel- en testactiviteiten kunnen onbedoelde veranderingen aan software of informatie veroorzaken als ze dezelfde informatieverwerkende omgeving delen. Het is daarom wenselijk om ontwikkel-, test- en productieomgevingen te scheiden, om het risico op onbedoelde verandering of onbevoegde toegang tot productiesoftware en bedrijfsgegevens te verlagen (zie 8.33 voor het beschermen van testinformatie).

In bepaalde gevallen kan het onderscheid tussen ontwikkel-, test- en productieomgevingen opzettelijk worden vervaagd en kan het testen worden uitgevoerd in een ontwikkelomgeving of door middel van beheerste uitrol naar livegebruikers of -servers (bijv. een kleine groep proefgebruikers). In bepaalde gevallen kan het product worden getest door het livegebruik van het product binnen de organisatie. Daarnaast, om uitval van live-implementaties te beperken, kunnen twee identieke productieomgevingen worden ondersteund, waarvan er altijd slechts één live is.

Er zijn ondersteunende processen nodig voor het gebruik van productiegegevens in ontwikkel- en testomgevingen (8.33).

Organisaties kunnen ook de hier gegeven richtlijnen voor trainingsomgevingen bij het trainen van eindgebruikers in aanmerking nemen.

## 8.32 Wijzigingsbeheer

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming

### Beheersmaatregel

Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.

### Doel

De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.

### Richtlijn

Nieuwe systemen en belangrijke wijzigingen aan bestaande systemen behoren volgens overeengekomen regels en een formeel proces van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie te worden geïntroduceerd. Verantwoordelijkheden en procedures voor beheer behoren te worden vastgelegd om afdoende beheersing van alle veranderingen te waarborgen.

Procedures voor wijzigingsbeheer behoren te worden gedocumenteerd en gehandhaafd om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie in informatieverwerkende faciliteiten en informatiesystemen te garanderen gedurende de gehele ontwikkelcyclus van systemen, vanaf het begin van de ontwerpfase tot en met alle daaropvolgende onderhoudsinspanningen.

Waar mogelijk behoren de procedures voor wijzigingsbeheer voor ICT-infrastructuur en -software te worden geïntegreerd.

De procedures voor wijzigingsbeheer behoren het volgende te omvatten:

- a) het plannen en beoordelen van de potentiële impact van wijzigingen, waarbij alle afhankelijkheden in aanmerking worden genomen;
- b) autorisatie van veranderingen;
- c) veranderingen aan relevante belanghebbenden communiceren;
- d) tests en de aanvaarding van tests voor de veranderingen (zie 8.29);
- e) implementatie van veranderingen met inbegrip van inzetplannen;
- f) nood- en voorzorgsoverwegingen, met inbegrip van vangnetprocedures;
- g) registraties onderhouden van veranderingen waarin alle bovenstaande punten worden opgenomen;
- h) waarborgen dat bedieningsdocumentatie (zie 5.37) en gebruikersprocedures indien nodig worden gewijzigd om ze toepasbaar te houden;
- i) bewerkstelligen dat de plannen voor ICT-continuïteit en de respons- en herstelprocedures (zie 5.30) worden gewijzigd naarmate nodig is om passend te blijven.

### **Overige informatie**

Onvoldoende beheersing van veranderingen aan informatieverwerkende faciliteiten en informatiesystemen is een algemene oorzaak van systeem- of beveiligingsfouten. Veranderingen aan de productieomgeving, in het bijzonder als software wordt gemuteerd van de ontwikkelings- naar de uitvoeringsomgeving, kunnen van invloed zijn op de integriteit en beschikbaarheid van toepassingen.

Het wijzigen van software kan van invloed zijn op de productieomgeving en vice versa.

Bij een goede werkwijze wordt het testen van ICT-componenten uitgevoerd in een omgeving die zowel gescheiden is van de productie- als van de ontwikkelomgevingen (zie 8.31). Hierdoor wordt het mogelijk om controle te hebben over nieuwe software en om extra bescherming te bieden voor uitvoeringsinformatie die wordt gebruikt voor testdoeleinden. Dit behoort te gelden voor patches, servicepacks en andere updates.

De productieomgeving omvat besturingssystemen, databases en middlewareplatforms. De controle behoort te worden toegepast voor veranderingen van toepassingen en infrastructuren.

### 8.33 Testgegevens

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit	#Beschermen	#Informatiebescherming	#Bescherming

#### Beheersmaatregel

Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.

#### Doel

De relevantie van het testen en de bescherming van operationele gegevens die voor het testen worden gebruikt, waarborgen.

#### Richtlijn

Testgegevens behoren dusdanig te worden geselecteerd dat de betrouwbaarheid van testresultaten en de vertrouwelijkheid van de relevante operationele gegevens gegarandeerd worden. Er behoren geen gevoelige gegevens (met inbegrip van persoonsgegevens) in de ontwikkel- en testomgevingen te worden gekopieerd (zie 8.31).

De volgende richtlijnen behoren te worden toegepast om de exemplaren of kopieën van operationele gegevens, wanneer deze worden gebruikt voor testdoeleinden, te beschermen, ongeacht of de testomgeving lokaal is gebouwd of zich op een clouddienst bevindt:

- de toegangsbeveiligingsprocedures die worden toegepast op operationele omgevingen, ook op testomgevingen toepassen;
- voor elke keer dat besturingsgegevens naar een testomgeving worden gekopieerd, een afzonderlijke autorisatie verkrijgen;
- logbestanden van het kopiëren en gebruiken van besturingsgegevens bijhouden om in een audittraject te voorzien;
- gevoelige gegevens beschermen door deze te verwijderen of te maskeren (zie 8.11) bij gebruik voor testen;
- operationele gegevens naar behoren uit een testomgeving wissen (zie 8.10) onmiddellijk nadat het testen is afgerond om zo gebruik van testgegevens door onbevoegden te voorkomen.

Testgegevens behoren veilig te worden opgeslagen (om manipulatie te voorkomen, die anders tot ongeldige resultaten kan leiden) en alleen voor testdoeleinden te worden gebruikt.

#### Overige informatie

Systeem- en acceptatietests kunnen substantiële hoeveelheden testgegevens vereisen die een zo getrouw mogelijke weergave zijn van operationele gegevens.

### 8.34 Bescherming van informatiesystemen tijdens audits

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerk-beveiliging #Informatiebescherming	#Governance_en_Ecosysteem #Bescherming

#### Beheersmaatregel

Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.

#### Doel

De impact van audit- en andere borgingsactiviteiten op operationele systemen en bedrijfsprocessen tot een minimum beperken.

#### Richtlijn

De volgende richtlijnen behoren te worden overwogen:

- verzoeken voor toegang tot systemen en gegevens in het kader van audits met de juiste managers overeenkomen;
- de reikwijdte van de technische audits overeenkomen en beheersen;
- audits beperken tot alleen-lezentoegang tot software en gegevens. Indien er geen alleen-lezentoegang beschikbaar is om de nodige informatie te verkrijgen, de test laten uitvoeren door een ervaren beheerder die namens de auditor over de nodige toegangsrechten beschikt;
- indien toegang wordt verleend, de beveiligingseisen (bijv. antivirus en patching) voor de apparatuur die wordt gebruikt voor toegang tot de systemen (bijv. laptops of tablets), vaststellen en verifiëren voordat toegang wordt verleend;
- toegang anders dan 'alleen lezen' alleen toelaten voor geïsoleerde kopieën van systeembestanden, deze wissen als de audit is uitgevoerd of ze voldoende beschermen indien het verplicht is deze bestanden bij de vereiste auditdocumenten te bewaren;
- verzoeken om speciale of extra verwerking, zoals het gebruik van auditinstrumenten, identificeren en hierover overeenstemming bereiken;
- audits die de beschikbaarheid van systemen kunnen beïnvloeden, buiten werkuren laten plaatsvinden;
- alle toegang voor audit- en testdoeleinden monitoren en in logbestanden registreren.

#### Overige informatie

Audits en andere borgingsactiviteiten kunnen ook plaatsvinden op ontwikkel- en testsystemen, waarbij deze tests bijvoorbeeld gevolgen kunnen hebben voor de integriteit van code of ertoe kunnen leiden dat in die omgevingen bewaarde gevoelige informatie openbaar wordt gemaakt.

## Bijlage A (informatief)

### Attributen gebruiken

#### A.1 Algemeen

Deze bijlage geeft een tabel die laat zien hoe attributen kunnen worden gebruikt om verschillende overzichten van de beheersmaatregelen te realiseren. De vijf voorbeelden van het gebruik van deze attributen zijn (zie 4.2):

- a) Typen beheersmaatregel (#Preventief, #Detectief, #Corrigerend)
- b) Informatiebeveiligingseigenschappen (#Vertrouwelijkheid, #Integriteit, #Beschikbaarheid)
- c) Cybersecurityconcepten (#Identificeren, #Beschermen, #Detecteren, #Reageren, #Herstellen)
- d) Operationele capaciteiten (#Governance, #Beheer\_van\_bedrijfsmiddelen, #Informatiebescherming, #Personeelsbeveiliging, #Fysieke\_beveiliging, #Systeem-\_en\_netwerkbeveiliging, #Toepassingsbeveiliging, #Veilige\_configuratie, #Identiteits-\_en\_toegangsbeheer, #Beheer\_van\_dreigingen\_en\_kwetsbaarheden, #Continuïteit, #Beveiliging\_in\_leveranciersrelaties, #Juridisch\_en\_compliance, #Beheer\_van\_informatiebeveiligingsgebeurtenissen, #Borging\_van\_informatiebeveiliging)
- e) Beveiligingsdomeinen (#Governance\_en\_Ecosysteem, #Bescherming, #Verdediging, #Veerkracht)

Tabel A.1 bevat een matrix van alle beheersmaatregelen in dit document met de bijbehorende attribuutwaarden.

De matrix kan worden gefilterd of gesorteerd met behulp van een hulpmiddel zoals een eenvoudige spreadsheet of een database, die nog meer informatie kan bevatten zoals teksten voor beheersmaatregelen, richtlijnen, organisatiespecifieke richtlijnen of attributen (zie A.2).

**Tabel A.1 — Matrix van beheersmaatregelen en attribuutwaarden**

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
5.1	Beleidsregels voor informatie-beveiliging	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Veerkracht
5.2	Rollen en verantwoordelijkheden bij informatie-beveiliging	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht

Identificatie- code beheers- maatregel ISO/IEC 27002: 2022	Naam beheers- maatregel	Type beheers- maatregel	Informatie- beveiligings- eigenschappen	Cybersecurity- concepten	Operationele capaciteiten	Beveiligings- domeinen
5.3	Func-tie-scheiding	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Governance #Identiteits- _en_toegangs- beheer	#Governance_en _Ecosysteem
5.4	Management- verantwoorde- lijkheden	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Governance	#Governance_en _Ecosysteem
5.5	Contact met overheids- instanties	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen #Reageren #Herstellen	#Governance	#Verdediging #Veerkracht
5.6	Contact met speciale belangen- groepen	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Reageren #Herstellen	#Governance	#Verdediging
5.7	Informatie en analyses over dreigingen	#Preventief #Detectief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Detecteren #Reageren	#Beheer_van_ dreigingen_en_ kwetsbaar- heden	#Verdediging #Veerkracht
5.8	Informatie- beveiliging in project- management	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Governance	#Governance_en _Ecosysteem #Bescherming
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmid- delen	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Beheer_van_ bedrijfsmid- delen	#Governance_en _Ecosysteem #Bescherming
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmid- delen	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Beheer_van_be drijfsmiddelen #Informatie- bescherming	#Governance_en _Ecosysteem #Bescherming
5.11	Retourneren van bedrijfsmid- delen	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Beheer_van_ bedrijfsmid- delen	#Bescherming
5.12	Classificeren van informatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Informatie- bescherming	#Bescherming #Verdediging

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
5.13	Labelen van informatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Informatie- bescherming	#Verdediging #Bescherming
5.14	Overdragen van informatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Beheer_van_ bedrijfsmid- delen #Informatie- bescherming	#Bescherming
5.15	Toegangs-beveiliging	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
5.16	Identiteits-beheer	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
5.17	Beheren van authenticatie-informatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
5.18	Toegangs-rechten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
5.19	Informatiebe- veiliging in leveranciers- relaties	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Beveiliging_in_ leveranciers- relaties	#Governance_en _Ecosysteem #Bescherming
5.20	Adresseren van informatiebe- veiliging in leve- ranciersover- eenkomsten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Beveiliging_in_ leveranciers- relaties	#Governance_en _Ecosysteem #Bescherming
5.21	Beheren van informatie- beveiliging in de ICT-keten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Beveiliging_in_ leveranciers- relaties	#Governance_en _Ecosysteem #Bescherming
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciers- diensten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Beveiliging_in_ leveranciers- relaties #Borging_van_ informatie- beveiliging	#Governance_en _Ecosysteem #Bescherming #Verdediging
5.23	Informatiebe- veiliging voor het gebruik van clouddiensten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Beveiliging_in_ leveranciers- relaties	#Governance_en _Ecosysteem #Bescherming

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
5.24	Plannen en voorbereiden van het beheer van informatie-beveiligings-incidenten	#Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Reageren #Herstellen	#Governance #Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.25	Beoordelen van en besluiten over informatie-beveiligings-gebeurtenissen	#Detectief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Detecteren #Reageren	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.26	Reageren op informatie-beveiligings-incidenten	#Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Reageren #Herstellen	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.27	Leren van informatie-beveiligings-incidenten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.28	Verzamelen van bewijsmateriaal	#Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Detecteren #Reageren	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.29	Informatie-beveiliging tijdens een verstoring	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht
5.30	ICT-gereedheid voor bedrijfs-continuïteit	#Corrigerend	#Beschikbaar- heid	#Reageren	#Continuïteit	#Veerkracht
5.31	Wettelijke, statutaire, regel-gevende en contractuele eisen	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Juridisch_en_ compliance	#Governance_en_ Ecosysteem #Bescherming
5.32	Intellectuele-eigendoms-rechten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Juridisch_en_ compliance	#Governance_en_ Ecosysteem
5.33	Beschermen van registraties	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Juridisch_en_ compliance #Beheer_van_ bedrijfsmidde- len #Informatie- bescherming	#Verdediging
5.34	Privacy en bescherming van persoons-gegevens	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Informatie- bescherming #Juridisch_en_ compliance	#Bescherming

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
5.35	Onafhankelijke beoordeling van informatie-beveiliging	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Borging_van_ informatie- beveiliging	#Governance_en _Ecosysteem
5.36	Naleving van beleid, regels en normen voor informatie-beveiliging	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Juridisch_en_ compliance #Borging_van_ informatie- beveiliging	#Governance_en _Ecosysteem
5.37	Gedocumen- teerde bedienings- procedures	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Herstellen	#Beheer_van_ bedrijfsmidde- len #Fysieke_ beveiliging #Systeem-_en_ netwerkbeveili- ging #Toepas- singsbeveiliging #Veilige_confi- guratie #Identi- teits-_en_toe- gangsbeheer #Beheer_van_ dreigingen_en_ kwetsbaarhe- den #Continuï- teit #Beheer_ van_informatie- beveiligings- gebeurtenissen	#Governance_en _Ecosysteem #Bescherming #Verdediging
6.1	Screening	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Personeels- beveiliging	#Governance_en _Ecosysteem
6.2	Arbeids- overeenkomst	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Personeels- beveiliging	#Governance_en _Ecosysteem
6.3	Bewustwording van, opleiding en training in informatie- beveiliging	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Personeels- beveiliging	#Governance_en _Ecosysteem
6.4	Disciplinaire procedure	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Reageren	#Personeels- beveiliging	#Governance_en _Ecosysteem

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging #Beheer_van_bedrijfsmidde-len	#Governance_en_Ecosysteem
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	#Preventief	#Vertrouwelijkheid	#Beschermen	#Personeelsbeveiliging #Informatiebescherming #Leveranciersrelaties	#Governance_en_Ecosysteem
6.7	Werken op afstand	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmidde-len #Informatiebescherming #Fysieke_beveiliging #Systeem_en_netwerkbeveiliging	#Bescherming
6.8	Melden van informatie-beveiligingsgebeurtenissen	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatie-beveiligingsgebeurtenissen	#Verdediging
7.1	Fysieke beveiligingszones	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.2	Fysieke toegangsbeveiliging	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Identiteits_en_toegangsbeheer	#Bescherming
7.3	Beveiligen van kantoren, ruimten en faciliteiten	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.4	Monitoren van de fysieke beveiliging	#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Fysieke_beveiliging	#Bescherming #Verdediging
7.5	Beschermen tegen fysieke en omgevingsdreigingen	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.6	Werken in beveiligde zones	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
7.7	'Clear desk' en 'clear screen'	#Preventief	#Vertrouwelijk- heid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.8	Plaatsen en beschermen van apparatuur	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfs-middelen	#Bescherming
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfs-middelen	#Bescherming
7.10	Opslagmedia	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfs-middelen	#Bescherming
7.11	Nuts-voorzieningen	#Preventief #Detectief	#Integriteit #Beschikbaar- heid	#Beschermen #Detecteren	#Fysieke_beveiliging	#Bescherming
7.12	Beveiligen van bekabeling	#Preventief	#Vertrouwelijk- heid #Beschikbaar- heid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.13	Onderhoud van apparatuur	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfs-middelen	#Bescherming #Veerkracht
7.14	Veilig verwijderen of hergebruiken van apparatuur	#Preventief	#Vertrouwelijk- heid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfs-middelen	#Bescherming
8.1	'User endpoint devices'	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Beheer_van_bedrijfsmid- delen #Informatie- bescherming	#Bescherming
8.2	Speciale toegangsrechten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
8.3	Beperking toegang tot informatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
8.4	Toegangs-beveiliging op broncode	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer #Toepassings- beveiliging #Veilige_conf- iguratie	#Bescherming

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
8.5	Beveiligde authenticatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Identiteits- _en_toegangs- beheer	#Bescherming
8.6	Capaciteits-beheer	#Preventief #Detectief	#Integriteit #Beschikbaar- heid	#Identificeren #Beschermen #Detecteren	#Continuïteit	#Governance_en _Ecosysteem #Bescherming
8.7	Bescherming tegen malware	#Preventief #Detectief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Detecteren	#Systeem- _en_netwerk- beveiliging #Informatie- bescherming	#Bescherming #Verdediging
8.8	Beheer van technische kwetsbaarheden	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Beheer_van_ dreigingen_en_ kwetsbaarhe- den	#Governance_en _Ecosysteem #Bescherming #Verdediging
8.9	Configuratie-beheer	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Veilige_conf- iguratie	#Bescherming
8.10	Wissen van informatie	#Preventief	#Vertrouwelijk- heid	#Beschermen	#Informatie- bescherming #Juridisch_en_ compliance	#Bescherming
8.11	Maskeren van gegevens	#Preventief	#Vertrouwelijk- heid	#Beschermen	#Informatie- bescherming	#Bescherming
8.12	Voorkomen van gegevenslekken (Data leakage prevention)	#Preventief #Detectief	#Vertrouwelijk- heid	#Beschermen #Detecteren	#Informatie- bescherming	#Bescherming #Verdediging
8.13	Back-up van informatie	#Corrigerend	#Integriteit #Beschikbaar- heid	#Herstellen	#Continuïteit	#Bescherming
8.14	Redundantie van informatie-verwerkende faciliteiten	#Preventief	#Beschikbaar- heid	#Beschermen	#Continuïteit #Beheer_van_ bedrijfsmidde- len	#Bescherming #Veerkracht
8.15	Logging	#Detectief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Detecteren	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Bescherming #Verdediging
8.16	Monitoren van activiteiten	#Detectief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Detecteren #Reageren	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
8.17	Kloksynchronisatie	#Detectief	#Integriteit	#Beschermen #Detecteren	#Beheer_van_informatie-beveiligings-gebeurtenissen	#Bescherming #Verdediging
8.18	Gebruik van speciale systeemhulpmiddelen	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem_en_netwerk-beveiliging #Veilige_configuratie #Toepassingsbeveiliging	#Bescherming
8.19	Installeren van software op operationele systemen	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie #Toepassingsbeveiliging	#Bescherming
8.20	Beveiliging netwerk-componenten	#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem_en_netwerk-beveiliging	#Bescherming
8.21	Beveiliging van netwerkdiensten	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem_en_netwerk-beveiliging	#Bescherming
8.22	Netwerksegmentatie	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem_en_netwerk-beveiliging	#Bescherming
8.23	Toepassen van webfilters	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem_en_netwerk-beveiliging	#Bescherming
8.24	Gebruik van cryptografie	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.25	Beveiligen tijdens de ontwikkelcyclus	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem_en_netwerk-beveiliging	#Bescherming
8.26	Toepassingsbeveiligings-eisen	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem_en_netwerk-beveiliging	#Bescherming #Verdediging

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
8.27	Veilige systeem-architectuur en technische uitgangspunten	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Toepassings- beveiliging #Systeem- _en_netwerk- beveiliging	#Bescherming
8.28	Veilig coderen	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Toepassings- beveiliging #Systeem- _en_netwerk- beveiliging	#Bescherming
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren	#Toepassings- beveiliging #Borging_van_ informatiebe- veiliging #Sys- teem-_en_net- werkbeveiliging	#Bescherming
8.30	Uitbestede systeem-ontwikkeling	#Preventief #Detectief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen #Detecteren	#Systeem- _en_netwerk- beveiliging #Toepassings- beveiliging #Beveiliging_in_ leveranciers- relaties	#Governance_en _Ecosysteem #Bescherming
8.31	Scheiding van ontwikkel-, test- en productie-omgevingen	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Toepassings- beveiliging #Systeem- _en_netwerk- beveiliging	#Bescherming
8.32	Wijzigings-beheer	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Toepassings- beveiliging #Systeem- _en_netwerk- beveiliging	#Bescherming
8.33	Testgegevens	#Preventief	#Vertrouwelijk- heid #Integriteit	#Beschermen	#Informatie- bescherming	#Bescherming
8.34	Bescherming van informatie-systemen tijdens audits	#Preventief	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen	#Systeem- _en_netwerk- beveiliging #Informatie- bescherming	#Governance_en _Ecosysteem #Bescherming

In tabel A.2 is een voorbeeld te zien van hoe een overzicht kan worden aangemaakt door te filteren op een bepaalde attribuutwaarde, in dit geval #Corrigerend.

Tabel A.2 — Overzicht van #Corrigerende beheersmaatregelen

Identificatie-code beheers-maatregel ISO/IEC 27002:2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
5.5	Contact met overheids-instanties	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen #Reageren #Herstellen	#Governance	#Verdediging #Veerkracht
5.6	Contact met speciale belangen-groepen	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Reageren #Herstellen	#Governance	#Verdediging
5.7	Informatie en analyses over dreigingen	#Preventief #Detectief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Detecteren #Reageren	#Beheer_van_ dreigingen_en_ kwetsbaar- heden	#Verdediging #Veerkracht
5.24	Plannen en voorbereiden van het beheer van informatie-beveiligings-incidenten	#Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Reageren #Herstellen	#Governance #Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.26	Reageren op informatie-beveiligings-incidenten	#Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Reageren #Herstellen	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.28	Verzamelen van bewijsmateriaal	#Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Detecteren #Reageren	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging
5.29	Informatie-beveiliging tijdens een verstoring	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht
5.30	ICT-gereedheid voor bedrijfs-continuïteit	#Corrigerend	#Beschikbaar- heid	#Reageren	#Continuïteit	#Veerkracht
5.35	Onafhankelijke beoordeling van informatie-beveiliging	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Identificeren #Beschermen	#Borging_van_ informatie- beveiliging	#Governance_en_ _Ecosysteem

Identificatie- code beheers- maatregel ISO/IEC 27002: 2022	Naam beheers- maatregel	Type beheers- maatregel	Informatie- beveiligings- eigenschappen	Cybersecurity- concepten	Operationele capaciteiten	Beveiligings- domeinen
5.37	Gedocumen- teerde bedienings- procedures	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Herstellen	#Beheer_van_ bedrijfsmidde- len #Fysieke_ beveiliging #Systeem-_en_ netwerkbeveili- ging #Toepas- singsbeveiliging #Veilige_confi- guratie #Identi- teits-_en_toe- gangsbeheer #Beheer_van_ dreigingen_en_ kwetsbaarhe- den #Continui- teit #Beheer_ van_informatie- beveiligings- gebeurtenissen	#Governance_en_ Ecosysteem #Bescherming #Verdediging
6.4	Disciplinaire procedure	#Preventief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Reageren	#Personeels- beveiliging	#Governance_en_ Ecosysteem
8.7	Bescherming tegen malware	#Preventief #Detectief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Beschermen #Detecteren	#Systeem- _en_netwerk- beveiliging #Informatie- bescherming	#Bescherming #Verdediging
8.13	Back-up van informatie	#Corrigerend	#Integriteit #Beschikbaar- heid	#Herstellen	#Continuïteit	#Bescherming
8.16	Monitoren van activiteiten	#Detectief #Corrigerend	#Vertrouwelijk- heid #Integriteit #Beschikbaar- heid	#Detecteren #Reageren	#Beheer_van_ informatie- beveiligings- gebeurtenissen	#Verdediging

## A.2 Organisatieoverzichten

Aangezien attributen worden gebruikt om verschillende overzichten van beheersmaatregelen te creëren, kunnen organisaties de voorbeelden van attributen die in dit document worden voorgesteld, verwijderen en hun eigen attributen met verschillende waarden creëren om in te gaan op specifieke behoeften in de organisatie. Daarnaast kunnen de waarden die aan elk attribuut worden toegekend, verschillen tussen organisaties, aangezien organisaties verschillende opvattingen kunnen hebben over het gebruik of de toepasbaarheid van de beheersmaatregel of van de waarden die aan het attribuut zijn gekoppeld (wanneer de waarden specifiek zijn voor de context van de organisatie). De eerste stap is inzicht verwerven in waarom een organisatiespecifiek attribuut wenselijk is. Als een organisatie bijvoorbeeld haar plannen voor risicobehandeling [zie ISO/IEC 27001:2013, 6.1.3 e)] op basis van gebeurtenissen heeft opgebouwd, wil zij mogelijk aan elke beheersmaatregel in dit document een risicoscenarioattribuut koppelen.

Het voordeel van zo'n attribuut is dat hiermee sneller aan de eis van ISO/IEC 27001 met betrekking tot risicobehandeling kan worden voldaan. Dit betreft het vergelijken van de via het proces van risicobehandeling vastgestelde beheersmaatregelen (die worden aangeduid als 'noodzakelijke' beheersmaatregelen) met de beheersmaatregelen in ISO/IEC 27001:2013, bijlage A (die de basis vormen voor de beheersmaatregelen in dit document) om te garanderen dat er geen noodzakelijke beheersmaatregel over het hoofd is gezien.

Zodra het doel en de voordelen bekend zijn, is het vaststellen van de attribuutwaarden de volgende stap. De organisatie zou bijvoorbeeld 9 gebeurtenissen kunnen identificeren:

- 1) verlies of diefstal van een mobiel apparaat;
- 2) verlies of diefstal in het gebouw en/of op het terrein van de organisatie;
- 3) overmacht, vandalisme en terrorisme;
- 4) storingen in software, hardware, voeding, internet en communicatie;
- 5) fraude;
- 6) hacken;
- 7) openbaarmaking;
- 8) overtreding van de wet;
- 9) 'social engineering'.

De tweede stap kan dan worden verwezenlijkt door aan elke gebeurtenis een identificatiecode toe te kennen (bijv. E1, E2, ..., E9).

De derde stap is het naar een spreadsheet of database kopiëren van de identificatiecodes en de namen van de beheersmaatregelen uit dit document en de attribuutwaarden met elke beheersmaatregel koppelen, in het besef dat elke beheersmaatregel meer dan één attribuutwaarde kan hebben.

De laatste stap is het sorteren van de spreadsheet of het doorzoeken van de database om de vereiste informatie te extraheren.

Andere voorbeelden van organisatiespecifieke attributen (en mogelijke waarden) zijn onder andere:

- a) volwassenheid (waarden uit de ISO/IEC 33000-reeks of andere modellen voor volwassenheid);
- b) staat van implementatie (nog te doen, in uitvoering, deels geïmplementeerd, volledig geïmplementeerd);
- c) prioriteit (1, 2, 3 enz.);
- d) betrokken gebieden van de organisatie (beveiliging, ICT, personeelszaken, directie enz.);
- e) gebeurtenissen;
- f) betrokken bedrijfsmiddelen;
- e\*) bouwen en uitvoeren, om onderscheid te maken tussen de beheersmaatregelen die in de verschillende stappen van de levenscyclus van de dienst worden gebruikt;
- g) overige kaders waarmee de organisatie werkt of vanwaaruit zij kan overstappen.

---

\*) Nederlandse voetnoot: Nummering als in de brontekst.

## Bijlage B

### (informatief)

### Overeenstemming van ISO/IEC 27002:2022 (dit document) met ISO/IEC 27002:2013

Het doel van deze bijlage is om achterwaartse compatibiliteit met ISO/IEC 27002:2013 te bieden aan organisaties die momenteel die norm gebruiken en nu naar deze editie willen overstappen.

Tabel B.1 laat zien hoe de in hoofdstuk 5 t/m 8 gespecificeerde beheersmaatregelen corresponderen met de beheersmaatregelen in ISO/IEC 27002:2013.

**Tabel B.1 — Overeenstemming tussen beheersmaatregelen in dit document en  
beheersmaatregelen in ISO/IEC 27002:2013**

Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Naam beheersmaatregel volgens ISO/IEC 27002: 2022
5.1	05.1.1, 05.1.2	Beleidsregels voor informatiebeveiliging
5.2	06.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging
5.3	06.1.2	Functiescheiding
5.4	07.2.1	Managementverantwoordelijkheden
5.5	06.1.3	Contact met overheidsinstanties
5.6	06.1.4	Contact met speciale belangengroepen
5.7	Nieuw	Informatie en analyses over dreigingen
5.8	06.1.5, 14.1.1	Informatiebeveiliging in projectmanagement
5.9	08.1.1, 08.1.2	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
5.10	08.1.3, 08.2.3	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen
5.11	08.1.4	Retourneren van bedrijfsmiddelen
5.12	08.2.1	Classificeren van informatie
5.13	08.2.2	Labelen van informatie
5.14	13.2.1, 13.2.2, 13.2.3	Overdragen van informatie
5.15	09.1.1, 09.1.2	Toegangsbeveiliging
5.16	09.2.1	Identiteitsbeheer
5.17	09.2.4, 09.3.1, 09.4.3	Beheren van authenticatie-informatie
5.18	09.2.2, 09.2.5, 09.2.6	Toegangsrechten
5.19	15.1.1	Informatiebeveiliging in leveranciersrelaties

Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Naam beheersmaatregel volgens ISO/IEC 27002: 2022
5.20	15.1.2	Adresseren van informatiebeveiliging in leveranciersovereenkomsten
5.21	15.1.3	Beheren van informatiebeveiliging in de ICT-keten
5.22	15.2.1, 15.2.2	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
5.23	Nieuw	Informatiebeveiliging voor het gebruik van clouddiensten
5.24	16.1.1	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten
5.25	16.1.4	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen
5.26	16.1.5	Reageren op informatiebeveiligingsincidenten
5.27	16.1.6	Leren van informatiebeveiligingsincidenten
5.28	16.1.7	Verzamelen van bewijsmateriaal
5.29	17.1.1, 17.1.2, 17.1.3	Informatiebeveiliging tijdens een verstoring
5.30	Nieuw	ICT-gereedheid voor bedrijfscontinuïteit
5.31	18.1.1, 18.1.5	Wettelijke, statutaire, regelgevende en contractuele eisen
5.32	18.1.2	Intellectuele-eigendomsrechten
5.33	18.1.3	Beschermen van registraties
5.34	18.1.4	Privacy en bescherming van persoonsgegevens
5.35	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging
5.36	18.2.2, 18.2.3	Naleving van beleid, regels en normen voor informatiebeveiliging
5.37	12.1.1	Gedocumenteerde bedieningsprocedures
6.1	07.1.1	Screening
6.2	07.1.2	Arbeidsovereenkomst
6.3	07.2.2	Bewustwording van, opleiding en training in informatiebeveiliging
6.4	07.2.3	Disciplinaire procedure
6.5	07.3.1	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband
6.6	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomsten
6.7	06.2.2	Werken op afstand
6.8	16.1.2, 16.1.3	Melden van informatiebeveiligingsgebeurtenissen
7.1	11.1.1	Fysieke beveiligingszones
7.2	11.1.2, 11.1.6	Fysieke toegangsbeveiliging
7.3	11.1.3	Beveiligen van kantoren, ruimten en faciliteiten

Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Naam beheersmaatregel volgens ISO/IEC 27002: 2022
7.4	Nieuw	Monitoren van de fysieke beveiliging
7.5	11.1.4	Beschermen tegen fysieke en omgevingsdreigingen
7.6	11.1.5	Werken in beveiligde gebieden
7.7	11.2.9	'Clear desk' en 'clear screen'
7.8	11.2.1	Plaatsen en beschermen van apparatuur
7.9	11.2.6	Beveiligen van bedrijfsmiddelen buiten het terrein
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Opslagmedia
7.11	11.2.2	Nutsvoorzieningen
7.12	11.2.3	Beveiligen van bekabeling
7.13	11.2.4	Onderhoud van apparatuur
7.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur
8.1	06.2.1, 11.2.8	'User endpoint devices'
8.2	09.2.3	Speciale toegangsrechten
8.3	09.4.1	Beperking toegang tot informatie
8.4	09.4.5	Toegangsbeveiliging op broncode
8.5	09.4.2	Beveiligde authenticatie
8.6	12.1.3	Capaciteitsbeheer
8.7	12.2.1	Bescherming tegen malware
8.8	12.6.1, 18.2.3	Beheer van technische kwetsbaarheden
8.9	Nieuw	Configuratiebeheer
8.10	Nieuw	Wissen van informatie
8.11	Nieuw	Maskeren van gegevens
8.12	Nieuw	Voorkomen van gegevenslekken (Data leakage prevention)
8.13	12.3.1	Back-up van informatie
8.14	17.2.1	Redundantie van informatieverwerkende faciliteiten
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	Nieuw	Monitoren van activiteiten
8.17	12.4.4	Kloksynchronisatie
8.18	09.4.4	Gebruik van speciale systeemhulpmiddelen
8.19	12.5.1, 12.6.2	Installeren van software op operationele systemen

Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Naam beheersmaatregel volgens ISO/IEC 27002: 2022
8.20	13.1.1	Beveiliging netwerkcomponenten
8.21	13.1.2	Beveiliging van netwerkdiensten
8.22	13.1.3	Netwerksegmentatie
8.23	Nieuw	Toepassen van webfilters
8.24	10.1.1, 10.1.2	Gebruik van cryptografie
8.25	14.2.1	Beveiligen tijdens de ontwikkelcyclus
8.26	14.1.2, 14.1.3	Toegangsbeveiligingseisen
8.27	14.2.5	Veilige systeemarchitectuur en technische uitgangspunten
8.28	Nieuw	Veilig coderen
8.29	14.2.8, 14.2.9	Testen van de beveiliging tijdens ontwikkeling en acceptatie
8.30	14.2.7	Uitbestede systeemontwikkeling
8.31	12.1.4, 14.2.6	Scheiding van ontwikkel-, test- en productieomgevingen
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Wijzigingsbeheer
8.33	14.3.1	Testgegevens
8.34	12.7.1	Bescherming van informatiesystemen tijdens audits

Tabel B.2 toont de overeenstemming tussen de in ISO/IEC 27002:2013 en in dit document gespecificeerde beheersmaatregelen.

**Tabel B.2 — Overeenstemming tussen beheersmaatregelen in ISO/IEC 27002:2013 en beheersmaatregelen in dit document**

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
5		Informatiebeveiligingsbeleid
5.1		Aansturing door de directie van de informatiebeveiliging
5.1.1	5.1	Beleidsregels voor informatiebeveiliging
5.1.2	5.1	Beoordeling van het informatiebeveiligingsbeleid
6		Organiseren van informatiebeveiliging
6.1		Interne organisatie
6.1.1	5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
6.1.2	5.3	Scheiding van taken
6.1.3	5.5	Contact met overheidsinstanties
6.1.4	5.6	Contact met speciale belangengroepen
6.1.5	5.8	Informatiebeveiliging in projectbeheer
6.2		Mobiele apparatuur en telewerken
6.2.1	8.1	Beleid voor mobiele apparatuur
6.2.2	6.7	Telewerken
7		Veilig personeel
7.1		Voorafgaand aan het dienstverband
7.1.1	6.1	Screening
7.1.2	6.2	Arbeidsvoorwaarden
7.2		Tijdens het dienstverband
7.2.1	5.4	Directieverantwoordelijkheden
7.2.2	6.3	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
7.2.3	6.4	Disciplinaire procedure
7.3		Beëindiging en wijziging van dienstverband
7.3.1	6.5	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband
8		Beheer van bedrijfsmiddelen
8.1		Verantwoordelijkheid voor bedrijfsmiddelen
8.1.1	5.9	Inventariseren van bedrijfsmiddelen
8.1.2	5.9	Eigendom van bedrijfsmiddelen
8.1.3	5.10	Aanvaardbaar gebruik van bedrijfsmiddelen
8.1.4	5.11	Teruggeven van bedrijfsmiddelen
8.2		Informatieclassificatie
8.2.1	5.12	Classificatie van informatie
8.2.2	5.13	Informatie labelen
8.2.3	5.10	Behandelen van bedrijfsmiddelen
8.3		Behandelen van media
8.3.1	7.10	Beheer van verwijderbare media
8.3.2	7.10	Verwijderen van media

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
8.3.3	7.10	Media fysiek overdragen
9		Toegangsbeveiliging
9.1		Bedrijfseisen voor toegangsbeveiliging
9.1.1	5.15	Beleid voor toegangsbeveiliging
9.1.2	5.15	Toegang tot netwerken en netwerkdiensten
9.2		Beheer van toegangsrechten van gebruikers
9.2.1	5.16	Registratie en afmelden van gebruikers
9.2.2	5.18	Gebruikers toegang verlenen
9.2.3	8.2	Beheren van speciale toegangsrechten
9.2.4	5.17	Beheer van geheime authenticatie-informatie van gebruikers
9.2.5	5.18	Beoordeling van toegangsrechten van gebruikers
9.2.6	5.18	Toegangsrechten intrekken of aanpassen
9.3		Verantwoordelijkheden van gebruikers
9.3.1	5.17	Geheime authenticatie-informatie gebruiken
9.4		Toegangsbeveiliging van systeem en toepassing
9.4.1	8.3	Beperking toegang tot informatie
9.4.2	8.5	Beveiligde inlogprocedures
9.4.3	5.17	Systeem voor wachtwoordbeheer
9.4.4	8.18	Speciale systeemhulpmiddelen gebruiken
9.4.5	8.4	Toegangsbeveiliging op programmabroncode
10		Cryptografie
10.1		Cryptografische beheersmaatregelen
10.1.1	8.24	Beleid inzake het gebruik van cryptografische beheersmaatregelen
10.1.2	8.24	Sleutelbeheer
11		Fysieke beveiliging en beveiliging van de omgeving
11.1		Beveiligde gebieden
11.1.1	7.1	Fysieke beveiligingszone
11.1.2	7.2	Fysieke toegangsbeveiliging
11.1.3	7.3	Kantoren, ruimten en faciliteiten beveiligen
11.1.4	7.5	Beschermen tegen bedreigingen van buitenaf
11.1.5	7.6	Werken in beveiligde gebieden

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
11.1.6	7.2	Laad- en loslocatie
11.2		Apparatuur
11.2.1	7.8	Plaatsing en bescherming van apparatuur
11.2.2	7.11	Nutsvoorzieningen
11.2.3	7.12	Beveiliging van bekabeling
11.2.4	7.13	Onderhoud van apparatuur
11.2.5	7.10	Verwijdering van bedrijfsmiddelen
11.2.6	7.9	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
11.2.7	7.14	Veilig verwijderen of hergebruiken van apparatuur
11.2.8	8.1	Onbeheerde gebruikersapparatuur
11.2.9	7.7	'Clear desk'- en 'clear screen'-beleid
12		Beveiliging bedrijfsvoering
12.1		Bedieningsprocedures en verantwoordelijkheden
12.1.1	5.37	Gedocumenteerde bedieningsprocedures
12.1.2	8.32	Wijzigingsbeheer
12.1.3	8.6	Capaciteitsbeheer
12.1.4	8.31	Scheiding van ontwikkel-, test- en productieomgevingen
12.2		Bescherming tegen malware
12.2.1	8.7	Beheersmaatregelen tegen malware
12.3		Back-up
12.3.1	8.13	Back-up van informatie
12.4		Verslaglegging en monitoren
12.4.1	8.15	Gebeurtenissen registreren
12.4.2	8.15	Beschermen van informatie in logbestanden
12.4.3	8.15	Logbestanden van beheerders en operators
12.4.4	8.17	Kloksynchronisatie
12.5		Beheersing van operationele software
12.5.1	8.19	Software installeren op operationele systemen
12.6		Beheer van technische kwetsbaarheden
12.6.1	8.8	Beheer van technische kwetsbaarheden
12.6.2	8.19	Beperkingen voor het installeren van software

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
12.7		Overwegingen betreffende audits van informatiesystemen
12.7.1	8.34	Beheersmaatregelen betreffende audits van informatiesystemen
13		Communicatiebeveiliging
13.1		Beheer van netwerkbeveiliging
13.1.1	8.20	Beheersmaatregelen voor netwerken
13.1.2	8.21	Beveiliging van netwerkdiensten
13.1.3	8.22	Scheiding in netwerken
13.2		Informatietransport
13.2.1	5.14	Beleid en procedures voor informatietransport
13.2.2	5.14	Overeenkomsten over informatietransport
13.2.3	5.14	Elektronische berichten
13.2.4	6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomst
14		Acquisitie, ontwikkeling en onderhoud van informatiesystemen
14.1		Beveiligingseisen voor informatiesystemen
14.1.1	5.8	Analyse en specificatie van informatiebeveiligingseisen
14.1.2	8.26	Toepassingen op openbare netwerken beveiligen
14.1.3	8.26	Transacties van toepassingen beschermen
14.2		Beveiliging in ontwikkelings- en ondersteunende processen
14.2.1	8.25	Beleid voor beveiligd ontwikkelen
14.2.2	8.32	Procedures voor wijzigingsbeheer met betrekking tot systemen
14.2.3	8.32	Technische beoordeling van toepassingen na wijzigingen besturingsplatform
14.2.4	8.32	Beperkingen op wijzigingen aan softwarepakketten
14.2.5	8.27	Principes voor engineering van beveiligde systemen
14.2.6	8.31	Beveiligde ontwikkelomgeving
14.2.7	8.30	Uitbestede systeemontwikkeling
14.2.8	8.29	Testen van systeembeveiliging
14.2.9	8.29	Systeemacceptatietests
14.3		Testgegevens
14.3.1	8.33	Bescherming van testgegevens
15		Leveranciersrelaties

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
15.1		Informatiebeveiliging in leveranciersrelaties
15.1.1	5.19	Informatiebeveiligingsbeleid voor leveranciersrelaties
15.1.2	5.20	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
15.1.3	5.21	Toeleveringsketen van informatie- en communicatietechnologie
15.2		Beheer van dienstverlening van leveranciers
15.2.1	5.22	Monitoring en beoordeling van dienstverlening van leveranciers
15.2.2	5.22	Beheer van veranderingen in dienstverlening van leveranciers
16		Beheer van informatiebeveiligingsincidenten
16.1		Beheer van informatiebeveiligingsincidenten en -verbeteringen
16.1.1	5.24	Verantwoordelijkheden en procedures
16.1.2	6.8	Rapportage van informatiebeveiligingsgebeurtenissen
16.1.3	6.8	Rapportage van zwakke plekken in de informatiebeveiliging
16.1.4	5.25	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
16.1.5	5.26	Respons op informatiebeveiligingsincidenten
16.1.6	5.27	Lering uit informatiebeveiligingsincidenten
16.1.7	5.28	Verzamelen van bewijsmateriaal
17		Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
17.1		Informatiebeveiligingscontinuïteit
17.1.1	5.29	Informatiebeveiligingscontinuïteit plannen
17.1.2	5.29	Informatiebeveiligingscontinuïteit implementeren
17.1.3	5.29	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren
17.2		Redundante componenten
17.2.1	8.14	Beschikbaarheid van informatieverwerkende faciliteiten
18		Naleving
18.1		Naleving van wettelijke en contractuele eisen
18.1.1	5.31	Vaststellen van toepasselijke wetgeving en contractuele eisen
18.1.2	5.32	Intellectuele-eigendomsrechten
18.1.3	5.33	Beschermen van registraties
18.1.4	5.34	Privacy en bescherming van persoonsgegevens
18.1.5	5.31	Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Identificatiecode beheersmaatregel ISO/IEC 27002: 2013	Identificatiecode beheersmaatregel ISO/IEC 27002: 2022	Naam beheersmaatregel volgens ISO/IEC 27002: 2013
18.2		Informatiebeveiligingsbeoordelingen
18.2.1	5.35	Onafhankelijke beoordeling van informatiebeveiliging
18.2.2	5.36	Naleving van beveiligingsbeleid en -normen
18.2.3	5.36, 8.8	Beoordeling van technische naleving

## Bibliografie

- [1] ISO 9000, *Quality management systems – Fundamentals and vocabulary*
- [2] ISO 55001, *Asset management – Management systems – Requirements*
- [3] ISO/IEC 11770 (all parts), *Information security – Key management*
- [4] ISO/IEC 15408 (all parts), *Information technology – Security techniques – Evaluation criteria for IT security*
- [5] ISO 15489 (all parts), *Information and documentation – Records management*
- [6] ISO/IEC 17788, *Information technology – Cloud computing – Overview and vocabulary*
- [7] ISO/IEC 17789, *Information technology – Cloud computing – Reference architecture*
- [8] ISO/IEC 19086 (all parts), *Cloud computing – Service level agreement (SLA) framework*
- [9] ISO/IEC 19770 (all parts), *Information technology – IT asset management*
- [10] ISO/IEC 19941, *Information technology – Cloud computing – Interoperability and portability*
- [11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
- [12] ISO 21500, *Project, programme and portfolio management – Context and concepts*
- [13] ISO 21502, *Project, programme and portfolio management – Guidance on project management*
- [14] ISO 22301, *Security and resilience – Business continuity management systems – Requirements*
- [15] ISO 22313, *Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301*
- [16] ISO/TS 22317, *Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)*
- [17] ISO 22396, *Security and resilience – Community resilience – Guidelines for information exchange between organizations*
- [18] ISO/IEC TS 23167, *Information technology – Cloud computing – Common technologies and techniques*
- [19] ISO/IEC 23751, *Information technology – Cloud computing and distributed platforms – Data sharing agreement (DSA) framework*
- [20] ISO/IEC 24760 (all parts), *IT Security and Privacy – A framework for identity management*
- [21] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*
- [22] ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*

- [23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing*
- [24] ISO/IEC TS 27008, *Information technology – Security techniques – Guidelines for the assessment of information security controls*
- [25] ISO/IEC 27011, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*
- [26] ISO/IEC TR 27016, *Information technology – Security techniques – Information security management – Organizational economics*
- [27] ISO/IEC 27017, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [28] ISO/IEC 27018, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [29] ISO/IEC 27019, *Information technology – Security techniques – Information security controls for the energy utility industry*
- [30] ISO/IEC 27031, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*
- [31] ISO/IEC 27033 (all parts), *Information technology – Security techniques – Network security*
- [32] ISO/IEC 27034 (all parts), *Information technology – Application security*
- [33] ISO/IEC 27035 (all parts), *Information technology – Security techniques – Information security incident management*
- [34] ISO/IEC 27036 (all parts), *Information technology – Security techniques – Information security for supplier relationships*
- [35] ISO/IEC 27037, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*
- [36] ISO/IEC 27040, *Information technology – Security techniques – Storage security*
- [37] ISO/IEC 27050 (all parts), *Information technology – Electronic discovery*
- [38] ISO/IEC/TS 27110, *Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines*
- [39] ISO/IEC 27701, *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*
- [40] ISO 27799, *Health informatics – Information security management in health using ISO/IEC 27002*
- [41] ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*
- [42] ISO/IEC 29115, *Information technology – Security techniques – Entity authentication assurance framework*

- [43] ISO/IEC 29134, *Information technology – Security techniques – Guidelines for privacy impact assessment*
- [44] ISO/IEC 29146, *Information technology – Security techniques – A framework for access management*
- [45] ISO/IEC 29147, *Information technology – Security techniques – Vulnerability disclosure*
- [46] ISO 30000, *Ships and marine technology – Ship recycling management systems – Specifications for management systems for safe and environmentally sound ship recycling facilities*
- [47] ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes*
- [48] ISO 31000:2018, *Risk management – Guidelines*
- [49] IEC 31010, *Risk management – Risk assessment techniques*
- [50] ISO/IEC 22123 (all parts), *Information technology – Cloud computing*
- [51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion*
- [52] INFORMATION SECURITY FORUM (ISF). The ISF Standard of Good Practice for Information Security 2020, augustus 2018. Beschikbaar op <https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/>
- [53] ITIL® Foundation, ITIL 4 editie, AXELOS, februari 2019, ISBN: 9780113316076
- [54] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [geraadpleegd op 2020-07-31]. Beschikbaar op <https://doi.org/10.6028/NIST.SP.800-37r2>
- [55] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [geraadpleegd op 31-07-2020]. Beschikbaar op [https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/)
- [56] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [online] [geraadpleegd op 2020-10-22]. Beschikbaar op <https://github.com/OWASP/DevGuide>
- [57] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. Februari 2020 [geraadpleegd op 2020-07-31]. Beschikbaar op <https://doi.org/10.6028/NIST.SP.800-63b>
- [58] OASIS. Structured Threat Information Expression. Beschikbaar op <https://www.oasis-open.org/standards#stix2.0>
- [59] OASIS. Trusted Automated Exchange of Indicator Information. Beschikbaar op <https://www.oasis-open.org/standards#taxii2.0>

## **Waarom betaalt u voor een norm?**

Normen zijn afspraken voor en door de markt. Het zijn afspraken over zaken waarmee iedereen te maken heeft. Bijvoorbeeld over gezondheidszorg, financiële dienstverlening, veiligheid en maatschappelijk verantwoord ondernemen. Zonder deze afspraken zou het leven een stuk complexer zijn. Normen zorgen voor verbetering van producten, diensten en processen. Op de werkvloer, in de omgang met elkaar en in de samenleving als geheel.

De afspraken worden gemaakt door belanghebbende partijen. Een belanghebbende partij kan een producent, ondernemer, dienstverlener, gebruiker, maar ook de overheid of een consumenten- of onderzoeksorganisatie zijn. Een breed draagvlak is belangrijk. De afspraken komen onder begeleiding van NEN tot stand en mogen niet strijdig zijn met andere geldige NEN-normen.

NEN is een stichting en heeft geen winstoogmerk. De diensten die NEN levert – van het bijeenbrengen van partijen en het maken en vastleggen van de afspraken tot het bieden van hulp bij de toepassing van de normen – moeten worden bekostigd. Daarom betalen alle deelnemende partijen voor het normalisatieproces en betaalt u als gebruiker voor normen, trainingen en andere producten.



# Altijd de actuele norm?

**Nooit meer zoeken in de systemen en zelf de vraag stellen:  
'Heb ik de laatste versie van ISO/IEC 27002:2022 nl?'**

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. Met een licentie kan de norm via NEN Connect altijd en overal makkelijk geraadpleegd worden, zowel online als offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op [www.nenconnect.nl](https://www.nenconnect.nl).

#### **Meer informatie over de mogelijkheden**

Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 uur tot 17.00 uur.

Telefoon: 015 2 690 391

E-mail: [klantenservice@nen.nl](mailto:klantenservice@nen.nl)

**nen**  
connect