In applicaties/systemen, waarin geautomatiseerd rekening wordt gehouden met deze functiescheiding, kan indien gewenst ruimer worden geautoriseerd. Hiermee wordt bedoeld dat als de applicatie/het systeem opeenvolgende handelingen in het proces door één functionaris op één en hetzelfde dossier niet toestaat, maar wel voor andere dossiers, waar nog geen conflicterende handeling door deze functionaris is uitgevoerd.

Per proces moet een beschrijving van de te gebruiken applicatie/systemen gemaakt worden, inclusief de mogelijkheden om te kunnen voldoen aan de functiescheiding.

Indien op het gebied van autorisaties niet kan worden voldaan aan de vereiste functiescheiding mag hiervan slechts worden afgeweken mits:

- de risico's in kaart zijn gebracht (op basis van een risicoanalyse);
- er voldoende compenserende maatregelen zijn ingeregeld;
- de beveiligingsadviseur positief heeft geadviseerd aan het verantwoordelijk management.

Muteerrechten in het ondersteunend proces, zoals het registreren van SAP-Tijd, worden in een bedrijfsonderdeel overstijgend profiel (Everyone) of in een bedrijfsvoerings- of managementprofiel opgenomen. Deze autorisaties zijn voor ieder bedrijfsonderdeel gelijk.

B.1.3.2.4 Bijzondere rechten

Onder bijzondere rechten worden toegangsrechten verstaan waaraan specifieke voorwaarden worden gesteld. Bevoegdheden kunnen bijzonder zijn omdat deze:

- Potentieel de functiescheiding kunnen doorbreken;
- Alleen beperkt functioneel mogen worden toegekend;
- Bijzondere informatie ontsluiten, zoals die van vips;
- Gepaard gaan met licentiekosten;
- Om performanceredenen slechts beperkt mogen worden gebruikt;
- De mogelijkheid bieden elektronisch gegevens uit te wisselen.

Privileges

Indien er binnen een proces functioneel behoefte is aan privileges, dan kunnen deze in het bestaande profiel of als sub-profiel worden opgenomen.

Indien een privilege niet functioneel wordt toegekend (het privilege is niet opgenomen in het procesprofiel), moet de geëigende aanvraagprocedure worden gevolgd.

Daar waar de classificatie van informatie hogere eisen stelt aan de afscherming, worden de rechten alleen op individuele wijze toegekend. Deze rechten worden binnen het bijbehorende proces in een apart profiel 'Bijzondere taken' opgenomen.

Live- en productiegegevens

Het gebruiken van live/productiegegevens buiten de doelbinding (Wbp) is niet toegestaan. Per geval dienen alternatieven te worden onderzocht, waaronder pseudonimisatie of anonimisatie. Als afdoende blijkt dat er geen andere mogelijkheden zijn (explain), dient voor een uitzondering een risicoafweging en -acceptatie te worden gedaan. De verantwoordlijkheid hiervoor ligt in de lijn.

Opleidingen

Voor het opleiden van medewerkers van de Belastingdienst is het vaak noodzakelijk dat zij kunnen leren of oefenen in de systemen en applicaties van de primaire processen. Daarom dient gebruik gemaakt te worden van testomgevingen of speciaal voor opleidingen ontwikkelde omgevingen die door de bedrijfsonderdelen zelf worden beheerd.

In de onder verantwoordelijkheid van de BelastingdienstAcademie ontwikkelde, beheerde en uitgevoerde opleidingen wordt geen gebruik gemaakt van het oefenen in live/productieomgevingen.

Wel kunnen praktijkopdrachten als onderdeel van de leertrajecten ingericht worden waarbij individuele medewerkers onder begeleiding van een ervaren collega werken in de systemen of applicaties. Dit gebeurt dan op de werkplek en onder verantwoordelijkheid van het bedrijfsonderdeel, in casu de ervaren collega.

B.1.3.2.5 Beleid op controle op gebruik van autorisaties

Autorisaties geven toegang tot (geautomatiseerde) bedrijfsmiddelen. Bedoeld of onbedoeld misbruik hiervan moet kunnen worden gesignaleerd zoals bij het onbevoegd raadplegen of onbevoegd muteren van gegevens. Dat geldt ook buiten de grenzen van de organisatie zoals op internet. Hiertoe zijn procedures vastgesteld, waarbij het resultaat ervan regelmatig wordt beoordeeld.

Beveiligingsfuncties

Identificatie, authenticatie en autorisatie zijn de functies die de handhaving van functiescheiding, de herleidbaarheid van handelingen en de beperking van de toegang tot gegevens ondersteunen. Het wijzigen of inzien van gegevens dient herleidbaar te zijn tot de natuurlijke persoon die de handeling verricht.

Autorisaties die hierbij bijzondere aandacht behoeven zijn de privileges, waarmee het mogelijk is interne elektronische informatie buiten het (beveiligings)domein van de Belastingdienst te brengen en vice versa.

B.1.4. Beleid op informatieuitwisseling

Vanuit informatie gezien

Informatieuitwisseling omvat zowel in- en uitgaande informatie, langs alle kanalen zoals post, telefoon of elektronisch, formeel of informeel.

Enerzijds geldt voor de Belastingdienst als organisatie dat hij gehouden is aan de relevante wet- en regelgeving over de bescherming van vertrouwelijke (persoons)gegevens en (elektronische) informatieuitwisseling. Anderzijds gelden er voorschriften voor de medewerkers, gericht op plichten als geheimhouding en gewenst gedrag. Met name in de contacten met burgers en bedrijven wordt hier aandacht aan besteed binnen de dienstverleningsstrategie. We hanteren de volgene uitgangspunten:

- Uitwisseling van informatie met een wettelijke grond, met ketenpartners, gebeurt op basis van de bestaande wet- en regelgeving. We voldoen hieraan en stellen geen aanvullende eisen. Massale gegevensuitwisseling met derden wordt namens de Belastingdienst uitsluitend door de Centrale Administratie uitgevoerd;
- Andere uitwisseling van formele of vertrouwelijke informatie gebeurt onder het treffen van adequate generieke maatregelen ten aanzien van vertrouwelijkheid of rechtsgeldigheid, om bijvoorbeeld de bescherming van persoonsgegevens, authenticiteit of onweerlegbaarheid te borgen;
- Voor alle andere uitwisseling van informatie gelden voorwaarden en gedragsregels.

Presentatie

We presenteren veel (persoons)gegevens aan burgers, bedrijven en overheden. Maar alleen de benodigde gegevens en alleen aan personen en organisaties waarvan we een bepaalde zekerheid hebben omtrent de identiteit en bevoegdheid. Ook letten we op welke gegevens fraudegevoelig kunnen zijn omdat we de drempel voor mis- en oneigenlijk gebruik van elektronisch berichtenverkeer niet willen verlagen. We sluiten aan op de overheidsbreed ontwikkelde voorzieningen als DigiD, eID en MijnOverheid.

Authenticatie

We vertrouwen onze medewerkers bij het muteren en vastleggen van gegevens. Onze gegevens zijn altijd vertrouwelijk. Het is in ons eigen belang dat we de aan ons toevertrouwde gegevens beschermen tegen ongeautoriseerde inzage of mutatie en dat de in- en uitgaande gegevens betrouwbaar zijn. We kiezen hierbij voor algemene authenticatiemiddelen met een beperkt aantal niveaus. Afhankelijk van de doelgroep maken we ruimte voor extra maatregelen.

Aanvullend gelden, voor alle uitwisseling, voorschriften als het ARAR en de PUB. Specifieke voorwaarden, bijvoorbeeld voor het gebruik van e-mail of informatie van internet, houden rekening met deze invalshoeken met aandacht voor samenhang en werkbaarheid (zie ook B.1.7).

Deze aspecten dienen breed in de bedrijfsvoering te worden verankerd.

Vanuit domein gezien

Naast de bovenstaande inhoudelijke indeling, kan ook een logische indeling worden gemaakt. De invalshoek is er dan één vanuit het organisatiedomein, waarbij domein vertaald kan worden in *invloedssfeer* in de zin van fysieke bescherming en beheer:

Binnen domein, buiten basis beveiligingsstelsel

- Uitwisseling van informatie met partijen *buiten* het domein van de Belastingdienst. Deze uitwisseling gebeurt met burgers, ondernemers en andere (overheids)partijen en betreft informatie uit het primaire proces. Zodra de informatie buiten het domein van de Belastingdienst is, hebben we minder invloed op risicomitigerende maatregelen. We hanteren afspraken voor beveiliging in transport, opslag en verwerking tot vernietiging.
- Uitwisseling van informatie *binnen* het domein van de Belastingdienst. Hiervoor geldt het basisniveau beveiliging.

Encryptie bij transport en opslag

Bij alle transport van gegevens zorgen we voor adequate beveiliging door middel van het principe van isolatie, bijvoorbeeld in de vorm van fysieke of logische paden of encryptie. Met name encryptie geldt niet alleen bij gestructureerde gegevensuitwisseling maar ook bij het interne netwerk, een laptop, tablet, CD/DVD, USB-stick of met externe e-mail.

Bedrijfsmiddelen

In principe wordt bedrijfsinformatie uitsluitend verwerkt op de door de (onder verantwoording van de) Belastingdienst beschikbaar gestelde middelen.

Gegevens van burgers en bedrijven dienen te worden versleuteld, niet alleen tijdens transport maar ook bij opslag. Dit ligt in lijn met de maatschappelijke en marktontwikkelingen en volgt onder meer uit het kabinetsstandpunt rond encryptie[15] en de risicorapportage van het Centraal Planbureau[16], op basis van het Cybersecuritybeeld Nederland van het NCSC[17].

Fysieke gegevensdragers

Bij fysieke gegevensdragers bedoeld voor gegevensuitwisseling met derden isoleren we bijvoorbeeld door middel van encryptie[18], aanvullend beschreven in de *Procedure voor fysieke gegevensuitwisseling met externe partijen – voor alle dienstonderdelen*[19].

Gevonden gegevensdragers

Bijzondere aandacht betreft de omgang met gevonden gegevensdragers. USB-sticks, CD's en dergelijke kunnen door kwaadwillenden gebruikt worden voor het introduceren van malware op computers. Een populaire werkwijze daarvoor is het "verliezen" van een gegevensdrager waarop de malware is geplaatst.

[15] Kamerbrief over kabinetsstandpunt encryptie, VenJ/EZ, 4 januari 2016
[16] Risicorapportage cyberveiligheid economie, Centraal Planbureau, 6 juli 2016,
[17] VenJ/Nationaal Cyber Security Centrum
[18] Informatiebeveiliging gegevensdragers, DGBel/CSO en CIO, 29 april 2010
[19] Versie 1.0, B/CIE, 28 april 2010

Gevonden USB-stick nooit bekijken	Vervolgens wordt vertrouwd op de nieuwsgierigheid en/of eerlijkheid van de vinder, die al dan niet in een poging om de rechtmatige eigenaar te achterhalen wil weten wat er op staat. Daarmee wordt de malware in werking gezet. Het is dan ook uitdrukkelijk verboden om een gevonden gegevensdrager in een PC te stoppen. Gevonden gegevensdragers dienen te worden onderzocht door het CIE/Security Operations Center. Daartoe wordt de gegevensdrager bij een receptiemedewerker ingeleverd, die de te volgen procedure[20] kent.
Antivirus, intrusion detection	Bij alle elektronische informatieuitwisseling van *buiten* het belastingdienstdomein wordt op schadelijke programmatuur gecontroleerd en gescand (virussen, malware etc, ook op versleutelde stromen) en wordt de grens van het domein beschermd en gecontroleerd tegen aanvallen van binnen en buiten. Hierbij worden de richtlijnen die binnen de rijksoverheid gelden (zoals vanuit het NCSC) gevolgd en worden adequate middelen ingezet.
Clouddiensten	We slaan zelf geen gegevens op buiten onze invloedssfeer. Ten aanzien van clouddiensten volgen we het rijksoverheidsbeleid zoals beschreven in de informatiseringsstrategie Rijk[21] en de daaraan voorafgaande cloudstrategie[22]. Wat informatiebeveiliging betreft blijkt dat het via een "open" cloud uitbesteden van ICT diensten, dan wel opslag van informatie buiten Nederland, risico's met zich meebrengt die nog niet voldoende kunnen worden afgedekt. (sic)
Sourcingstrategie	In de herijkte sourcingstrategie[23] staat dat het afnemen van clouddiensten tot de mogelijkheden behoort maar dat er alleen geshopt mag worden in de private cloud van de Belastingdienst of de Rijksoverheid, en dan nog alleen onder strikte condities. Deze condities hebben met name betrekking op het waarborgen van de beschikbaarheid en vetrouwelijkheid van data die gehost wordt in de cloud.
Mobiele apparatuur	Een bijzondere vorm informatieuitwisseling binnen het domein zie je bij draagbare apparatuur (PDA's, tablets, smartphones, USB-sticks of draagbare computers (PPC's)). Deze apparatuur kan fungeren als informatiedrager, die weliswaar binnen het domein van de Belastingdienst valt, maar buiten de beschermende invloedssfeer ervan kan verkeren. Hiervoor treffen we extra beveiligingsmaatregelen: We transporteren ook hier niet onnodig gegevens, verstrekken geen onnodige autorisaties en we bieden hard- en softwarematige voorzieningen aan zoals externe media encryptie. Daarbij zijn we kritisch op de noodzaak van het gebruik van een bedrijfsmiddel, koppelen dat bij voorkeur aan een functie en zien er op toe dat de extra maatregelen ook daadwerkelijk worden gebruikt.
Label, logo of merk	Voor al de *bedrijfsmiddelen* die in dit kader worden gebruikt, geldt dat de herkenbaarheid als belastingdiensteigendom minimaal moet zijn.
	Uitwisseling en verwerking van informatie in het primair proces zoals de massale gegevensverwerking, ook binnen de eigen organisatie, is gebonden aan de wet- en regelgeving omtrent de bescherming van persoonsgegevens. Koppeling van (data uit) geautomatiseerde systemen gebeurt met inachtneming hiervan.
Koppeling van systemen	Bij de koppeling van (data uit) kantoorautomatiseringssystemen ontstaan risico's voor bijvoorbeeld controlemedewerkers, rechercheurs, vertrouwenspersonen, bedrijfsartsen en OR-leden (toegankelijkheid tot e-mail, agenda). Deze worden opgevangen door huisregels, houding en gedrag. Dit

[20] Richtlijn voor de omgang met gevonden gegevensdragers, B/CIE, 19 januari 2015.
[21] I-strategie Rijk, BZK/DGOBR, 15 november 2011
[22] Cloud Strategie, BZK/DIR, 20 april 2011
[23] Actualisatie Sourcingbeleid IV Belastingdienst, IV-Overleg, versie 4 september 2013

hoort thuis in de decentrale risicoanalyse en valt onder het desbetreffende management van een bedrijfsonderdeel.

Archiefbeheer

De Belastingdienst heeft de verantwoordelijkheid te borgen dat de ontvangen, gecreëerde en verzonden informatie betrouwbaar en duurzaam toegankelijk is. Dit geldt tot het moment van verwijdering, waarbij de verwijdering conform vastgelegde procedures verloopt.

De informatie moet daarom volledig en authentiek zijn, vindbaar en beschikbaar, blijvend leesbaar (in bepaalde formaten zijn vastgelegd), waar selectiebeleid op kan worden toegepast.

Bewaartermijnen

Dergelijk informatiebeheer stelt de Belastingdienst in staat om aantoonbaar te voldoen aan de wettelijk vastgestelde bewaartermijnen. Hiermee ondersteunen we het leidend beginsel "Ik weet dat de Belastingdienst mijn gegevens niet langer bewaart dan wettelijk is toegestaan"[24].

Autorisaties

De kwaliteit van het informatiebeheer is in sterke mate bepalend voor de kwaliteit van de informatievoorziening, waarbij informatie wordt verstrekt op basis van autorisaties.

B/CFD stelt als archiefbeheerder kaders voor de archivering en stelt instrumenten ter beschikking voor archiefbeheer zodat kan worden voldaan aan gestelde eisen. De eisen aan archiefbeheer worden bij het ontwerp van processen en informatiesystemen meegenomen en geborgd in de concernarchitectuur.

Vanuit de toezichthoudende taak van B/CFD[25] wordt de informatiehuishouding jaarlijks middels een monitor getoetst of deze voldoet aan de normen en of er aanleiding is tot verbetering.

Afvoer en vernietiging

Een onbedoelde vorm van informatieuitwisseling betreft afvoer en vernietiging van ICT materieel, waaronder we hier met name Pc's, laptops, tablets, verwijderbare of externe harde schijven en USB-sticks verstaan.

Afvoer gebeurt door Domeinen Roerende Zaken (DRZ), volgens de regelgeving voor afvoer materieel[26] en de *Regeling materieelbeheer rijksoverheid 2006*[27], waarin onder meer de bepalingen voor registratie en beheer staan opgenomen. De verantwoordelijkheid en risico's blijven bij de Belastingdienst tot de formele overdracht aan DRZ (proces-verbaal van acceptatie).

Meldplicht bij datalekken van persoonsgegevens

Een andere onbedoelde vorm van informatieuitwisseling betreft datalekken. Deze moeten worden gemeld zoals de Wet bescherming persoonsgegevens voorschrijft met de meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens.

Een melding van een datalek gebeurt aan de Autoriteit Persoonsgegevens[28]. De meldplicht geldt wanneer de nadelige gevolgen zich hebben voorgedaan en dat er ernstige nadelige gevolgen zijn voor de bescherming van de verwerkte persoonsgegevens. *Ernstig* wordt bepaald aan de hand van de aard en omvang van de inbreuk, de aard van de gelekte persoonsgegevens en de mate waarin technische beschermingsmaatregelen zijn getroffen. De ernst wordt ingeschat en hoeft niet te zijn gebleken, zodat dit van geval tot geval moet worden beoordeeld. Voorts geldt dat alleen gemeld moet worden als de gelekte

[24] Leidend beginsel bij afspraak 9 uit het Toetsingskader Architectuurboard Belastingdienst.
[25] Regeling Archiefbeheer Belastingdienst 2011
[26] Vanaf 1 juli 2010 vernietigt DRZ alle af te voeren ICT middelen (shredder)
[27] Handboek Financiële Informatie en Administratie Rijksoverheid (Hafir), MvF, 18 april 2006
[28] Voorheen het College Bescherming Persoonsgegevens

persoonsgegevens niet op passende wijze zijn beschermd, bijvoorbeeld door versleuteling, anonimisering of *remote wipe*. Bovendien wordt er gemeld aan de betrokkenen als er waarschijnlijk ongunstige gevolgen zijn voor zijn of haar persoonlijke levenssfeer.

Sancties

Specifieke overtredingen

De Autoriteit Persoonsgegevens heeft de bevoegdheid om aan verantwoordelijken en bewerkers bestuurlijke boetes op te leggen voor een groot aantal specifieke overtredingen van de Wbp, zoals het verwerken van persoonsgegevens zonder legitiem belang of zonder rechtvaardigingsgrond (bijv. toestemming), het gebruik van persoonsgegevens voor onverenigbare doeleinden, het te lang bewaren van persoonsgegevens, schending van de beroepsgeheimhoudingsplicht, het niet of onvoldoende nemen van beveiligingsmaatregelen, overtreding van het verbod op verwerken van bijzondere gegevens (zoals etniciteit, gezondheidsgegevens en strafrechtelijke veroordelingen) of het BSN nummer, het niet of onvoldoende informeren van de betrokkene over het privacybeleid van de organisatie, het niet melden van een datalek, niet voldoen aan inzage-, of correctieverzoeken of het negeren van het recht van verzet, en het overtreden van de regels rond data-export naar niet-Europese landen.

Geheimhoudingsplicht

De Autoriteit Persoonsgegevens heeft ook de mogelijkheid om aan individuele werknemers een boete op te leggen voor het niet naleven van hun geheimhoudingsplicht.

B.1.5. Beleid op gebruik van mobiele apparatuur

Mobile devices

De inzet van ICT-middelen wordt steeds meer geharmoniseerd met rijksbrede ontwikkelingen. De hoofdlijn hiervan is: functionaliteit komt los van het eronder liggende apparaat. Dit geldt voor alle applicaties. Naast bedrijfsapplicaties is er het interne en rijksbrede ICT-aanbod voor persoonlijke productiviteit. We spreken dan over digitaal, online samenwerken en aanvullende applicaties. Hierin vallen zaken als e-mail, agenda, contacten, kantoor- en applicaties voor specifieke taken.

Footprint

Voor alle functionaliteiten geldt: de afhankelijkheid met het apparaat wordt gereduceerd tot een minimale *footprint*. Dat betekent dat functionaliteit alleen nog via de browser en/of een mobiele app aangeboden wordt. Ook alle identiteits- en autorisatiefuncties worden op (of achter) dit concept gebouwd.

Appstores

Beveiliging van data en het netwerktransport er van zal op het niveau van de functionaliteit (browser of app) plaatsvinden. Tussen browser of app en de *rijkscloud* zal een veilige verbinding zorgen voor de exclusiviteit van gegevens in (met name) het primaire proces. In de Belastingdienst en rijksbrede 'appstores' zal het formeel toegekende aanbod aan apps beschikbaar komen.

B.1.5.1. Gebruik van mobiele apparatuur in het buitenland

Wanneer de noodzaak bestaat om mobiele apparatuur mee te nemen naar of te gebruiken in het buitenland, dient toestemming gevraagd te worden aan de direct leidinggevende. Impliciet in deze toestemming wordt het risico geaccepteerd dat bij een grenscontrole het wachtwoord moet worden afgegeven, zodat de medewerker geen integriteitsrisico loopt. Wel dient het wachtwoord zo snel mogelijk daarna te worden gewijzigd.

B.1.5.2. Beheer van mobiele apparatuur

Centraal beheerd

De Belastingdienst voert centraal beheer uit op mobiele apparatuur voor de ondersteuning en beveiliging er van. Het richt zich op alle mobiele apparaten die verbinding (willen) maken met de Belastingdienst-infrastructuur of diensten

en werkt daarmee in principe apparaatonafhankelijk. Het gaat uit van de te gebruiken functionaliteiten (apps, diensten) om op een apparaat bepaalde(beveiligings) instellingen af te dwingen. De eisen die achter deze instellingen zitten, worden ingegeven vanuit de exploitatie (CIE) samen met de business (bedrijfsonderdelen).

Keuze bij medewerker

Het logische gevolg hiervan is dat we niet alle apps of diensten op alle soorten apparaten ondersteunen en dat het niet-accepteren van onze instellingen inhoudt dat een bepaalde functionaliteit in dat geval niet kan worden gebruikt.

Er wordt permanent toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Daarom wordt een algemeen basisniveau ingesteld aan de hand van *best practices*. Aanvullend maken we bepaalde keuzes die bij onze organisatie en cultuur passen, maar wel generiek zijn. Deze keuzes worden hieronder toegelicht.

B.1.5.3. Instellingen op mobiele apparatuur

Vertrouwen en verantwoordelijkheid

Bij de bepaling van de verschillende instellingen gaan we uit van het vertrouwen in onze medewerkers, waarbij een grotere vrijheid past bij de eigen verantwoordelijkheid. De medewerkers blijven altijd wel gehouden aan het hiertoe opgestelde gebruiks- en privacybeleid. De generieke keuzes zijn als volgt:

Wachtwoorden voor toegang

- We stellen eisen aan de minimale lengte en samenstelling van de toegangscode tot het apparaat. Afhankelijk van de ontwikkelingen en het gebruik van vertrouwelijke gegevens op het apparaat, stellen we aanvullende eisen aan de lengte en samenstelling van de code;
- We vereisen een periodieke wijziging van de toegangscode;
- Na een beperkt aantal mislukte pogingen tot toegang wordt het apparaat teruggezet naar fabrieksinstellingen (gewist).

Versleuteling van de gegevens

- Gegevens die op het apparaat worden opgeslagen moeten worden versleuteld;
- Op iOS apparaten worden gegevens versleuteld zodra een wachtwoord is ingesteld. Op Android apparaten wordt versleuteling op applicatie/containerniveau afgedwongen;
- De eisen die we aan versleuteling stellen zijn marktconform.

Blokkeren van toegang bij afwijkingen

- Wanneer een apparaat afwijkt van de af te dwingen instellingen (non-compliance), wordt de toegang tot de infrastructuur geblokkeerd en/of worden de zakelijke gegevens gewist en/of wordt een melding aan de beheeromgeving gedaan. Dit laatste gebeurt bijvoorbeeld wanneer het apparaat een bepaald aantal dagen niet met de infrastructuur verbonden is geweest;
- Wanneer de noodzakelijke beheercomponenten of accounts van het apparaat worden verwijderd wordt de toegang geblokkeerd. Dit gebeurt ook bij jailbreaking of rooting van een apparaat of bij het uitzetten van de versleuteling;
- We stellen eisen aan (versies van de) besturingssystemen op het apparaat.

Wissen van mobiele apparaten

Remote wipe

- Een apparaat kan door de medewerker zelf of de servicedesk worden gewist, waarbij er onderscheid gemaakt kan worden tussen zakelijke en privégegevens.

Privacy van medewerkers

Geïnstalleerde apps

- De aanwezigheid (installatie) van de noodzakelijke beheercomponenten op een apparaat wordt bijgehouden (gesynchroniseerd). Deze synchronisatie omvat ook de andere op het apparaat geïnstalleerde apps en kan worden gebruikt voor licentiedoeleinden en het kunnen weren van ongewenste apps (blacklist);

Laatst bekende locatie

- De locatiegegevens worden alleen gebruikt voor het bijhouden van de laatst bekende locatie ten behoeve van het terugvinden van het apparaat of in het kader van strafrechtelijk onderzoek bij diefstal.

Indien er sprake is van een redelijke verdenking of vermoeden van ongeoorloofd handelen kan in opdracht van het management en DGBel/JZ in het kader van een integriteitsonderzoek de locatiefunctionaliteit worden gebruikt.

B.1.6. Beleid op telewerken/thuiswerken

Telewerken in de zin van plaats- en tijdsonafhankelijk werken zal in onze organisatie een prominentere rol krijgen. Hierin sluiten we aan bij de tendens in de rijksdienst, waarin actief wordt ingespeeld op de mogelijkheden die de ICT biedt. De Raamregeling Telewerken[29] is ook voor onze organisatie van toepassing.

Vrijwilligheid

Deze regeling staat echter los van de beleidsmatige wenselijkheid van telewerken, waarbij de medewerker werkzaamheden verricht in of vanuit zijn of haar woning. Zo gauw deze werkvorm niet is vereist vanuit de functie van een medewerker, wordt deze per definitie op basis van vrijwilligheid toegepast De raamregeling geeft wel meer duidelijkheid over de rechtspositionele aspecten van telewerken zodat toepassing ervan op dat vlak zorgvuldig kan gebeuren.

Telewerken wordt in onze organisatie uitsluitend op basis van vrijwilligheid toegepast: het is geen recht. Maar het is ook geen plicht: er zijn bijvoorbeeld geen functies waarbij de plaats van tewerkstelling de woning van de medewerker is. De organisatie is niet verplicht om telewerkvoorzieningen te verschaffen.

Keuze aan bedrijfsonderdeel

Zoals de raamregeling ook voorstaat, worden afspraken over de invoering van telewerken het best op decentraal, dat wil zeggen op bedrijfsonderdeelniveau, gemaakt. Uiteindelijk wordt de afweging tot telewerken door leidinggevende en medewerker samen gedaan.

DWB en DWR

Telewerken sluit aan bij de mogelijkheden die de Digitale Werkomgeving Belastingdienst[30] (DWB) biedt. DWB is gericht op plaats-, tijd- en apparaatonafhankelijk werken en houdt eveneens rekening met de eisen die aan de mobiliteit van de medewerkers worden gesteld vanuit de organisatiegerichte huisvesting. DWB volgt in principe de Digitale Werkomgeving Rijk die eveneens in de I-strategie Rijk wordt benoemd.

De functionaliteit van DWB wordt uiteindelijk gekoppeld aan *digitale profielen* van onze medewerkers, waarbij beheer en beheersing van risico's is ingeregeld. In principe is de functionaliteit ontkoppeld van het gebruikte soort apparaat.

TPAW

Steeds meer medewerkers zijn in staat de werkzaamheden tijd-, plaats- en apparaatonafhankelijk (TPAW) uit te voeren voor de Belastingdienst. Dit maakt

[29] Raamregeling Telewerken, BZK, 1 juni 2001.
[30] De Digitale Werkomgeving Belastingdienst volgt de Rijkswerkomgeving.

ons flexibeler in waar en wanneer we ons werk doen maar vraagt een grote mate van zelfstandigheid, zorgvuldigheid en verantwoordelijkheid van ons. Privé en werk lopen vaker in elkaar over en ieder voor zich moet hierin een balans vinden. Er wordt van je verwacht dat je werk van goede kwaliteit is en volgens de gemaakte resultaatafspraken wordt opgeleverd.

Zaken als afspraken nakomen, frequent en helder communiceren over het werk en je beschikbaarheid worden nog belangrijker. Een verantwoorde omgang met gevoelige data en informatie is vereist als deze informatie op afstand wordt geraadpleegd.

HNW

De visie van de Belastingdienst op Het Nieuwe Werken (HNW) en TPAW is bepaald[31]. Ons eigen zakelijk social media platform ConnectPeople biedt een veilige en beveiligde manier van samenwerken en communiceren over het werk.

BYOD/CYOD/COPE

Er zijn rijksbrede beleidskaders[32] voor het werken op eigen apparatuur. Hierin wordt onderscheid gemaakt tussen apparatuur "buiten beheer", "met enig beheer" en "met extra beheer". De eerste categorie is te associëren met *bring your own device*, de tweede met *company owned, personally enabled* of *choose your own device*, zoals dit in de Belastingdienst is ingevoerd. Er zijn nog witte vlekken op dit relatief nieuwe terrein, zoals de financiële en juridische consequenties, aansprakelijkheid, arbeidsvoorwaarden etc. die hierbij komen kijken. Bij de invoering van HNW wordt hier aandacht aan besteed en we volgen de (toekomstige) rijksbrede beleidskaders op dit vlak.

De Belastingdienst gebruikt Enterprise Mobility Management voor het beheer van mobiele devices. Hiermee worden (beveiligings)instellingen afgedwongen voor alle mobiele devices die verbinding hebben met onze infrastructuur.

Apps

In het verlengde van het bedoelde gebruik van mobiele apparatuur geldt als richtlijn dat wanneer applicaties (*apps*) op de mobiele devices worden gebruikt met vertrouwelijke gegevens ofwel ter ondersteuning van bedrijfsprocessen, dat deze door de Belastingdienst of Rijksoverheid moeten worden verstrekt. Apps die niet in eigendom of licentie zijn bij de Belastingdienst of Rijksoverheid dienen hiervoor niet gebruikt te worden. Zie hiervoor ook de cloudstrategie in paragraaf B.1.4.

Beveiliging van apps omvat niet alleen de technische maatregelen maar raakt vooral ook de bewustwording van de medewerker. Daarnaast vormt onvoldoende aandacht voor monitoring en beheer een groot afbreukrisico. De business dient een bewuste afweging te maken tussen beveiliging en functionaliteit.

Eigen apparatuur

Telewerken is in eerste instantie gericht op toegang tot de interne algemene informatiebronnen (intranetten), e-mail en agenda en is geschikt voor gebruik op apparatuur "buiten beheer", zij het met enige aanvullende maatregelen zoals versleuteling en twee-factor authenticatie (*bring your own device*), meestal in de vorm van de eigen thuis-PC van de medewerker.

Hier treffen we adequate aanvullende maatregelen voor bijvoorbeeld de verbinding en het desbetreffende apparaat (eisen aan de browserversie, versleuteling, wissen van elektronische sporen etc, gedragsvoorschriften).

[31] Visiedocument Het Nieuwe Werken, MT BD, maart 2013
[32] BZK/DGOBR en ICCIO *Rijksbrede beleidskaders voor ondersteuning apparaatonafhankelijk werken*, november 2012 Gebaseerd op de *I-strategie Rijk* en notitie *Rijksbrede ambities rondom Tijd-, Plaats- en Apparaatonafhankelijk Werken (TPAW)*, juli 2012

Bedrijfsmiddelen

Voorts kan telewerken worden ingericht met behulp van Belastingdienst apparaten "met enig beheer" waarbij toegang tot bedrijfsapplicaties tot de mogelijkheden behoort. Het betreft dan bedrijfsmiddelen (*choose your own device*) waarbij ook extra beveiligingsmaatregelen en gedragsregels horen.

Extra bescherming

Er dienen afdoende en zoveel mogelijk generiek aanvullende maatregelen te worden getroffen. Denk in de techniek aan *browsercache-cleaners* waarmee informatie die ongemerkt is achtergebleven wordt verwijderd en *host-checkers* die vooraf controleren of een platform op een afdoende onderhouden niveau zit of dat vereiste antivirusmaatregelen zijn getroffen.

Bedrijfsonderdelen kunnen bepaalde vormen van telewerken verbijzonderen en daarbij aanvullende maatregelen treffen.

Randvoorwaarden telewerken

Telewerken stelt het vertrouwen in de medewerker centraal, zowel wat betreft integriteit, houding en gedrag, als op het gebied van beveiliging.

Aanvullend vindt de toegang tot het bedrijfsnetwerk minimaal plaats op basis van twee-factor authenticatie en versleuteling en worden er minimumeisen gesteld aan de apparaten waarmee toegang wordt verkregen, waarbij verplichte installatie van Belastingdienst-controleprogrammatuur tot de mogelijkheden behoort. Daarnaast gelden er (gedrags)voorwaarden aan het gebruik van voorzieningen voor telewerken.

Taak- of kenniswerker, mobiel of op kantoor

De digitale profielen sluiten in de basis aan bij de vier typologieën die voor de medewerkers worden gehanteerd in de Meerjarenvisie Huisvesting: de taakwerker en kenniswerker op kantoor en de mobiele taakwerker en kenniswerker. Elke groep heeft specifieke eisen voor wat betreft functionaliteit en eisen die vanuit de organisatie worden gesteld. De invulling van de eisen moet met behulp van profielen en privileges worden beheerd.

Overigens wordt door de invoering van HNW het onderscheid tussen de groepen minder zichtbaar.

B.1.7. Beleid op het gebruik van internet en e-mail

Geheimhoudingsplicht

Het gebruik van internet is niet zonder risico's. E-mailberichten kunnen door veel partijen worden gelezen of gewijzigd. Hyperlinks in berichten kunnen worden misbruikt. Het vinden van informatie is eenvoudig, maar we weten vaak niet of die informatie ook betrouwbaar is. Als je informatie naar buiten brengt, kan dat leiden tot het niet nakomen van de geheimhoudingsplicht. Ook mag je geen standpunt innemen dat het goed functioneren van jezelf in je functie of de overheid belemmert.

E-mail mag worden gebruikt voor de uitwisseling van vertrouwelijke informatie of formele berichten mits we vooraf aanvullende maatregelen hebben getroffen en afspraken hebben gemaakt ten aanzien van het borgen van vertrouwelijkheid en authenticiteit van een bericht. Deze kunnen anders niet voldoende gewaarborgd worden, waarmee de geheimhoudingsplicht in het geding komt. Als deze maatregelen niet getroffen zijn, dienen zulke berichten op de gebruikelijk manier, zoals per post, te worden verzonden.

Terughoudendheid

De BelastingTelefoon (Roadmap Digitale Dienstverlening) positioneert e-mail niet als massaal kanaal maar voor één op één contacten, met de nodige terughoudendheid.

Hyperlinks

E-mail wordt eventueel gebruikt voor berichten als notificaties en statusupdates. De Belastingdienst gebruikt nooit hyperlinks in e-mailberichten vanwege het risico op misbruik door cybercriminelen.

Goed ambtenaarschap

In het gebruik van internet, e-mail en online communicatie wordt van de medewerkers *goed ambtenaarschap* verwacht. Daarom stelt de Belastingdienst

voorwaarden aan het gebruik van internet. Ze zijn gebaseerd op de Personele Uitvoeringsbepalingen Belastingdienst (PUB) en geven een nadere invulling aan het begrip *goed ambtenaar* zoals bedoeld in artikel 50 van het Algemeen Rijksambtenarenreglement.

Scannen en loggen

Overigens wordt er permanent toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Alle communicatiestromen (inclusief versleutelde) worden hiertoe gescand en gelogd. Verwerkingen van persoonsgegevens worden verricht met inachtneming van de Wet bescherming persoonsgegevens.

Risicoanalyse en -acceptatie

Ten behoeve van het gebruik van internet op de werkplek wordt toegang geboden volgens het principe van black- en whitelisting. Wijzigingen hierin dienen vooraf te worden beoordeeld onder meer op basis van risicoanalyse en -acceptatie door zowel het Security Operations Center (aanbodzijde) als het betrokken management (vraagzijde).

B.1.8. Beleid op het gebruik van sociale media

Werk en privé

Sociale media zijn in deze tijd niet meer weg te denken. Privé gebruik je het om contacten te onderhouden, foto's met vrienden te delen, deel te nemen aan discussies, filmpjes te bekijken etc. Maar ook voor je werk wordt het gebruik van sociale media steeds belangrijker. Hoe ga je nu goed met dit platform om en waar ligt de grens tussen werk en privé?

Sociale media zijn media die voor jouw werk bij de Belastingdienst veel voordelen hebben. Zo kun je snel en makkelijk informatie opzoeken, met collega's van gedachten wisselen, op de hoogte blijven van nieuwe ontwikkelingen en inzicht krijgen in wat de buitenwereld over de Belastingdienst en dienstverlening denkt, zodat we deze constant kunnen verbeteren. De Belastingdienst moedigt het dan ook aan, dat je actief gebruik maakt van al deze mogelijkheden.

Het gebruik van sociale media is echter ook gebonden aan bepaalde regels. Net als bij andere soorten van communicatie, zijn de drie basiswaarden van de Belastingdienst leidend: geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid. Daarbij is het van groot belang te bedenken dat wat je op internet plaatst lange tijd beschikbaar blijft en makkelijk door anderen kan worden gebruikt of misbruikt. Het is daarom extra belangrijk om goed na te denken of de teksten, foto's en/of filmpjes die je plaatst de reputatie van de Belastingdienst kunnen schaden of de organisatie in verlegenheid kunnen brengen. Blijf daarom zakelijk in je uitlatingen en bespreek en deel nooit gevoelige informatie online over de Belastingdienst, onze klanten, partners of over elkaar. Dit betekent ook dat je geen collega's of andere belanghebbenden van de Belastingdienst citeert.

Persoonlijke titel

Omdat je sociale media zowel voor je werk als voor privédoeleinden gebruikt is het belangrijk om duidelijk aan te geven wanneer je als medewerker van de Belastingdienst online actief bent en wanneer op persoonlijke titel.

Ook wanneer je op persoonlijke titel informatie online zet is het altijd belangrijk na te denken, of dat wat je zegt en/of laat zien de Belastingdienst geen schade kan berokkenen. Kortom: gedraag je online ook als goed ambtenaar net zoals je dat offline zou doen, respecteer elkaars privacy, wees vriendelijk en behandel de ander met respect.

Glazen huis

Daarnaast moet je je ook bewust zijn van de mogelijk negatieve effecten voor jezelf. Internetten is werken in een glazen huis. Je bent persoonlijk zichtbaar. Realiseer je dat lezers snel achter je identiteit kunnen komen door profielen en andere informatiesporen aan elkaar te koppelen.

Als je via de pers een algemene vraag of interviewverzoek ontvangt, stuur dit dan door naar de persvoorlichter[33] van je bedrijfsonderdeel.

Aanvullend heeft het Ministerie van Algemene Zaken de *Uitgangspunten online communicatie rijksambtenaren* gepubliceerd. Deze uitgangspunten volgen we en zijn samen met het bovengenoemde opgenomen in de in mei 2011 vastgestelde *Voorwaarden aan het gebruik van e-mail, internet en online communicatie* die zijn opgenomen in de PUB.

B.1.9. Beleid op versterkte weerbaarheid

B.1.9.1. Computercriminaliteit

Cybercrime

Onder computercriminaliteit of cybercrime verstaan we alle vormen van criminaliteit die betrekking hebben op computersystemen of die met computersystemen (inclusief netwerken) worden gepleegd, zowel van binnen als van buiten de organisatie. Het gaat om (georganiseerde) criminele activiteiten waarbij gebruik wordt gemaakt van ICT.

Ze zijn gericht tegen personen, eigendommen of organisaties, of tegen elektronische communicatienetwerken en informatiesystemen.

We bestrijden computercriminaliteit door:

- Het versterken van detectie van interne en externe computercriminaliteit via monitoring van informatiesystemen, het alert maken van de medewerkers en de melding van mogelijk strafbare feiten;
- De afhandeling van meldingen, verstoringen en incidenten niet alleen gericht te laten zijn op continuïteit van de bedrijfsvoering, maar ook op het verzamelen van bewijsmateriaal en het veiligstellen van gegevens die kunnen helpen bij opsporing, vervolging en het eventueel verhalen van schade;
- Aansluiting te hebben met het NCSC en het in overleg met DGBel/JZ doen van aangifte van computercriminaliteit bij de politie.

Phishing

Voor de afhandeling van *phishingmails* is een proces ingeregeld zowel intern voor medewerkers als extern voor burgers, bedrijven en organisaties. De meldingsprocedure hiervoor dient helder en het loket goed vindbaar te zijn. In samenwerking met het NCSC worden vervolgacties ondernomen.

B.1.9.2. Spionage

KWAS

Mede naar aanleiding van de kabinetsreactie op het rapport *Kwetsbaarheidsanalyse Spionage Nederland (KWAS)* van de Inspectie Openbare Orde en Veiligheid[34] zijn de *cruciale belangen* van de Belastingdienst in kaart gebracht en vastgesteld. Onder een cruciaal belang verstaan we een verzameling van gegevens waarvan onbevoegde kennisname onze bedrijfsbelangen aantast en waarvan redelijkerwijs aangenomen kan worden dat andere partijen er interesse in hebben[35].

Indien opportuun wordt in de rapportagecyclus rekening gehouden met dreigingen vanuit spionage.

[33] De Instructie Perscontacten is op Belastingnet te vinden
[34] Vanaf 16 april 2012 de Inspectie Veiligheid en Justitie
[35] Definitie uit de Handleiding KWAS, BZK/AIVD januari 2011

Backdoors

In dit kader dienen er ook garanties te zijn dat onze gegevens veilig zijn bij verwerking door (*closed source*) programmatuur en over in hoeverre leveranciers de vertrouwelijkheid van onze gegevens kunnen waarborgen.

Sourcecode

De door ons (of in opdracht) ontwikkelde programmatuur en met name broncode behoeft daarbij conform de cruciale belangen passende bescherming, onverlet het intellectueel eigendom.

Hier ligt ook een relatie met de meldplicht op datalekken. Deze onderwerpen hebben rijksoverheidsbreed verhoogde aandacht[36]

B.1.9.3. Responsible disclosure

Beveiligingsonderzoek

Beveiligingsonderzoekers en goedwillende (white-hat) hackers kunnen een belangrijke rol vervullen in het veelal via internet zichtbaar maken van kwetsbare systemen. Momenteel bestaat er bij beveiligingsonderzoekers angst om kwetsbaarheden rechtstreeks bij een bedrijf of organisatie te melden, onder andere door de kans op strafrechtelijke vervolging.

Door met hen samen te werken kan de beveiligingsgemeenschap onze ICT-veiligheid verhogen. Daarbij geven we aan hoe we met de melding van een beveiligingsonderzoeker omgaan en leggen de afspraken over deze van waarborgen voorziene handelswijze vast en dragen die uit. Een belangrijk voordeel hiervan is dat we de tijd krijgen om een lek te dichten, voordat het publiek gemaakt wordt.

SOC

Het CIE/Security Operations Center bewaakt deze handelswijze.

Eén en ander is eveneens invulling van de nadrukkelijke wens van de Minister van VenJ[37]. De *Leidraad om te komen tot een praktijk van responsible disclosure* van het NCSC is hierbij gevolgd.

B.1.10. Beleid op personele veiligheid en integriteit

B.1.10.1. Veiligheid

Fysieke veiligheid

De individuele veiligheid van onze medewerkers, bezoekers en ingehuurd personeel (de personele veiligheid) is verankerd in het voldoen aan de (arbo)wet- en regelgeving op dit gebied en heeft verwantschap met de fysieke toegangsbeveiliging uit paragraaf B.1.3.1. Een bijzonder aspect is brandveiligheid, aanvullend gericht op de bescherming van personeel, bezoekers en de omgeving van gebouwen. Hier is ook de wet- en regelgeving leidend, waaraan we dienen te voldoen.

VPT

We sluiten aan bij het programma Veilige Publieke Taak[38] dat als doel heeft agressie en geweld tegen werknemers met een publieke taak te voorkomen en de daders aan te pakken.

B.1.10.2. Integriteit

Basiswaarden

De *Gedragscode Belastingdienst – Een integere Belastingdienst*[39] beschrijft hoe onze basiswaarden geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid in de praktijk gebracht kunnen worden ten gunste van het imago van de Belastingdienst, met als doel de bereidheid van burgers en bedrijven te

[36] Notitie Tussentijds beeld 2013 aan SG-Overleg, ADR, september 2013.
[37] Kamerbrief Responsible Disclosure 336692, VenJ, 28 december 2012
[38] Programma Veilige Publieke Taak 2011-2015, BZK en VenJ, 8 juli 2011
[39] De Gedragscode is te vinden op Belastingnet

vergroten om aan hun verplichtingen te voldoen. Hiermee geeft deze code invulling aan het tactisch beleid op personeelsgedrag.

Het gaat in op de basiswaarden en integriteit, onze verantwoordelijkheden naar belastingplichtigen en externen, vertrouwelijke informatie, onze verantwoordelijkheden naar de eigen organisatie en naar elkaar.

Gedragscode Integriteit Rijk

De code past binnen de Gedragscode Integriteit Rijk[40]. Het integriteitsbeleid wordt periodiek door de Kennisgroep Integriteit geactualiseerd (zie B.4.4).

B.1.10.3. Geheimhoudingsplicht

Als medewerker van de Belastingdienst kun je toegang hebben tot vertrouwelijke en persoonlijke gegevens. Dat soort informatie mag je natuurlijk nooit voor je eigen voordeel gebruiken, aan derden ter beschikking stellen of bij nevenwerkzaamheden gebruiken. Iedere ambtenaar heeft de geheimhoudingsplicht. Uitgangspunt is dat informatie voor geen ander doel mag worden gebruikt dan waarvoor de informatie is verstrekt. Belastingplichtigen moeten erop kunnen vertrouwen dat we hun gegevens alleen gebruiken voor het werk. Ze mogen ervan uitgaan dat al hun informatie bij ons veilig is en dat we deze alleen gebruiken als dat voor het werk noodzakelijk is. Daarom tilt de Belastingdienst zwaar[41] aan de geheimhoudingsplicht van zijn medewerkers. Deze plicht blijft ook gelden als je de Belastingdienst verlaat.

Vertrouwen in overheid

B.1.10.4. Beleid op clear desk en clear screen

Behalve je geheimhoudingsplicht heb je ook de verantwoordelijkheid om te voorkomen dat gegevens bij derden (collega's of buitenstaanders) terechtkomen. Daarom voert de Belastingdienst een clear-desk beleid: vertrouwelijke gegevens mogen niet onbeschermd op de werkplek achterblijven. Je hoort alle dossiers en elektronische gegevensdragers op te ruimen in afsluitbare kasten. Verder hoor je ervoor te zorgen dat niemand bij de gegevens in jouw computer kan komen. Geef je wachtwoord aan niemand, ook niet aan je naaste collega's en schakel, als je je werkplek verlaat, meteen de schermbeveiliging in (clear screen). Realiseer je, dat deze spelregels overal gelden waar je werkt zoals op kantoor, thuis, in de trein en bij de klant.

B.1.10.5. Beleid op aanvaardbaar gebruik van bedrijfsmiddelen

De Belastingdienst stelt bedrijfsmiddelen ter beschikking om je werk te kunnen doen. Er wordt van je verwacht dat je hier zorgvuldig mee omgaat.

Privégebruik

Het uitgangspunt is dat privégebruik van deze bedrijfsmiddelen beperkt is toegestaan. We realiseren ons, dat in de huidige tijd werk en privé steeds meer met elkaar vermengd worden. Desondanks is het niet de bedoeling dat je bijvoorbeeld:

- vaak of lang privégesprekken voert met de telefoon van de werkgever;
- Privé- of illegale content downloadt op gegevensdragers van de Belastingdienst;
- vaak of veel kopieert voor privégebruik;
- allerlei materiaal meeneemt voor privégebruik;

[40] Gedragscode Integriteit Rijk, BZK/DGOO, oktober 2016,
[41] De Autoriteit Persoonsgegevens heeft daarnaast de bevoegdheid sancties op te leggen aan individuele werknemers bij het niet naleven van de geheimhoudingsplicht

- dienstauto's en andere bedrijfsmiddelen anders dan bedoeld gebruikt.

Sluitende regels zijn niet te geven. Wanneer je bedrijfsmiddelen voor privédoeleinden wilt gebruiken, moet je je dus afvragen of je hiervoor goede redenen hebt.[42]

Voorwaarden en gedragsregels

Voor ter beschikking gestelde ICT bedrijfsmiddelen met een verhoogd beveiligingsrisico hanteren we stringente (ondertekende) voorwaarden en gedragsregels. Denk hierbij aan *tokens* voor 2-factor authenticatie of door de Belastingdienst verstrekte smartphones of tablets. Overtreding van dergelijke regels kunnen worden aangemerkt als plichtsverzuim.

B.1.10.6. Arbeidsvoorwaarden

Voor de medewerkers geldt het Algemeen Rijksambtenarenreglement (ARAR) en de Personele Uitvoeringsbepalingen Belastingdienst (PUB), waarin onder meer de wederzijdse verantwoordelijkheden ten aanzien van beveiliging staan beschreven.

Hieronder vallen ook de verplichting om de eed of belofte af te leggen (artikel 51 ARAR) en de geheimhoudingsplicht (artikel 1.5 PUB, artikel 125a Ambtenarenwet)[43], de registratie van het identiteitsbewijs en het overleggen van een Verklaring Omtrent het Gedrag (VOG).

Voor de VOG dient de handleiding *Werkwijze Verklaring omtrent het Gedrag (VOG)*[44] te worden gebruikt.

Voor tijdelijk (ingehuurd) personeel en stagiaires gelden aanvullende maatregelen waaronder het expliciet tekenen van een geheimhoudingsverklaring en het overleggen van een VOG.

B.2. Basis beveiligingsniveau en risicoafweging

Subsidiariteit

Voor het merendeel van de processen en ondersteunende informatiesystemen (volgens VIR 2007) kunnen maatregelen worden getroffen volgens het basis beveiligingsniveau. Specifieke maatregelen worden getroffen op basis van een risicoafweging. Deze zijn nodig als de kenmerken van de processen en ondersteunende informatiesystemen afwijken ten opzichte van het basisniveau. Afwijkende situaties hebben betrekking op een ander dan het hier geformuleerde dreigingenprofiel, maar kunnen ook betrekking hebben op hogere beschikbaarheidseisen, voor wat betreft de Belastingdienst ongeëigend gebruik van of nieuwe technologie, gegevens met een bijzonder belang etc.

Proportionaliteit

Er zijn meer factoren op grond waarvan er in specifieke situaties afgeweken kan worden van de basismaatregelen: te hoge kosten, onvoldoende haalbaarheid, de mate van effectiviteit in de specifieke situatie, de ouderdom van het gebouw of van het informatiesysteem, etc. Die factoren vormen de randvoorwaarden.

Stelsel van maatregelen

Bij het niet-implementeren van maatregelen op het basisniveau zal eveneens een risicoafweging moeten plaatsvinden: weegt de besparing van de maatregel op tegen de kans van het optreden van de dreiging, waartegen de maatregel

[42] Regels voor het gebruik van bedrijfsmiddelen staan beschreven in Rijksportaal/Personeel/Dienstverband/Integriteit/Gebruik van bedrijfsmiddelen/mijn organisatie

[43] Nadere informatie is te vinden op het Rijksportaal. De fiscale geheimhoudingsplicht staat beschreven in artikel 67 AWR

[44] B/CA Unit Concerncontrol & Analyse, juni 2015 (http //intranet.belastingdienst nl/cso/)

een bijdrage levert. Hierbij speelt mee dat er meestal ook andere maatregelen zijn, die een bijdrage leveren aan het beperken van het risico.

Risicoafweging

Bij een risicoafweging worden de bedreigingen benoemd en in kaart gebracht. Per bedreiging wordt de kans van het optreden ervan bepaald. Vervolgens wordt nagegaan wat de schade is die zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet. Daarna worden analyses gemaakt van de kosten van te treffen maatregelen versus de baten van de hiermee te vermijden schaden of wordt bezien of de risico's kunnen worden vermeden, bijvoorbeeld door een andere procesimplementatie of het gebruik van beter beveiligbare ICT-middelen.

Accepteren van restrisico's

Tenslotte worden de restrisico's door het management geaccepteerd. Op basis van de onderkende risico's worden compenserende maatregelen (bovenop het basisniveau en passend in het bestaande stelsel) getroffen.

Methoden en standaarden

Vakkundigheid

Voor het maken van risicoafwegingen bestaan vele methoden, standaarden en praktische uitwerkingen daarvan. Vooralsnog is er geen standaard methode ontwikkeld, die zich richt op specifieke bedreigingen bovenop de "normale" waarop het basisniveau is gebaseerd. Het beoordelen welke extra maatregelen geschikt zijn om de extra bedreigingen af te dekken is een zaak van vakkundige beoordeling en het rekening houden met de randvoorwaarden. Er is geen methode die dat kan overnemen.

CRSA, IRAM

Voor de verplicht gestelde risicoanalyse bij nieuwe projecten of majeure wijzigingen worden in de IV-keten methoden als Control & Risk Self Assessment (CRSA) en Information Risk Analysis Methodology (IRAM) gebruikt.

PIA

Met ingang van 1 september 2013 is het rijksbrede Toetsmodel Privacy Impact Assessment (PIA) verplicht. De Belastingdienst heeft een eigen PIA- instrument ontwikkeld dat expliciet geschikt is voor zijn uitvoeringspraktijk.

Veranderde omgeving

Maar ook voor bestaande infrastructuur, programmatuur en diensten dient te worden gekeken naar nieuwe risico's in een veranderde omgeving, zeker als deze dicht bij internet komt of mobiel is. Met name komen dan in aanmerking DWB, apps, mobiele apparatuur, netwerkverbindingen, remote of draadloos werken tot *Voice over IP*.

APK voor veilige exploitatie

Dit verstaan we onder *veilige exploitatie*, waarbij bijvoorbeeld periodiek een verplichte aanvals- en penetratietest wordt uitgevoerd, vergelijkbaar met een Algemene Periodieke Keuring.

Het strekt tot aanbeveling om de uitkomsten van de diverse analyses te aggregeren en centraal beschikbaar te maken zodat de opgedane kennis kan worden hergebruikt en de business verantwoordelijkheid kan nemen in de risicoacceptatie.

ISMS

Daartoe kunnen hulpmiddelen zoals een Information Security Management System op basis van NEN-ISO 27001 worden ingezet.

B.3. Pas toe of leg uit

Verplichte beheersmaatregelen en te volgen implementatierichtlijnen

Comply or explain

In hoeverre zijn beheersmaatregelen en implementatierichtlijnen verplicht? Beheersmaatregelen zijn verplicht, tenzij aangetoond kan worden dat ze niet van toepassing zijn. Implementatierichtlijnen zijn niet verplicht, maar omdat ze als *best practice* zijn vastgesteld moet bij het afwijken ervan aangetoond worden dat een andere implementatie tot het voldoen aan de beheersmaatregel leidt. Hierbij hanteren we het principe van *comply or explain*: pas toe of leg uit.

PDCA cyclus

Er dient aandacht te worden besteed aan het inpassen van de maatregelen in de PDCA cyclus[45].

Hierbij zijn de volgende kanttekeningen te maken:

- Om te voldoen aan een beheersmaatregel zal op basis van de implementatierichtlijnen in- of externe controle moeten worden uitgeoefend. Indien van de *best practice* wordt afgeweken zal eerst (bij voorkeur in een operationeel beleidsdocument) gemotiveerd moeten worden en vastgelegd hoe de beheersmaatregel anders wordt geïmplementeerd om in- of externe controle mogelijk te maken.
- Als bij de gezamenlijke evaluatie van het normenkader door allen die het moeten toepassen, blijkt dat velen tot een andere implementatie komen, zal de *best practice* moeten worden aangepast.

[45] De Autoriteit Persoonsgegevens legt in de richtsnoeren meer de nadruk op de PDCA cyclus

B.4. Opbouw van de beveiligingsorganisatie

B.4.1. Sturing van beveiliging

De sturing van beveiliging benaderen we vanuit verschillende gezichtspunten.

Maatregelsturing

- **Sturing op de maatregelen**: deze verloopt langs de primaire verantwoordelijkheidsverdeling van de Belastingdienst. Beveiliging is een integraal onderdeel van de bedrijfsvoering en alle soorten maatregelen, die een organisatie treft om haar doelen te bereiken. Beveiliging is één van de vele aspecten waarop in samenhang moet worden gestuurd;

Aspectsturing

- **Lijnsturing op het aspect**: deze verloopt langs de lijn van de CFO's. Hierbij gaat het om de managementverantwoordelijkheid voor het aspect beveiliging met een accent op naleving van beveiligingskaders en samenhang van de maatregelen binnen het competentiegebied;

Functionele sturing

- **Functionele sturing**: deze verloopt van de strategisch beveiligingsadviseur tot de beveiligingsmedewerker en draagt bij zowel aan de lijnsturing op het aspect als de sturing op maatregelen.

B.4.2. Strategische beveiliging in het MT Belastingdienst

De invulling van strategische beveiliging staat beschreven in Deel A, paragraaf A.4.1.

B.4.3. Tactisch Beveiligingsoverleg (TBO)

Deelnemers TBO

De deelnemers zijn vertegenwoordigers van alle bedrijfsonderdelen.

- Voorzitter: DGBel/Cluster Bedrijf;
- Secretaris: DGBel/Cluster IV.

Inhoud overleg:

- Besluitvorming over onderhoud HBB;
- Evaluatie geaggregeerde en geanonimiseerde bedrijfsonderdeelrapportages inzake beveiliging;
- Evaluatie uitkomsten beveiligingsaudits;
- Voorbespreking stukken voor CFO-overleg;
- Evaluatie jaarlijkse risicoanalyses per bedrijfsonderdeel;
- Voorstellen beveiligingsaudits.

Frequentie overleg

Het TBO komt drie keer per jaar bijeen of vaker naar aanleiding van bijvoorbeeld thema's of actuele beleidsonderwerpen.

B.4.4. Clusters en kennisgroepen

De groepen zijn:

- Cluster Business Continuity Management;
- Cluster Informatiebeveiliging;
- Cluster Fysieke Beveiliging;
- Cluster Personele Veiligheid en Integriteit;
- Kennisgroep Integriteit;
- Kennisgroep Privacy.

Deelnemers clusters

De deelnemers aan de clusters zijn vertegenwoordigers van de bedrijfsonderdelen.

De taken van de clusters/kennisgroepen zijn onder meer:

- Uitwerken voorstellen tot onderhoud HBB;

- Adviseren TBO over planning en uitvoering ICP's beveiliging;
- Adviseren over risico's;
- Adviseren bij veranderingen in de organisatie.

Kennisgroep Integriteit

De Kennisgroep Integriteit is opgericht op grond van het besluit van het MT[46] met betrekking tot de uitkomsten van het project 'Revitalisering Integriteit'.

Integriteitsmanagement is een taak en verantwoordelijkheid van het management van de Belastingdienst op alle niveaus. De Kennisgroep treedt niet in die verantwoordelijkheid maar beoogt vanuit een concentratie van kennis en professionaliteit een waardevolle adviserende en ondersteunende bijdrage te leveren aan deze managementverantwoordelijkheid.

Het doel hierbij is om de snelheid, daadkracht en kwaliteit bij de ontwikkeling en evaluatie en bijstelling van het integriteitbeleid (en de bijbehorende regelgeving) te verhogen. Tevens is de Kennisgroep voor de bedrijfsonderdelen beschikbaar bij de uitvoering van het integriteitsbeleid. Dit alles vanuit een geïntegreerde bundeling van kennis en professionaliteit.

Deelnemers kennisgroep

De Kennisgroep bestaat uit integriteitscoördinatoren van alle bedrijfsonderdelen, een communicatie-expert, een (arbeids)jurist, de compliance officer, de landelijk vertrouwenspersoon integriteit, een expert onderzoeker en de voorzitter.

De samenwerking tussen de beveiligingsadviseur of -medewerker en de integriteitscoördinator op elk bedrijfsonderdeel afzonderlijk is van groot belang. Vanuit de Kennisgroep worden planning en voortgang van initiatieven, activiteiten en producten binnen het TBO gemeld en zo nodig besproken. Het resultaat van het overleg binnen het TBO wordt vermeld op door te sturen documenten richting het MT.

Kennisgroep Privacy

Als gevolg van de versterkte Europese en nationale wetgeving[47] voor gegevensbescherming en de daaraan verbonden verplichting tot *privacymanagement* is de Kennisgroep Privacy ingesteld.

De Kennisgroep Privacy monitort, signaleert en adviseert met betrekking tot de (interne) naleving van wettelijke regels bij de veilige verwerking van persoonsgegevens. De Kennisgroep heeft de ambitie om hét juridisch uitvoerings-, advies- en kenniscentrum te zijn voor de verwerking van (bijzondere) persoonsgegevens. De groep werkt samen langs de lijnen die er zijn op het gebied van informatiebeveiliging, in het bijzonder vanuit het oogpunt van *privacy by design* en *privacy by default*.

De Kennisgroep voorziet onder meer in:

- Advisering over implementatie en uitvoering van (nieuwe) wet- en regelgeving;
- Ontwikkeling en tot uitvoering brengen van beleid, onder andere in de vorm van kaders, normen, richtlijnen en (toetsings)producten;
- Actieve signalering ten aanzien van maatschappelijke en juridische ontwikkelingen en dilemma's in relatie tot gegevensverwerkingen;
- Juridische ondersteuning in de dagelijkse uitvoering van de gegevenspraktijk op het snijvlak van het mogen, willen en kunnen leveren van gegevensdiensten;
- Het geven van voorlichting, training en workshops ter bevordering van kennis en bewustzijn én zelfredzaamheid m.b.t. een zorgvuldige

[46] MT Belastingdienst d d 2 juli 2012. De Kennisgroep Integriteit is gestart per 1 januari 2013 op basis van het Startdocument Kennisgroep Integriteit v1 0 d d 13 november 2012
[47] Waar onder de Algemene Verordening Gegevensbescherming (AVG) en meldplicht datalekken/Wbp

gegevensverwerking door specialisten in het gegevensdomein;
- Het bevorderen van in- en externe samenwerking en relaties tussen specialisten, organisaties en bedrijfsonderdelen m.b.t. gegevensverwerking. Deelname aan in- en externe werkgroepen;

De Kennisgroep Privacy bestaat onder meer uit de Wbp-coördinatoren van de bedrijfsonderdelen, de Functionaris voor de Gegevensbescherming en experts uit het vakgebied.

B.4.5. Rollen en functies

Rol of functie

In de functies van beveiliging kan onderscheid worden gemaakt naar beveiligingsrollen en -functies. Met beveiligings*rol* bedoelen we het uitvoeren van een deeltaak op het gebied van beveiliging, naast de primaire hoofdtaken van een functie.

Bij de beveiligings*functies* gaan we alleen uit van de adviserende functies en niet op de uitvoerende beveiligingsfuncties die met een grote verscheidenheid overal in de organisatie van de Belastingdienst voorkomen. Denk hierbij aan: portiers- en bewakingsfuncties, security administrators, firewallbeheerders, IT-security ontwerpers etc.

BVA en FG

Naast de rollen en functies voor de (interne) beveiligingsorganisatie kennen we ook de departementale rollen van de Beveiligingsambtenaar (BVA, volgens VIR) en de Functionaris voor de gegevensbescherming (FG, volgens Wbp) die nauw betrokken zijn bij beveiliging in de Belastingdienst.

B.4.6. Beveiligingsrollen

In deze paragraaf staan de beelden van de beveiligingsrollen nader uitgewerkt.

B.4.6.1. Chief Security Officer (CSO)

Deze rol omvat de volgende taken:

- Opdrachtgever strategisch beveiligingsadviseurs;
- Vormt zich een visie op de betekenis van beveiliging voor de hele organisatie;
- Stelt doelen en beleid ter uitvoering vast;
- Draagt ervoor zorg dat er voldoende middelen voor uitvoering van het beleid aanwezig zijn;
- Draagt doelen en beleid uit in de hele organisatie;
- Draagt ertoe bij dat auditbevindingen en incidenten van ernstige aard worden opgelost.

B.4.6.2. Beleidsmedewerker voor een deelgebied van beveiliging

Deze rol omvat de volgende taken:

- Vormt zich een visie op de betekenis van het beleidsgebied binnen de hele organisatie;
- Draagt zorg voor het actueel houden van het tactisch beveiligingsbeleid voor het beleidsgebied;
- Bevordert dat er op strategisch niveau voldoende randvoorwaarden zijn voor het treffen van de beveiligingsmaatregelen op het beleidsgebied;
- Draagt doelen en beleid op het beleidsgebied uit in de hele organisatie;
- Draagt ertoe bij dat auditbevindingen en incidenten van ernstige aard binnen het beleidsgebied worden opgelost.

B.4.6.3. Integriteitscoördinator

Deze rol omvat de volgende taken:

- Draagt bij aan beleid, ontwikkeling en advies binnen het eigen bedrijfsonderdeel:
  - Inventariseert risico's;
  - Signaleert kansen en knelpunten;
  - Adviseert over bijstelling van beleid en/of uitvoering.
- Coördineert opleidingen, bewustwording en interventies op het gebied van integriteit binnen het eigen bedrijfsonderdeel:
  - Coördineert de integriteitsopleidingen;
  - Houdt zicht op het volgen van verplichte integriteitsopleidingen.
- Treedt op als aanspreekpunt binnen het eigen bedrijfsonderdeel en voor de Kennisgroep Integriteit:
  - Coördineert de aanpak van integriteitsincidenten binnen het eigen bedrijfsonderdeel;
  - Coördineert als Registratiepunt Integriteit de meldingen van vermoedens van misstanden en/of integriteitsschendingen binnen het eigen bedrijfsonderdeel.
- Neemt deel aan het integriteitscoördinatorenoverleg.

B.4.6.4. Wbp-coördinator/privacy officer

Deze rol omvat de volgende taken:

- Draagt bij aan alle privacygerelateerde onderwerpen:
  - Beleid binnen het eigen bedrijfsonderdeel;
  - Uitvoeringstoetsen, Privacy Impact Analyses (PIA), Compliance checks, convenanten;
  - Ontwikkeling van normen, kaders en sjablonen;
  - Inrichtingsproducten in de vorm van AO-IC en procesinrichting;
- Signaleert kansen en knelpunten, is kaderstellend en toetsend, adviseert gevraagd of ongevraagd over bijstelling van beleid en/of uitvoering.
- Coördineert workshops, trainingen en bewustwording op het gebied van gegevensbescherming binnen het eigen bedrijfsonderdeel.
- Is aanspreekpunt binnen het eigen bedrijfsonderdeel en voor de Kennisgroep Privacy en neemt deel aan het Wbp-coördinatorenoverleg.

B.4.6.5. Business Continuity Manager

De rol van Business Continuity Manager bestaat zowel op strategisch als op tactisch niveau (per bedrijfsonderdeel) en overbrugt (strategische) bedrijfsvoering en de (uitvoerende) lijn.

Deze rol omvat de volgende taken:

- Vormt zich een visie op de betekenis van het beleidsgebied BCM binnen de hele organisatie;
- Heeft kennis van de organisatorische inrichting van het BCM-proces;
- Stelt de BCM-visie en -beleid op op basis van de BCM-normatiek;
- Heeft kennis van bedreigingen- en kwetsbaarheidsanalyses;
- Heeft kennis van Business Impact Analyses (BIA);
- Stelt het calamiteitenplan op;

- Heeft kennis van bedrijfshulpverlening, crisismanagement, IT recovery, facilitair recovery, process recovery;
- Heeft kennis van het testen van calamiteitenplannen.

B.4.6.6. Crisismanager

Een crisismanager is tijdens een crisis onderdeel van een crisis-managementteam. Een crisis is een situatie waarbij de continuïteit van de bedrijfsvoering, de veiligheid van medewerkers (en bezoekers) en/of de reputatie van het bedrijf in gevaar is.

De rol van crisismanager omvat de volgende taken:

- Gemandateerd leidinggevende voor de gehele organisatie of bedrijfsonderdeel;
- Vastleggen besluiten en actiepunten (plotter);
- Verzorgen van de interne en externe comunicatie (communicator);
- Actiehouder voor (deel)taken (portefeuillehouder);
- Draagt bij aan het besluitvormingsproces dat een crisis moet bezweren.

Een crisismanager wordt gekenmerkt door de volgende competenties:

- Persoonlijk gedrag: durf, initiatief, schakelvermogen, stressbestendigheid, optimisme en intrinsieke motivatie;
- Management en leidinggeven: taakgericht leiderschap, plannen & organiseren, voortgangsbewaking;
- Analyse en besluitvorming: besluitvaardigheid, probleemanalyse;
- Samenwerken en communicatie: teamwork, overwicht, overtuigingskracht.

B.4.7. Beveiligingsfuncties

Functieweging

In deze paragraaf zijn de beelden van de beveiligingsfuncties nader uitgewerkt. Bij waardering van de beveiligingsfuncties wordt gebruik gemaakt van de vigerende methode van functiewaardering.

B.4.7.1. Strategisch beveiligingsadviseur

Doel van de functie

Het ontwikkelen van strategie en beleid gericht op beveiliging. Bevorderen en coördineren van de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

Functiecontext

Functioneert als zelfstandig opererend intern beleidsadviseur, ressorterend onder het lid van het MT Belastingdienst dat verantwoordelijk is voor beveiliging. Geeft functioneel leiding aan beveiligingsmedewerkers in de gehele organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het beveiligingsbeleid en het naleven van uitvoeringsrichtlijnen.

Resultaatgebieden

Leidinggeven

- Geeft functioneel leiding aan beveiligingsmedewerkers in de gehele organisatie;
- Treedt op als projectleider of opdrachtgever voor organisatiebrede projecten op het gebied van beveiliging;
- Organiseert en faciliteert overleg voor sturing en coördinatie op het gebied van beveiliging.

Plan: Beveiligingseisen

- Vormt zich een visie op de betekenis van beveiliging voor de gehele organisatie door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het organisatiebeleid;
- Stelt doelen voor beveiliging voor;
- Ontwikkelt een strategie om die doelen te bereiken;
- Ontwikkelt beleid ter uitvoering van de strategie en stelt het centraal beleids- en jaarplan samen mede op basis van de deelplannen beveiliging.

Do: Treffen maatregelen

- Bevordert het ontwikkelen van uitvoeringsrichtlijnen en geeft hieraan richting;
- Initieert voorlichtings- en IB-bewustzijnsprogramma's;
- Adviseert bij en faciliteert risicoanalyses en PIA's op niveau van de hele organisatie;
- Toetst uitvoeringsrichtlijnen aan het beleid en adviseert zonodig over verbetering;
- Bereidt organisatiebrede beslissingen op het gebied van beveiliging voor;
- Adviseert de leiding van de organisatie, bedrijfsonderdelen en de IV-organisatie bij beleid(sbeslissingen) met consequenties voor beveiliging.

Check: Evaluatie en controle

- Beoordeelt rapportages van bedrijfsonderdelen over de naleving van uitvoeringsrichtlijnen;
- Beoordeelt rapportages van in- en externe auditinstanties op relevantie voor beveiliging;
- Geeft opdrachten tot het verrichten van interne onderzoeken en audits;
- Houdt een centrale registratie bij van beveiligingsincidenten en de afhandeling en evalueert de incidenten;
- Beoordeelt ontwikkelingen in de maatschappij, de overheid en het vakgebied.

Act: Aanpassen

- Stelt IB-visie, -strategie en -beleid bij en bevordert aanpassing van uitvoeringsrichtlijnen op basis van evaluaties.

Contacten

- Intern: CSO, leiding bedrijfsonderdelen, BVA van het ministerie, andere beveiligingsfunctionarissen;
- Extern: auditors, andere overheidsbeveiligingsfunctionarissen en beroepsgenoten.

Kennisgebieden

- IV en beveiliging (breed);
- Organisatie van informatievoorziening;
- Business processen (breed).

B.4.7.2. Beveiligingsadviseur

Doel van de functie

Het ontwikkelen van beleid gericht op het naleven van kaders voor beveiliging, ondersteunen van de CFO van het bedrijfsonderdeel hierbij en toezien op de realisatie van het beleid.

Resultaatgebieden

Plan: Beveiligingseisen

- Stelt jaarlijks het beveiligingsplan voor het bedrijfsonderdeel op;
- Draagt bij aan beleidsplannen voor beveiliging vanuit het perspectief van het bedrijfsonderdeel.

Do: Treffen maatregelen

- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging, zowel centraal voor de Belastingdienst als bij het bedrijfsonderdeel;
- Draagt uitvoeringsrichtlijnen op het gebied van beveiliging actief uit in de organisatie;
- Initieert voorlichtings- en bewustzijnsprogramma's en geeft hieraan richting;
- Voert risicoanalyses uit binnen zijn competentiegebied;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen het bedrijfsonderdeel met gevolgen voor beveiliging.

Check: Evaluatie en controle

- Beoordeelt interne rapportages op beveiligingsaspecten;
- Stelt periodiek verantwoordingsrapportage op over beveiliging;
- Beoordeelt rapportages van in- en externe controle en auditinstanties;
- Adviseert de CFO inzake het verrichten van interne onderzoeken en audits;
- Zorgt voor centrale melding van beveiligingsincidenten en beoordeelt afhandeling.

Act: Aanpassen

- Stelt het jaarplan beveiliging op en adviseert over uitvoeringsrichtlijnen op basis van zijn evaluaties.

Contacten

- Intern: management bedrijfsonderdeel op alle niveaus en andere beveiligingsfuncties;
- Extern: auditors en toezichtorganen

Koppelingen

- Beveiliging
- Belastingdienst processen;
- Interne regelgeving.

Doel van de functie

B.4.7.3. Beveiligingsmedewerker

Het ondersteunen en toezien op de realisatie van beleid gericht op het naleven van Belastingdienstkaders voor beveiliging en het management van het bedrijfsonderdeel hierbij ondersteunen.

Resultaatgebieden

Plan: Beveiligingsessies

- Draagt bij aan de beleidsplannen voor beveiliging van het bedrijfsonderdeel.

Do: Treffen maatregelen

- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging bij het bedrijfsonderdeel;
- Draagt uitvoeringsrichtlijnen op het gebied van beveiliging actief uit in de organisatie;
- Draagt bij aan risicoanalyses binnen zijn competentiegebied;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen het bedrijfsonderdeel met gevolgen voor beveiliging.

Check: Evaluatie en controle

- Beoordeelt interne rapportages op beveiligingsaspecten;
- Stelt periodieke verantwoordingsrapportage op over beveiliging;
- Beoordeelt rapportages van interne controle.

Act: Aanpassen

Stelt adviezen over uitvoeringsrichtlijnen bij op basis van zijn evaluaties.

Contacten

- Intern: management bedrijfsonderdeel op alle niveaus en andere beveiligingsfuncties;
- Extern: auditors en beroepsgenotes.

Kennisgebieden

- Beveiliging;
- Beleidsmiddelen/processen;
- Bescherming persoonsgegevens;
- Interne regelgeving.

B.4.7.4. Procesarchitect Informatiebeveiliging

Doel van de functie

Het ontwikkelen en actueel houden van een visie op de deelarchitectuur voor het aspect informatiebeveiliging in de bedrijfs- of procesarchitectuur als concretisering van een deel van het strategisch beveiligingsbeleid en de positionering van generieke beveiligingsfunctionaliteiten daarbinnen.

Functionele context

Procesarchitect met als specialisatie beveiliging. Vertaalt beleidskaders voor beveiliging naar bedrijfs- of procesarchitectuur en vervult daarbij zowel een architecten- als adviseursrol. Treedt met name op als procesarchitect

voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging en auditing. Ziet toe op naleving van architectuurprincipes voor beveiliging. Houdt voortdurend zicht

op marktontwikkelingen op het gebied van beveiligingsproducten.

Resultaatgebieden

Plan: Beveiligingsaanpak

- Vormt zich een visie op de ontwikkeling van beveiliging in het kader van de bedrijfs- of procesarchitectuur en houdt daarbij rekening met de organisatiestrategie voor beveiliging;
- Draagt bij aan de strategie van de organisatie voor beveiliging vanuit het perspectief van procesontwikkeling;
- Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied.

Do: Treffen maatregelen

- Ontwerpt zelfstandig de architectuur van de bedrijfs- of procesarchitectuur voor het aanwijzen van beveiliging of draagt bij aan het expliciet maken van het aspect beveiliging als integraal onderdeel van deze architectuur;
- Voert risicoanalyses en PIA's uit binnen zijn competentiegebied;
- Toetst procesontwerpen aan architectuuruitgangspunten voor beveiliging en adviseert zonodig over verbetering van die ontwerpen;
- Toetst ontwerpen voor generieke beveiligingsfunctionaliteiten aan architectuuruitgangspunten voor beveiliging en adviseert zonodig over verbetering van die ontwerpen.

Check: Evaluatie en controle

- Beoordeelt procesmatige ontwikkelingen in de bedrijfsvoering met mogelijke gevolgen voor IB-aspecten;
- Beoordeelt IT-audit rapportages, rapportages over beveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten.

Act: Aanpassen

- Draagt zorg voor het bijstellen van het aspect beveiliging in de bedrijfs- of procesarchitectuur of implementaties daarvan op basis van zijn evaluaties.

Contacten

- **Intern:** bedrijfsprocesarchitecten, procesontwerpers, informatiemanagers, projectleiders voor procesmatige vernieuwingen, andere beveiligingsfunctie;
- **Extern:** IT-auditors en beroepsgenoten.

Kennisgebieden

- IV en beveiliging;
- Organisatie van informatievoorziening;
- Bescherming persoonsgegevens;
- Architectuurprincipes;
- Belastingdienstprocessen (hoofd en diep).

Doel van de functie

B.4.7.5. Beveiligingsmanager ICT

Het ontwikkelen van beleid gericht op informatiebeveiliging binnen de ICT-aanbodorganisatie, onderdelen van het managementsysteem, inregelingen voor de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

Functiecontext

Functioneert namens het management van ICT-aanbod als zelfstandig en breed opererend adviseur en toezichthouder op het gebied van beveiliging. Geeft functioneel leiding aan beveiligingsfunctionarissen in de ICT-organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het beveiligingsbeleid en het naleven van uitvoeringsrichtlijnen. Overwint weerstand om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.

Resultaatgebieden

Plan: Beveiligingseisen

- Stelt jaarlijks het informatiebeveiligingsplan voor de ICT-aanbodorganisatie op;
- Draagt bij aan de centrale strategie en -beleidsplannen voor beveiliging vanuit het perspectief van de ICT-aanbodorganisatie.

Leidinggeven

- Geeft eventueel functioneel of direct leiding aan andere beveiligingsfuncties binnen de ICT-aanbodorganisatie;
- Organiseert en faciliteert overleg om maatregelen en evaluaties binnen de ICT-aanbodorganisatie op het gebied van beveiliging op elkaar af te stemmen.

Do: Treffen maatregelen

- **Adviseert over** uitvoeringsrichtlijnen op het gebied van beveiliging, zowel centraal voor de Belastingdienst als bij de ICT-aanbodorganisatie;
- Initieert voorlichtings- en IB-bewustzijnsprogramma's en geeft hiervan richting;
- Voert risicoanalyses uit binnen zijn complete tiegebied en op centraal niveau als vertegenwoordiger van de ICT-aanbodorganisatie;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen de ICT-aanbodorganisatie met gevolgen voor beveiliging;
- Ziet toe op naleving adviezen/controlebevindingen bij certificerings-processen.

Check: Evaluatie en controle

- Beoordeelt afdelings- en procesrapportages binnen de ICT-aanbodorganisatie;
- Beoordeelt rapportages van in- en externe controle en auditinstanties;

- Geeft opdrachten tot het verrichten van interne onderzoeken en audits;
- Beoordeelt of participeert in de afhandeling van beveiligingsincidenten;

Act: Aanpassen

- Stelt het beveiligingsjaarplan en adviezen over beveiligingsuitvoeringstechnieken bij op basis van zijn evaluaties.

Contacten

- Intern: management bedrijfsonderdeel op alle niveaus en andere beveiligingsfuncties
- Extern: auditors, branche- en beroepsgenoten.

Kennisgebieden

ICT en informatiebeveiliging;
- Organisatie van informatievoorziening
- Bescherming persoonsgegevens;
- ITIL.

B.4.7.6. Informatiebeveiligingsarchitect

Doel van de functie

Het ontwikkelen en actueel houden van het aspect beveiliging binnen de IV-architectuur dat zowel gericht is op het voldoen aan het beveiligingsbeleid en -voorschriften als op de generieke beveiligingsfunctionaliteiten binnen de technische infrastructuur. Daarbij moet het toepasbaar maken van deze architectuur op handlijnen (systeemniveaus) van het ontwerp en het onderhoud van de generieke beveiligingsfunctionaliteiten.

Functieomschrijving

IV-architect met als specialisatie beveiliging in relatie tot IV. Vertaalt beleidskaders voor beveiliging naar IV-architecturen en vervult daarbij zowel een architect- als adviesrol. Treedt mee aan op als IV-specialist voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging- en auditing.

Zet toe op naleving van architectuurprincipes voor beveiliging. Houdt zicht op marktontwikkelingen op het gebied van beveiligingsproducten.

Resultaatgebieden

Plan: Beveiligingseisen

- Vormt zich een visie op de toekomst van beveiliging voor IV vanuit de centrale strategie door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het centrale beleid.
- Draagt bij aan de centrale strategie voor IV in relatie tot beveiliging;
- Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied.

Do: Treffen maatregelen

Ontwerpt zelfstandig doelarchitectuur van het IV complex voor het domein beveiliging of draagt bij aan het expliciet maken van het aspect beveiliging als integraal onderdeel van de IV-architecturen;
- Treedt op als IV-architect voor generieke beveiligingsfunctionaliteiten;
- Toetst IV-ontwerpen aan architectuuruitgangspunten voor beveiliging waaronder *Privacy by design* en adviseert zonodig over verbetering van die ontwerpen.

Check: Evaluatie en controle

- Beoordeelt ontwikkelingen in de markt t.a.v. nieuwe informatiebeveiligingsrisico's en generieke oplossingen van leveranciers;
- Beoordeelt interne ontwikkelingen binnen de IV met mogelijke gevolgen voor IE-aspecten in de IV;

- Beoordeelt IT-audit rapportages, rapportages over beveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten.

Act: Aanpassen

- Draagt zorg voor het bijstellen van het aspect beveiliging in IV-architecturen op basis van zijn evaluaties.

Contacten

- Intern: IV-architecten, IV-ontwerpers, projectleiders IV, andere beveiligingsfunctie;
- Extern: IT-auditors, IV-leveranciers en beroepsgenoten.

Kennisgebieden

- IV en beveiliging;
- Architectuurprincipes;
- Bescherming persoonsgegevens;
- Standaards inzake beveiliging.

B.5. Structuur van de implementatierichtlijnen

Voor het samenstellen en ordenen van de implementatierichtlijnen zijn een aantal uitgangspunten gehanteerd. Ze kunnen worden gebruikt als toetsingskader voor acceptatie van wijzigingen.

Deel C is gebaseerd op de NEN-ISO 27002:2013 die de invalshoek kent vanuit de informatietechnologie.

Deel D vindt zijn oorsprong in de NEN ISO 22313:2012 die een invalshoek heeft vanuit de bedrijfsprocessen, waarbij informatiebeveiliging een geïntegreerd onderdeel van BCM is.

B.5.1. Eigen implementatierichtlijnen

De richtlijnen en beheersmaatregelen zijn gebaseerd op de NEN-ISO 27002. Niet alle beheersmaatregelen en richtlijnen hoeven van toepassing te zijn en mogelijk zijn aanvullende beheersmaatregelen en richtlijnen vereist die niet in deze norm zijn opgenomen. De richtlijnen kunnen daarom worden beschouwd als uitgangspunt voor het ontwikkelen van organisatiespecifieke richtlijnen.

B.5.2. Ontwerpcriteria

Samenhang

Één kader voor de hele Belastingdienst
Door alle beveiligingsnormen in één handboek op te nemen is de onderlinge consistentie en volledigheid beter te borgen en het *pas toe of leg uit* beginsel van de aan de overheid opgelegde standaarden beter te handhaven.

Actualiteit en uitvoerbaarheid

Onderhoudbaar van de organisatie
Indien beveiligingsnormen te zeer op de organisatie van de Belastingdienst en te zeer implementatiemethodiekgebonden worden geformuleerd is niet meer duidelijk wat de oorspronkelijke uitgangspunten van de norm zijn. Er zal dan veel onderhoud moeten worden gepleegd omdat organisaties steeds dynamischer worden. Bovendien kunnen de normen dan niet goed meer met derden worden afgestemd en kunnen ze niet meer dienen als eisen die aan toeleveringsketenpartijen zijn te stellen.

Onderscheid tussen proces en product
Het maken van onderscheid naar normen voor processen en normen voor de uitkomsten van processen - dat zijn producten - dient meerdere doelen.

Het onderscheid is van belang bij het stellen van eisen aan projecten en derden, omdat het daarbij vaak alleen maar gaat om het opleveren van een product, bijvoorbeeld een IT-component of alleen het antwerp ervan. Het ze lde geldt bij fysieke objecten, zoals een gebouw of computerruimte.

De kennis die nodig is om proces- of productnormen toe te passen bij advisering en controle is verschillend.

Processen

Bij processen zijn vaak dezelfde ordeningsprincipes van toepassing. De volgorde van gebeurtenissen of de PDCA-cyclus. Bij de eenduidigheid van processen kan altijd dezelfde formele benadering worden gevolgd. Kennis omtrent de inhoud van de processen is niet primair vereist.

Producten

Bij producten is dit anders. Dat vergt bijna altijd specialistische kennis en een specifieke benadering bij het kunnen aantonen van de kwaliteit.

Dit onderscheid spoort met het onderscheid tussen de procesgerichte en een gegeven specifieke kwaliteitsbenadering.

Onderscheid tussen klant en leverancier (klantonafhankelijk)

Verantwoordelijkheid, wederzijds

Organisaties (en zeker overheidsorganisaties) opereren steeds meer in ketens waarbij ze sterk van elkaar afhankelijk zijn. Uitbesteding van facilitaire diensten, zoals IT, maar bijvoorbeeld ook huisvesting, is daarvan een prominent voorbeeld. Omdat verantwoordelijkheden niet kunnen worden uitbesteed, is het van belang zekerheid te krijgen over de juiste uitvoering van de uitbestede activiteiten. Hiervoor is het noodzakelijk de juiste risico's en normen aan de ander te kunnen stellen en hierop controle te kunnen laten uitoefenen. De huidige beveiligingsstandaards zijn hiervoor niet ingedeeld.

Duidelijk belegde verantwoordelijkheid

Zo klein mogelijke verantwoordelijkheidsgebieden

De indeling van de normen moet zodanig zijn dat naleving ondubbelzinnig is toe te wijzen binnen een organisatie. Het moet niet de expertise van de controleur zijn die uiteindelijk bepaalt bij welke afdeling of als welk onderdeel van een proces normen op naleving moeten worden gecontroleerd. Het onderscheid tussen beleid en uitvoering bijvoorbeeld is in grote organisaties vaak geschieden en dat betekent dat een dergelijk onderscheid ook moet doorwerken in de formulering van normen.

Ondubbelzinnige normen

Controleerbaar met bewijsstukken

Indien naleving van een norm niet rechtstreeks kan worden aangetoond met bewijsstukken is de formulering van de norm niet concreet genoeg. Vaak neigt de omschrijving meer naar een doelstelling dan een norm. Een norm moet zo min mogelijk interpretatieverschillen toelaten.

Om die reden worden de normen ingedeeld naar beheersmaatregelen op een hoog abstractieniveau en verder ingevuld met zo concreet mogelijke *implementatierichtlijnen*. Het is echter vanwege de organisatie-onafhankelijkheid niet altijd mogelijk interpretatieverschillen geheel te voorkomen. In het Hbbi werkboek wil vage formuleringen.

B.5.3. Betekenis en opbouw normen

Beheersmaatregelen en implementatierichtlijnen

De normen zijn onderverdeeld in twee hiërarchische niveaus, de beheersmaatregelen met daaronder de implementatierichtlijnen. De beheersmaatregelen dienen voor coördinatie/sturing en rapportage, de implementatierichtlijnen zijn *best practices*, die aan de maatregelen invulling geven.

De interne controleprogramma's zijn op deze implementatierichtlijnen gericht en vervolgens per beheersmaatregel tot een oordeel te kunnen komen volgens het *pas toe of leg uit* principe.

B.6. Verklaring van toepasselijkheid

B.6.1. Internationale normen

NEN-ISO

Volgens de NEN-ISO 27001 2013 dient een verklaring van toepasselijkheid (*statement of applicability*) te worden opgesteld. Hierin staat beschreven welke beheersmaatregelen van toepassing zijn, hoe die zich verhouden tot de beheersmaatregelen uit NEN-ISO 27002:2013 en welke maatregelen om welke redenen zijn uitgesloten.

De Belastingdienst volgt de NEN-ISO 27002:2013 in zijn geheel, met waar van toepassing aanvullende maatregelen die specifiek voor de eigen organisatie gelden.

B.6.2. Nationale normen

NORA

De Nederlandse Overheid Referentie Architectuur katern Beveiliging is als vastgestelde norm voor de Nederlandse overheid van toepassing voor de Belastingdienst. Dit katern van de NORA is online te raadplegen[48].

BIR

De Baseline Informatiebeveiliging Rijksdienst – Tactisch Normenkader (BIR-TKN) wordt opgevolgd, inclusief de specifiek voor de Rijksoverheid geldende normen en de operationele handleiding.

[48] http://www.noraonline.nl/wiki/Beveiliging

Gebruikte afkortingen

ADR	Auditdienst Rijk
AIVD	Algemene Inlichtingen- en Veiligheidsdienst (BZK)
ARAR	Algemeen Rijksambtenarenreglement
BCM	Business continuity management, bedrijfscontinuïteitsbeheer
BCMS	Business continuity management system
BHV	Bedrijfshulpverlening
BIA	Business Impact Analysis
BIR	Baseline Informatiebeveiliging Rijksdienst
BVA	Beveiligingsambtenaar
BYOD	Bring your own device
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CFD	Centrum voor Facilitaire Dienstverlening
CFO	Chief Financial Officer
CHRO	Chief Human Resource Officer
CIE	Centrum voor Infrastructuur en Exploitatie
CIO	Chief Information Officer
COPE	Company owned personally enabled
CPB	Centraal Planbureau
CSO	Chief Security Officer
CYOD	Choose Your Own Device
DGBel	Directoraat-generaal Belastingdienst
DRZ	Domeinen Roerende Zaken
FG	Functionaris voor de Gegevensbescherming
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
HBB	Handboek Beveiliging Belastingdienst
IB	Informatiebeveiliging
IBR	Integraal Beveiligingsberaad Rijksoverheid
ICT	Informatie- en communicatietechnologie
ICP	Intern controleprogramma
IT	Informatietechnologie
IV	Informatievoorziening
MT	Managementteam
MvF	Ministerie van Financiën
NCSC	Nationaal Cyber Security Centrum
NORA	Nederlandse Overheid Referentie Architectuur
PDCA	Plan - do - check – act
PIA	Privacy Impact Assessment
PUB	Personele Uitvoeringsbepalingen Belastingdienst
SOC	Security Operations Center
TBO	Tactisch Beveiligingsoverleg
VenJ	Ministerie van Veiligheid en Justitie
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIRBI	VIR – Bijzondere Informatie
VOG	Verklaring Omtrent het Gedrag

bylage 32

Handboek Beveiliging Belastingdienst

2017

Deel C
Implementatierichtlijnen

Inhoudsopgave

Boekdata

Titel	Handboek Bevrijding Belastingdienst 2017 Deel C : implementatierichtlijnen
Versie	December 2016
Auteur	Tactisch Bevrijdingsoverleg

Versie	Opmerkingen
Mei 2011	Eerste jaargang HBB Deel C
December 2012	Tweede jaargang HBB Deel C
December 2013	Derde jaargang HBB Deel C
December 2014	Vierde jaargang HBB Deel C
Februari 2016	Vijfde jaargang HBB Deel C
December 2016	Zesde jaargang HBB Deel C - Boekdata, MN

Toelichting op Deel C

1. Beheersmaatregelen zijn verplicht, tenzij aangetoond kan worden dat ze niet van toepassing zijn. Implementatierichtlijnen zijn niet verplicht, maar omdat ze als best practice zijn vastgesteld moet bij het afwijken ervan aangetoond worden dat een andere implementatie tot het vervullen van de beheersmaatregel leidt. (I-BB B.3.2.)
2. De nummering zijn onderverdeeld in hiërarchische niveaus, de doelstellingen, de beheersmaatregelen en daaronder de implementatierichtlijnen. De beheersmaatregelen dienen voor oordeelsvorming en rapportage, de implementatierichtlijnen zijn best practices die aan de maatregelen invulling geven.
3. De verwijzingen naar de NEN-ISO 27002:2013 staan opgenomen in de vorm (ISO...) en dienen ter referentie. Ze zijn niet bedoeld als nadere invulling van de richtlijn.

C.1. Strategisch beveiligingsbeleid en -organisatie

Doelstelling

Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving. (ISO 5.1)

Het strategisch beveiligingsbeleid en -organisatie geeft voor de gehele organisatie richting aan het treffen van maatregelen voor beveiliging overeenkomstig de bedrijfsmatige eisen en van toepassing zijnde standaarden, wetten en voorschriften en het handhaven daarvan.

Toelichting

Het beveiligingsbeleid kan worden onderscheiden in een strategisch deel en beleidsonderwerpen die te zien zijn als een nadere invulling van het strategisch beleidsdocument op het tactisch niveau. Het strategisch deel is bedoeld voor managers en algemene voorlichtingsdoeleinden en daarbij staat leesbaarheid en begrijpelijkheid voorop. Het tactisch deel is meer bedoeld voor specialisten, die verantwoordelijk zijn voor de inrichting van organisatie, processen en middelen.

Motivering

Gezien de complexiteit van beveiliging als integraal aspect van de bedrijfsvoering is het van belang om op globaal niveau voor samenhang te zorgen en richting te geven aan het treffen van beveiligingsmaatregelen in de gehele organisatie. Door voor een reeks van onderwerpen over de verschillende verantwoordelijkheden been op hoofdlijnen het strategisch beleid verder uit te werken, kan een organisatie sturing geven aan de invulling/implementatie van de normen.

C.1.1. Strategisch beveiligingsbeleid

Beheersmaatregel

Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. (ISO 5.1.1)

Toelichting

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

Het beleidsdocument voor beveiliging geeft de betrokkenheid van het hoogste management weer evenals de benadering van de organisatie ten aanzien van het beheer van beveiliging.

Implementatierichtlijn

Beleidsregels inzake informatiebeveiliging behoren eisen te behandelen die voortkomen uit:

a) bedrijfsstrategie;

b) wet- en regelgeving en contracten;

c) huidige en verwachte bedreigingen inzake informatiebeveiliging.

Het informatiebeveiligingsbeleid behoort uiteenzettingen te bevatten betreffende:

a) de definitie van doelstellingen en principes van informatiebeveiliging om richting te geven aan alle activiteiten die verband houden met informatiebeveiliging;

b) toekenning van algemene en specifieke verantwoordelijkheden voor informatiebeveiligingsbeheer aan gedefinieerde rollen;

c) processen voor het behandelen van afwijkingen en uitzonderingen.

Op een lager niveau behoort het informatiebeveiligingsbeleid te worden ondersteund door onderwerpspecifieke beleidsregels die de implementatie van beheersmaatregelen inzake informatiebeveiliging verplicht stellen en die specifiek gestructureerd zijn om de behoeften van bepaalde doelgroepen binnen een organisatie aan de orde te stellen of om bepaalde onderwerpen te behandelen.

Deze beleidsregels behoren te worden gecommuniceerd aan medewerkers en relevante externe partijen in een vorm die relevant, toegankelijk en begrijpelijk is voor de beoogde lezer, bijv. in de context van een 'bewustzijns-, opleidings- en trainingsprogramma voor informatiebeveiliging' (zie ISO 7.2.2).

C.1.2. Beoordeling van het informatiebeveiligingsbeleid

Beheersmaatregel

Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. (ISO 5.1.2)

Implementatierichtlijn

Het toewijzen van de verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met de beleidsregels voor informatiebeveiliging (zie ISO 5.1.1) Verantwoordelijkheden voor het beschermen van individuele bedrijfsmiddelen en voor het uitvoeren van specifieke informatiebeveiligingsprocessen behoren te worden geïdentificeerd. Verantwoordelijkheden behoren te worden gedefinieerd voor activiteiten met betrekking tot risicobeheer van informatiebeveiliging en in het bijzonder voor het accepteren van de overblijvende risico's. Deze verantwoordelijkheden behoren waar nodig te worden aangevuld met meer gedetailleerde richtlijnen voor specifieke locaties en informatieverwerkende faciliteiten. Lokale verantwoordelijkheden voor het beschermen van bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsprocessen behoren te worden gedefinieerd.

Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend mogen beveiligingstaken aan anderen delegeren. Niettemin blijven zij verantwoordelijk en behoren zij vast te stellen dat gedelegeerde taken correct zijn verricht.

Vastgelegd behoort te worden welke personen voor welke gebieden verantwoordelijk zijn. Het volgende behoort in het bijzonder te gebeuren:

a) de bedrijfsmiddelen en informatiebeveiligingsprocessen behoren te worden geïdentificeerd en gedefinieerd;

b) de entiteit die verantwoordelijk is voor elk bedrijfsmiddel of informatiebeveiligingsproces behoort te worden bepaald en de details van deze verantwoordelijkheid behoren te worden gedocumenteerd (zie ISO 6.1.2)

c) autorisatieniveaus behoren te worden geïdentificeerd en gedocumenteerd;

d) om in staat te zijn om de verantwoordelijkheden in het informatiebeveiligingsgebied te vervullen behoren de betrokken personen op het desbetreffende gebied competent te zijn en betrokken te mogelijkheden te worden geboden om de ontwikkelingen bij te houden;

e) coördinatie en overzicht van informatiebeveiligingsaspecten van leveranciersrelaties behoren te worden geïdentificeerd en gedocumenteerd.

C.1.3. Organisatie van beveiliging

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de Informatiebeveiliging Binnen de organisatie te initiëren en te beheersen. (ISO 6.1)

C.1.3.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

Beheersmaatregel

Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. (ISO 6.1.1)

Implementatierichtlijn

Het toewijzen van de verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met de beleidsregels voor informatiebeveiliging (zie ISO 5.1.1) Verantwoordelijkheden voor het beschermen van individuele bedrijfsmiddelen en voor het uitvoeren van specifieke informatiebeveiligingsprocessen behoren te worden geïdentificeerd.

Verantwoordelijkheden behoren te worden gedefinieerd voor activiteiten met betrekking tot risicobeheer van informatiebeveiliging en in het bijzonder voor het accepteren van de overblijvende risico's. Deze verantwoordelijkheden behoren waar nodig te worden aangevuld met meer gedetailleerde richtlijnen voor specifieke locaties en informatieverwerkende faciliteiten. Lokale verantwoordelijkheden voor het beschermen van bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsprocessen behoren te worden gedefinieerd.

Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend mogen beveiligingstaken aan anderen delegeren. Niettemin blijven zij verantwoordelijk en behoren zij vast te stellen dat gedelegeerde taken correct zijn verricht.

Vastgelegd behoort te worden welke personen voor welke gebieden verantwoordelijk zijn. Het volgende behoort in het bijzonder te gebeuren:

a) de bedrijfsmiddelen en informatiebeveiligingsprocessen behoren te worden geïdentificeerd en gedefinieerd;

b) de entiteit die verantwoordelijk is voor elk bedrijfsmiddel of informatiebeveiligingsproces behoort te worden bepaald en de details van deze verantwoordelijkheid behoren te worden gedocumenteerd (zie ISO 8.1.2);

c) autorisatieniveaus behoren te worden gedefinieerd en gedocumenteerd;

d) om in staat te zijn om de verantwoordelijkheden in het informatiebeveiligingsgebied te vervullen behoren de betrokkende personen op het desbetreffende gebied competent te zijn en behoort hun de mogelijkheden te worden geboden om de ontwikkelingen bij te houden;

e) coördinatie en overzicht van informatiebeveiligingsaspecten van leveranciersrelaties behoren te worden geïdentificeerd en gedocumenteerd.

C.1.3.2 Contact met overheidsinstanties

Beheersmaatregel

Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden. (ISO 6.1.3)

Implementatierichtlijn

Organisaties behoren procedures te hebben die aangeven wanneer en door wie contact behoort te worden opgenomen met overheidsinstanties (bijv. politie, nutsbedrijven, brandweer, toezicht (inwoners) en hoe geïdentificeerde informatiebeveiligingsincidenten tijdig behoren te worden gerapporteerd (bijv. indien het vermoeden bestaat dat mogelijk wetgeving is overtreden).

C.1.3.3 Contact met speciale belangengroepen

Beheersmaatregel

Er behoren passende contacten met speciale belangengroepen of anders gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden. (ISO 6.1.4)

Implementatierichtlijn

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

a) kennis te verbeteren over 'best practices' en op de hoogte te blijven van relevante beveiligingsinformatie;

b) ervoor te zorgen dat de kennis van informatiebeveiliging actueel en volledig is;

c) vroegtijdige waarschuwingen te ontvangen inzake alarm, adviezen en patches die verband houden met aanvallen en kwetsbaarheden;

d) toegang te krijgen tot gespecialiseerd advies over informatiebeveiliging;

e) informatie over nieuwe technologieën, producten, bedreigingen of kwetsbaarheden te delen en uit te wisselen;

f) geschikte contactpunten te verkrijgen als er informatiebeveiligingsincidenten zijn (ISO 16).

C.1.3.4 Informatiebeveiliging in projectbeheer

Beheersmaatregel

Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. (ISO 6.1.5)

Implementatierichtlijn

Informatiebeveiliging behoort te worden geïntegreerd in de projectbeheermethode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico's worden geïdentificeerd en aangepakt als deel van een project. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, IT, facility management, en andere ondersteunende processen. De gebruikte projectbeheermethoden behoren te vereisen dat:

a) informatiebeveiligingsdoelstellingen worden opgenomen in projectdoelstellingen;

b) een risicobeoordeling van informatiebeveiliging in een vroeg stadium van het project wordt uitgevoerd om de nodige beheersmaatregelen te identificeren;

c) informatiebeveiliging deel uitmaakt van alle fasen van de toegepaste projectmethodologie.

In alle projecten behoren implicaties van informatiebeveiliging regelmatig te worden behandeld en beoordeeld. Verantwoordelijkheden voor informatiebeveiliging behoren te worden gedefinieerd en toegewezen aan specifieke rollen die zijn gedefinieerd in de projectbeheermethoden.

C.2. Tactisch beveiligingsbeleid

Doelstelling

Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen. (ISO 6.1)

Het tactisch uitvoeringsbeleid geeft beleidsuitgangspunten voor de inrichting van beveiliging overkoepelend aan de onderscheiden processen en producten.

Toelichting

De beleidsverantwoordelijkheid wordt als gescheiden verantwoordelijkheid gezien t.o.v. de uitvoeringsverantwoordelijkheid.

De tactische beveiligingsmaatregelen hebben voor het merendeel betrekking op meerdere verantwoordelijke organisaties waarbij de samenhang tussen de verschillende maatregelen gehoord moet zijn of ze overstijgen het belang van de desbetreffend verantwoordelijke manage".

Motivering

Door een aantal stromen voor de inrichting op hoofdlijnen van beveiligingsaspecten afzonderlijk te definiëren kan de verantwoordelijkheid hiervoor nadrukkelijk door het hoogste management zelf – met ondersteuning van tactisch beveiligingsbeheer - worden gepositioneerd.

C.2.1. "Naleving van wettelijke en contractuele eisen"

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen. (ISO 18.1)

C.2.1.1 Identificatie van toepasselijke kaders

Beheersmaatregel

Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden. (ISO 18.1.1)

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. (ISO 18.1.4)

Implementatierichtlijn

Ook de specifieke beheersmaatregelen en individuele verantwoordelijkheden om aan deze eisen te voldoen behoren te worden gedefinieerd en gedocumenteerd.

Managers behoren alle wetgeving die toepasselijk is op hun organisatie vast te stellen om te voldoen aan de eisen voor hun soort bedrijfsactiviteit. Indien de organisatie zakelijke activiteiten in andere landen verricht, behoren managers te letten op naleving in alle relevante landen.

C.2.1.2 Privacy en bescherming van persoonsgegevens

Beheersmaatregel

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. (ISO 18.1.4)

Implementatierichtlijn

Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid behoort te worden gecommuniceerd aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens.

Naleving van dit beleid en van alle relevante wet- en regelgeving betreffende het beschermen van de privacy van personen en de bescherming van persoonsgegevens vereist een geschikte beheerstructuur en toezicht. Vaak kan dit het beste worden bereikt door een persoon te benoemen

die hiervoor verantwoordelijk is, zoals een privacyfunctionaris, die schriftelijke behoort te geven aan managers, gebruikers en aanbieders van diensten over hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Het toewijzen van verantwoordelijkheid voor het hanteren van persoonsgegevens en het waarborgen dat medewerkers zich bewust zijn van de privacyprincipes behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving. Er behoren passende technische en organisatorische maatregelen te worden geïmplementeerd om persoonsgegevens te beschermen.

C.2.1.3 Beschermen van registraties

Beheersmaatregel

Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. (ISO 18.1.3)

Implementatierichtlijn

Bij besluitvorming over bescherming van specifieke registraties van de organisatie behoort de classificatie daarvan gebaseerd op het classificatieschema van de organisatie in overweging te worden genomen. Registraties behoren te worden gecategoriseerd naar type, bijv. boekhoudkundige registraties, databaserecords, transactielogbestanden, auditlogbestanden en operationele procedures. Bij elk type behoort de bewaartermijn en toegestane soorten opslagmedia te worden vermeld, bijv. papier, microfiche, magnetische of optische opslag. Gerelateerde cryptografische sleutels en programma's die samenhangen met versleutelde archieven of digitale handtekeningen (zie hoofdstuk ISO 10), behoren ook te worden bewaard om decodering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties.

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

Als elektronische opslagmedia worden gekozen, behoren procedures te worden vastgesteld om te waarborgen dat de gegevens tijdens de bewaarperiode toegankelijk blijven (leesbaarheid van zowel de media als van het gegevensformaat), om te voorkomen dat de informatie verloren gaat als gevolg van toekomstige technologische veranderingen.

Systemen voor gegevensopslag behoren zo te worden gekozen dat vereiste gegevens binnen een aanvaardbare tijdsspanne en in een aanvaardbaar formaat kunnen worden opgevraagd, afhankelijk van de eisen waaraan moet worden voldaan.

Het systeem waarmee gegevens worden opgeslagen en behandeld, behoort de identificatie van registraties en hun bewaarperiode te waarborgen zoals gedefinieerd door, indien van toepassing, nationale of regionale wet- of regelgeving. Dit systeem behoort toe te staan de registraties na afloop van die termijn op een passende manier te vernietigen als de organisatie ze niet langer nodig heeft.

Om te voldoen aan deze doelstellingen met betrekking tot het veiligstellen van registraties behoren binnen een organisatie de volgende stappen te worden genomen:

a) er behoren richtlijnen te worden verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie;

b) er behoort een bewaarschema te worden opgesteld waarin registraties en de periode dat ze moeten worden bewaard, zijn vastgelegd;

c) er behoort een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.

C.2.2. Scheiding van taken

Beheersmaatregel

Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.(ISC 6.1.2)

Toelichting

In de daarvoor in aanmerking komende paragrafen voor processen en producten zijn gedetailleerde normen uitgewerkt voor functiescheidingen. Deze hebben betrekking voor de procesinrichting en het toekennen van autorisaties. In het tactisch beleid wordt aangegeven welke functiescheidingen er op het hoogste niveau van een organisatie worden gehanteerd.

Implementatierichtlijn

Er behoort op te worden gelet dat geen enkele persoon aangemerkt of zonder autorisatie toegang kan krijgen tot bedrijfsmiddelen, ze kan wijzigen of gebruiken. Het initiëren van een gebeurtenis behoort te worden gescheiden van de autorisatie ervan. Bij het ontwerpen van beheersmaatregelen behoort rekening te worden gehouden met de mogelijkheid van samenzwering.

Er is functiescheiding tussen

a) beleidsvoorbereiding en uitvoering;

b) gebruikers en ontwikkeling en beheer van faciliteire voorzieningen (Huisvesting en ICT);

c) tactische beleisprocessen en uitvoerende processen;

d) beslissende, bewarende, registrerende, uitvoerende en controlerende functies.

C.2.3. Vertrouwensfuncties

Beheersmaatregel

Er behoort te worden vastgesteld welke functies in de organisatie worden aangemerkt als vertrouwensfuncties conform de *Leidraad aanwijzing vertrouwensfuncties* van de AIVD.

C.2.4. Toegangsbeveiliging

C.2.4.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: toegang tot informatie en informatieverwerkende faciliteiten beperken. (ISO 9.1)

C.2.4.1.1 Beleid voor toegangsbeveiliging

Beheersmaatrege

Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. (ISO 9.1.1)

Implementatierichtlijn

Eigenaren van bedrijfsmiddelen behoren passende regels voor toegangsbeveiliging, -rechten en -beperkingen voor specifieke gebruikersrollen ten aanzien van hun bedrijfsmiddelen vast te stellen, waarbij de details en de strikheid van de beheersmaatregelen consistent zijn met de gerelateerde informatiebeveiligingsrisico's.

Toegangsbeveiligingsmaatregelen zijn zowel logisch als fysiek van aard (zie hoofdstuk ISO 11) en behoren als een geheel te worden beschouwd. Gebruikers en dienstverleners behoren een duidelijke verklaring te ontvangen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiligingsmaatregelen moeten voldoen.

Het beleid behoort rekening te houden met het volgende:

a) beveiligingseisen van de bedrijfsprocestoepassingen;

b) beleidsregels voor informatieverspreiding en -autorisatie, bijv. het 'need-to-know' of 'need-to-do'-principe, informatiebeveiligingsniveaus en -classificatie (zie ISO 8.2);

c) consistentie tussen de toegangsrechten en de beleidsregels inzake informatieclassificatie van systemen en netwerken;

d) relevante wetgeving en contractuele verplichtingen met betrekking tot beperking aan de toegang tot gegevens of diensten (zie ISO 15.1);

e) het beheer van toegangsrechten in een distributie- en netwerkomgeving die alle beschikbare

soorten verbindingen herkent;

f) scheiding van toegangsbeveiligingsrollen bijv. toegangsverzoek, -autorisatie, -administratie;

g) eisen voor formele autorisatie van toegangsverzoeken (zie ISO 9.2.1 en ISO 9.2.2);

h) eisen voor het periodiek beoordelen van toegangsrechten (zie ISO 9.2.5);

i) intrekken van toegangsrechten (zie ISO 9.2.6);

j) archiveren van verslaglegging van alle belangrijke gebeurtenissen betreffende het gebruik en het beheer van gebruikersidentificaties en geheime authenticatie-informatie;

k) rollen met speciale toegangsrechten (zie ISO 9.2.3).

Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. (ISO 9.4.4)

C.2.4.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. (ISO 9.2)

C.2.4.2.1 Registratie en afmelden van gebruikers

Beheersmaatregel

Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. (ISO 9.2.1)

Implementatierichtlijn

De procedure voor het beheren van gebruikersidentificaties behoort te omvatten:

a) het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun acties; het gebruik van groepsidentificaties behoort alleen te worden toegestaan als deze om bedrijfs- of operationele redenen noodzakelijk zijn en behoort te worden goedgekeurd en gedocumenteerd;

b) het onmiddellijk ongeldig maken of verwijderen van de gebruikersidentificatie van gebruikers die de organisatie hebben verlaten (zie ISO 9.2.6);

c) het periodiek identificeren en verwijderen van overbodige gebruikersidentificaties;

d) het ervoor zorgen dat overtollige gebruikersidentificaties niet aan andere gebruikers worden uitgegeven.

C.2.4.2.2 Gebruikers toegang verlenen

Beheersmaatregel

Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. (ISO 9.2.2)

Implementatierichtlijn

De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties behoort te omvatten:

a) autorisatie verkrijgen van de eigenaar van het informatiesysteem of de informatiedienst voor het gebruik van het informatiesysteem of de informatiedienst (zie beheersmaatregel ISO 8.1.2); afzonderlijke goedkeuring voor toegangsrechten door de directie is mogelijk ook relevant;

b) verifiëren dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang (zie ISO 9.1) en consistent is met andere eisen zoals een scheiding van taken (zie ISO 6.1.2);

c) waarborgen dat toegangsrechten niet worden geactiveerd (bijv. door dienstverleners) voordat de autorisatieprocedures zijn afgerond;

d) bijhouden van een centraal overzicht van toegangsrechten die aan een gebruikersidentificatie zijn toegekend dat toegang te verlenen tot informatiesystemen en -diensten;

e) aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren;

f) met eigenaren van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie ISO 9.2.5).

C.2.4.2.3 Beheren van speciale toegangsrechten

Beheersmaatregel

Het toewijzen en gebruik van speciale toegangsrechten beheren te worden beperkt en beheerst. (ISO 9.2.3)

Implementatierichtlijn

Het toewijzen van speciale toegangsrechten behoort te worden beheerst door een formele autorisatieprocedure die in overeenstemming is met het relevante toegangsbeveiligingsbeleid (zie beheersmaatregel ISO 9.1.1). De volgende stappen behoren in overweging te worden genomen:

a) de speciale toegangsrechten behorend bij elk systeem of proces, bijv. besturingssysteem, databasebeheersysteem en elke toepassing, en de gebruikers aan wie ze moeten worden toegewezen, behoren te worden geïdentificeerd;

b) speciale toegangsrechten behoren op basis van noodzaak tot gebruik en per gebeurtenis aan gebruikers te worden toegekend in overeenstemming met het toegangsbeveiligingsbeleid (zie ISO 9.1.1), d.w.z. gebaseerd op wat minimaal is vereist voor hun functionele rollen;

c) er behoort een autorisatieprocedure en een vastlegging van alle toegekende speciale toegangsrechten te worden bijgehouden. Speciale toegangsrechten behoren niet te worden verleend voordat de autorisatieprocedure is afgerond;

d) voor het vervallen van speciale toegangsrechten behoren eisen te worden gedefinieerd;

e) speciale toegangsrechten behoren te worden toegekend aan een gebruikersidentificatie die verschilt van identificaties die voor reguliere bedrijfsactiviteiten worden gebruikt. Reguliere bedrijfsactiviteiten behoren niet met een speciale gebruikersidentificatie te worden verricht;

f) de competenties van gebruikers met speciale toegangsrechten behoren regelmatig te worden beoordeeld om te verifiëren of ze in overeenstemming zijn met hun taken;

g) specifieke procedures behoren te worden vastgesteld en onderhouden om onbevoegd gebruik van gebruikersidentificaties voor algemeen beheer te voorkomen, in overeenstemming met de configuratiemogelijkheden van het systeem;

h) voor gebruikersidentificaties voor algemeen beheer behoort de geheimhouding van geheime authenticatie-informatie in acht te worden genomen als deze wordt gewijzigd (bijv. vaak veranderen van wachtwoord en zodra een speciale gebruiker vertrekt of van functie verandert, dit onder speciale gebruikers communiceren met de passende mechanismen).

C.2.4.2.4 Beheer van geheime authenticatie-informatie van gebruikers

Beheersmaatregel

Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. (ISO 9.2.4)

Implementatierichtlijn

Het proces behoort de volgende elementen te bevatten:

a) gebruikers behoren te worden verplicht een verklaring te ondertekenen dat zij persoonlijke geheime authenticatie-informatie geheimhouden en groepsinformatie, d.w.z. gedeelde geheime authenticatiegegevens, binnen de groep houden; deze getekende verklaring kan worden opgenomen in de arbeidsvoorwaarden (zie ISO 7.1.2);

b) als gebruikers hun eigen geheime authenticatie-informatie moeten onderhouden behoort hun eerst tijdelijke geheime authenticatie-informatie te worden gegeven die zij bij het eerste gebruik moeten wijzigen;

c) er behoren procedures te worden vastgesteld om de identiteit van een gebruiker vast te stellen voordat nieuwe, vervangende of tijdelijke geheime authenticatie-informatie wordt verstrekt;

d) tijdelijke geheime authenticatie-informatie behoort op een veilige manier aan gebruikers te worden gegeven; gebruikmaken van externe partijen of onbeschermde e-mailberichten (niet-gecodeerde tekst) behoort te worden vermeden;

e) tijdelijke geheime authenticatie-informatie behoort uniek voor een persoon te zijn en behoort niet te kunnen worden geraden;

f) gebruikers behoren de ontvangst van geheime authenticatie-informatie te bevestigen;

g) standaard geheime authenticatie-informatie van een leverancier behoort te worden gewijzigd na de installatie van systemen of software.

C.2.4.2.5 Beoordeling van toegangsrechten van gebruikers

Beheersmaatregel

Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. (ISO 9.2.5)

Implementatierichtlijn

Bij het beoordelen van toegangsrechten van gebruikers behoren de volgende aspecten in overweging te worden genomen:

a) toegangsrechten van gebruikers behoren regelmatig en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld (zie hoofdstuk ISO 7);

b) toegangsrechten van gebruikers behoren te worden beoordeeld en opnieuw te worden toegekend bij functieverandering binnen dezelfde organisatie;

c) autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld;

d) toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen;

e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden.

C.2.4.2.6 Toegangsrechten intrekken of aanpassen

Beheersmaatregel

De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd en bij wijzigingen behoren ze te worden aangepast. (ISO 9.2.6)

Implementatierichtlijn

Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten en diensten te worden ingetrokken of opgeschort. Hierdoor kan worden vastgesteld of het noodzakelijk is om toegangsrechten in te trekken.

Wijzigingen in het dienstverband behoren te worden weerspiegeld in het intrekken van alle toegangsrechten die niet voor het nieuwe dienstverband zijn goedgekeurd. De toegangsrechter die behoren te worden ingetrokken of aangepast omvatten ook de fysieke en logische toegangsrechten. Intrekking of aanpassing kan plaatsvinden door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatieverwerkende faciliteiten of abonnementen. Elk document dat toegangsrechten van medewerkers en contractanten identificeert, behoort de intrekking of aanpassing van toegangsrechten weer te geven. Indien een medewerker die uit dienst gaat of een externe gebruiker wachtwoorden kent van gebruikersidentificaties die actief blijven, dan behoren deze bij beëindiging of wijziging van dienstverband, contract of overeenkomst te worden gewijzigd.

Toegangsrechten voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten behoren te worden verminderd of ingetrokken voordat het dienstverband eindigt of wijzigt, afhankelijk van de evaluatie van risicofactoren zoals:

a) of de beëindiging of wijziging is geïnitieerd door de medewerker, de externe gebruiker of door de directie, en de reden voor de beëindiging;

b) de huidige verantwoordelijkheden van de medewerker, externe gebruiker of overige gebruikers;

c) de waarde van de bedrijfsmiddelen die op dat moment toegankelijk zijn.

C.2.4.2.7 Geheime authenticatie-informatie gebruiken

Beheersmaatregel

Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie. (ISO 9.3.1)

Implementatierichtlijn

Alle gebruikers behoren het advies te krijgen om:

a) vertrouwelijk om te gaan met geheime authenticatie-informatie, en ervoor te zorgen dat deze informatie niet openbaar wordt gemaakt aan andere partijen, met inbegrip van zeggenschappende personen;

b) geen geheime authenticatie-informatie te registreren (bijv. op papier, in een computerbestand of op een zakapparaat), tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd (bijv. "password vault";

c) geheime authenticatie-informatie te wijzigen als er een aanwijzing is dat deze mogelijk is gecompromitteerd;

d) as a wachtwoorden als geheime authenticatie-informatie worden gebruikt, sterke wachtwoorden te kiezen van voldoende minimumlengte, die:

1) gemakkelijk te onthouden zijn;

2) niet zijn gebaseerd op gegevens die iemand anders gemakkelijk kan raden of achterhalen door persoonsgerelateerde informatie te gebruiken, zoals namen, telefoonnummers en geboortedata;

3) niet kwetsbaar zijn voor woordenboekaanvallen (d.w.z. niet bestaan uit woorden die in woordenboeken zijn opgenomen);

4) geen opeenvolgende identieke tekens bevat, en niet alleen uit cijfers of letters bestaat

5) bij het eerste inloggen worden gewijzigd als ze tijdelijk zijn;

e) geen geheime authenticatie-informatie te delen;

f) te zorgen voor passende bescherming van wachtwoorden wanneer wachtwoorden worden gebruikt als geheime authenticatie-informatie in geautomatiseerde inlogprocedures en worden opgeslagen;

g) niet dezelfde geheime authenticatie-informatie voor zakelijke en particuliere toepassingen te gebruiken.

C.2.5. Informatieuitwisseling en -transport

C.2.5.1 Classificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie. (ISO 8.2)

C.2.5.1.1 Classificatie van informatie

Beheersmaatregel

Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor ongeoorloofde bekendmaking of wijziging. (ISO 8.2.1)

Implementatierichtlijn

Classificaties en de bijbehorende beschermende beheersmaatregels en voor informatie behoren rekening te houden met de zakelijke behoeften om informatie te delen of te beperken, en met wettelijke eisen. Aan deze 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 informatiebedrijfsmiddelen behoren verantwoordelijk te zijn voor de classificatie ervan.

Het classificatiesysteem behoort regels voor het classificeren te bevatten en criteria voor het na verloop van tijd opnieuw beoordelen van de classificatie. Het beschermingsniveau dat in het schema wordt vastgelegd behoort te worden vastgesteld door de vertrouwelijkheid, integriteit en beschikbaarheid en eventuele andere eisen voor de desbetreffende informatie te analyseren. Het schema behoort in overeenstemming te worden gebracht met het beleid voor toegangsbeveiliging (zie ISO 9.1.1)

Elk 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 zodat iedereen informatie en gerelateerde bedrijfsmiddelen op dezelfde manier classificeert op basis van een gemeenschappelijk begrip van beschermingseisen en de passende bescherming toepast.

Classificatie behoort te worden opgenomen in de procedures van de organisatie en organisatiebreed consistent en coherent te zijn. Resultaten van classificatie behoren de waarde van bedrijfsmiddelen aan te geven afhankelijk van hun gevoeligheid en belang voor de organisatie, bijv. in te zien van vertrouwelijkheid, integriteit en beschikbaarheid. Resultaten van classificatie behoren te worden geactualiseerd in overeenstemming met wijzigingen in hun waarde, gevoeligheid en belang in de loop van hun levenscyclus.

C.2.5.1.2 Informatie labelen

Beheersmaatregel

Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. (ISO 8.2.2)

Implementatierichtlijn

Procedures voor het labelen van informatie behoren te gaan over informatie en gerelateerde bedrijfsmiddelen in fysieke en elektronische formaten. De labeling behoort in overeenstemming te zijn

met het classificatieschema vastgesteld in ISO 8.2.1. 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 media. De procedures kunnen gevallen definiëren waarin labelen niet wordt toegepast, bijv. bij niet-vertrouwelijke informatie, om de werklast te verminderen. Medewerkers en contractanten behoren op de hoogte te worden gebracht van de labelprocedures.

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

C.2.5.1.3 Behandelen van bedrijfsmiddelen

Beheersmaatregel

Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. (ISO 8.2.3)

Implementatierichtlijn

Voor het hanteren, verwerken, opslaan en communiceren van informatie behoren procedures te worden opgesteld die consistent zijn met de classificatie van de informatie (zie ISO 8.2.1).

Met de volgende aspecten behoort rekening te worden gehouden:

a) toegangsbeperkingen die de beschermingseisen van elk classificatieniveau ondersteunen;

b) onderhoud van een formele verslaglegging van de bevoegde ontvangers van 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 IT-bedrijfsmiddelen in overeenstemming met de voorschriften van de fabrikant;

e) duidelijke markering van alle kopieën van media ter attentie van de bevoegde ontvanger.

Het binnen de organisatie gebruikte classificatieschema is mogelijk niet gelijk aan de schema's die door andere organisaties worden gebruikt, zelfs als de namen van de niveaus gelijk zijn; bovendien kan informatie die zich tussen organisaties beweegt variëren in classificatie afhankelijk van de context in elke organisatie, zelfs als de classificatieschema's identiek zijn.

Overeenkomsten met andere organisaties waar het delen van informatie in voorkomt, behoren procedures te bevatten voor het identificeren van de classificatie van die informatie en voor het interpreteren van de classificatielabels van andere organisaties.

C.2.5.2 Beleid en procedures voor informatietransport

Beheersmaatregel

Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn. (ISO 13.2.1)

Implementatierichtlijn

Bij procedures die moeten worden gevolgd en beheersmaatregelen die moeten worden uitgevoerd bij het gebruik van communicatiefaciliteiten voor informatietransport behoren de volgende punten in overweging te worden genomen:

a) procedures die zijn ontworpen ter beveiliging van overgedragen informatie tegen interceptie, kopiëren, wijziging, foutieve routering en vernietiging;

b) procedures voor het opsporen van en beschermen tegen malware die kan worden overgebracht door het gebruik van elektronische communicatie (zie ISO 12.2.1);

c) procedures ter bescherming van als bijlage gecommuniceerde gevoelige elektronische informatie;

c) beleid of richtlijnen die aanvaardbaar gebruik van communicatiefaciliteiten omschrijven (zie ISO 7.1.3);

d) verantwoordelijkheden van personeel, van externe partijen en van andere gebruikers om de organisatie niet te compromitteren, bijv. door laster, posten, aannemen van een valse hoedanigheid, lastigvallen, onbevoegde inkopen enz.;

f) gebruik van cryptografische technieken, bijv. om de vertrouwelijkheid, integriteit en authenticiteit van informatie te beschermen (zie hoofdstuk ISO 10);

g) richtlijnen voor bewaren en vernietigen van alle bedrijfscorrespondentie, waaronder berichten, in overeenstemming met relevante nationale en lokale wet- en regelgeving;

h) beheersmaatregelen en beperkingen die samenhangen met het gebruik van communicatiefaciliteiten, bijv. het geautomatiseerd doorsturen van e-mail naar externe e-mailadressen;

i) personeel adviseren om passende voorzorgsmaatregelen te treffen om geen vertrouwelijke informatie bekend te maken;

j) geen berichten die vertrouwelijke informatie bevatten achterlaten op antwoordapparaten omdat deze kunnen worden afgespeeld door onbevoegde personen, op gemeenschappelijke systemen kunnen worden opgeslagen of zelfs kunnen worden opgeslagen als gevolg van foutieve nummerkeuze;

k) personeel informeren over problemen in verband met het gebruik 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;

3) documenten en berichten naar het verkeerde nummer sturen door onjuiste nummerkeuze of door het verkeerde opgeslagen nummer te gebruiken.

Bovendien behoort personeel eraan te worden herinnerd dat zij geen vertrouwelijke gesprekken mogen inplannen gebeuren of via onbeveiligde communicatiekanalen, in open kantoren en op vergaderlocaties.

Diensten op het gebied van informatietransport behoren te voldoen aan re evante wetteljke eisen (zie ISO 15.1).

C.2.5.3 Overeenkomsten over informatietransport

Beheersmaatregel

Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen. (ISO 13.2.2)

Implementatierichtlijn

Overeenkomsten over informat etransport behoren het volgende te bevatten:

a) directieverantwoordelijkheden voor het beheersen en notificeren van overdracht, verzending en ontvangst;

b) procedures om de traceerbaarheid en onweerlegbaarheid te waarborgen;

c) technische minimumeisen voor het verpakken en versturen;

d) bergoveree nkomsten;

e) koerieridentificatienormen;

f) verantwoordelijkheden en aansprakelijkheden in geval van informatiebeveiligingsincidenten, zoals verlies van gegevens;

g) gebruik van een afgesproken labelsysteem voor gevoelige of essentiele informatie dat waarborgt dat de betekenis van de labels meteen duidelijk is en dat de informatie passend is beschermd (zie ISO 6.2).

h) technische normen voor het vastleggen en lezen van informatie en software;

i) speciale beheersmaatregelen die vereist zijn om gevoelige informatie te beschermen, zoals cryptografie (zie hoofdstuk ISO 10).

j) handhaven van een bewakingsketen voor informatie tijdens verzending;

k) acceptabele niveaus van toegangsbeveiliging.

Ter bescherming van informatie en fysieke media dienen duidelijke overeenkomsten, beleidsregels, procedures te bestaan te worden vastgesteld en gehandhaafd (zie ISO 8.3.3), en kunnen behoort in overdrachtsovereenkomsten te worden verwerkt.

De informatiebeveiligingsinhoud van een overeenkomst behoort de gevoeligheid van de desbetreffende bedrijfsinformatie weer te geven.

C.2.5.4 Archiefbeheer

Beheersmaatregel

Er worden voldoende maatregelen genomen om op een effectieve manier bij te dragen aan het borgen en het voortdurend verbeteren van de informatiehuishouding. Het archiefbeheer moet voldoen aan de gestelde eisen zoals opgenomen in de Baseline Informatiehuishouding Rijksoverheid.

Implementatierichtlijn

De verbeteringen die voortkomen uit de bevindingen van de jaarlijkse monitor (vanuit het toezicht) zijn ingebed in de werkprocessen van de bedrijfsonderdelen. Bij de bedrijfsonderdelen is een kwaliteitssysteem binnen de eigen plan- en cyclusopzet geïmplementeerd en in werking.

C.2.5.5 Beheer van verwijderbare media

Beheersmaatregel

Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld. (ISO 8.3.1)

Implementatierichtlijn

Voor het beheren van verwijderbare media behoren de volgende richtlijnen in acht te worden genomen:

a) van herbruikbare media die de organisatie verlaten, behoort de inhoud, als die niet meer nodig is, onherstelbaar te worden verwijderd;

b) indien nodig en haalbaar behoort goedkeuring te worden verkregen om media uit de organisatie te verwijderen en er behoort een verslaglegging van dergelijke verwijderingen te worden bijgehouden voor het ondersteunen van een auditspoor;

c) alle media behoren te worden opgeslagen in een veilige beveiligde omgeving, in overeenstemming met de voorschriften van de fabrikant;

d) indien vertrouwelijkheid of integriteit van gegevens belangrijke overwegingen zijn, behoren cryptografische technieken te worden gebruikt om gegevens op verwijderbare media te beschermen;

e) om het risico te verkleinen dat media in kwaliteit achteruitgaan terwijl de opgeslagen gegevens nog nodig zijn, behoren de gegevens te worden overgebracht naar nieuwe media voordat ze onleesbaar worden;

f) van waardevolle gegevens behoren meerdere kopieën op verschillende media te worden opgeslagen om het risico verder te verminderen van toevallige beschadiging of verlies van gegevens;

g) om de kans op verlies van gegevens te beperken behoort registratie van verwijderbare media te worden overwogen;

h) stations voor verwijderbare media behoren alleen te worden ingeschakeld als een bedrijfsreden is om dit te doen;

i) als er behoefte is om verwijderbare media te gebruiken behoort de overdracht van informatie op dergelijke media te worden gemonitord.

Procedures en aanbiedingsniveaus behoren te worden gedocumenteerd.

C.2.6.6 Verwijderen van media

Beheersmaatregel

Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. (ISO 8.3.2)

Implementatierichtlijn

Voor het beveiligd verwijderen van media behoren formele procedures te worden vastgesteld om het risico zo klein mogelijk te houden dat vertrouwelijke informatie bij onbevoegde personen terechtkomt. De procedures voor het beveiligd verwijderen van media 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) media die vertrouwelijke informatie bevatten behoren op een beveiligde manier te worden opgeslagen en verwijderd, bijv. door verbranding of vernippering, of de gegevens behoren te worden gewist voordat de media worden gebruikt door een andere toepassing in de organisatie;

b) er behoren procedures te zijn om media te identificeren die mogelijk veilig moeten worden verwijderd;

c) mogelijk is het eenvoudiger om ervoor te kiezen alle media in te zamelen en veilig te verwijderen in plaats van te proberen de gevoelige media te scheiden van de rest;

d) veel organisaties bieden voor media inzamelings- en verwijderingsdiensten aan; de keuze voor een passende externe partij dient te beschikken over adequate beheersmaatregelen en ervaring behoort zorgvuldig te geb[illegible];

e) verwijdering van gevoelige media behoort te worden geregistreerd om een audittraject te ondersteunen.

Bij het accumuleren van media voor verwijdering behoort rekening te worden gehouden met het zogenaamde aggregatie-effect, waardoor een grote hoeveelheid niet-gevoelige informatie gevoelig kan worden.

C.2.6.7 Media fysiek overdragen

Beheersmaatregel

Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport. (ISO 8.3.3)

Implementatierichtlijn

De volgende richtlijnen behoren te worden overwogen om media die informatie bevatten te beschermen tijdens transport:

a) er behoren betrouwbare transport- of koeriersdiensten te worden gebruikt;

b) met de directie kan worden afgesproken welke koeriersdiensten bevoegd zijn;

c) er behoren procedures te worden ontwikkeld om de identificatie van koeriers te verifiëren;

d) de verpakking behoort toereikend te zijn om de inhoud te beschermen tegen fysieke schade die tijdens transport kan ontstaan en behoort in overeenstemming te zijn met de voorschriften van de fabrikant, bijv. bescherming tegen milieufactoren die het herstelvermogen van de media kunnen verminderen zoals blootstelling aan hitte, vocht of elektromagnetische velden;

e) er behoren registraties te worden bijgehouden die de inhoud van de media en de toegepaste bescherming identificeren en waarin wordt vastgelegd hoe vaak de media zijn vervoerd naar de beheerder en het in ontvangst nemen op de plaats van bestemming.

C.2.5.8 Elektronische berichten

Beheersmaatregel

Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd. (ISO

13.2.3)

Implementatierichtlijn

Overwegingen betreffende informatiebeveiliging van elektronisch berichtenverkeer behoren de volgende aspecten te behelzen:

a) berichten beschermen tegen onbevoegde toegang, wijziging of weigering van dienstverlening in overeenstemming met het classificatieschema dat de organisatie heeft aangenomen;

b) correcte adressering en transport van het bericht waarborgen;

c) betrouwbaarheid en beschikbaarheid van de dienst;

d) wettelijke overwegingen, bijv. eisen voor elektronische handtekeningen;

e) toestemming verkrijgen voorafgaand aan het gebruiken van externe openbare diensten zoals instant messaging, sociale netwerken of delen van bestanden;

f) hogere niveaus van authenticatie voor het controleren van de toegang vanuit openbaar toegankelijke netwerken.

C.2.6. Mobiele apparatuur

Doelstelling

Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. (ISO 6.2.1)

Implementatierichtlijn

Bij het gebruikmaken van mobiele apparatuur behoort er speciaal op te worden gelet dat bedrijfsinformatie niet wordt gecompromitteerd. Het beleid voor mobiele apparatuur behoort rekening te houden met de risico's van werken met mobiele apparatuur in onbeschermde omgevingen.

Het beleid voor mobiele apparatuur behoort in overweging te nemen:

a) registratie van mobiele apparatuur;

b) eisen voor fysieke bescherming;

c) beperking van installeren van software;

d) eisen voor softwareversies voor mobiele apparatuur en voor het toepassen van patches;

e) beperking van verbinding met informatiediensten;

f) toegangsbeveiligingsmaatregelen;

g) cryptografische technieken;

h) bescherming tegen malware;

i) het op afstand onbruikbaar maken, wissen, uitsluiten;

j) back-ups;

k) gebruik van internetdiensten en -apps.

Voorzichtigheid is geboden bij het gebruik van mobiele apparatuur in openbare ruimten, vergaderruimten en andere onbeschermde locaties. Er behoort bevestiging te zijn om onbevoegde toegang tot of openbaarmaking van de op deze apparaten opgeslagen of verwerkte informatie te voorkomen, bijv. door gebruik te maken van cryptografische technieken (zie hoofdstuk ISO 10) en het gebruik van geheime authenticatie-informatie (zie ISO 9.2.4).

Mobiele apparatuur behoort ook fysiek te zijn beveiligd tegen diefstal, in het bijzonder wanneer deze wordt achtergelaten in bijv. een auto of andere vervoermiddelen, in hotelkamers, conferentie- en vergaderruimten. Er behoort een speciale procedure te worden vastgesteld voor diefstal, verlies van mobiele apparatuur e.d. waarin rekening is gehouden met juridische, verzekerings- en andere veiligheidseisen die in de organisatie gelden. Apparatuur die belangrijke, gevoelige of essentiële bedrijfsinformatie draagt, behoort niet onbewaakt te worden achtergelaten, en behoort, waar mogelijk fysiek achter slot en grendel te worden opgeborgen of er behoren speciale sloten te worden gebruikt om de apparatuur te beveiligen.

Medewerkers die mobiele apparatuur gebruiken, behoren te worden getraind zodat ze zich bewust worden van de extra risico's die deze manier van werken met zich meebrengt en ze weten welke beheersmaatregelen behoren te worden geïmplementeerd

Als het beleid voor mobiele apparatuur toestaat dat medewerkers gebruikmaken van mobiele apparatuur die hun eigendom is, behoren het beleid en gerelateerde veiligheidsmaatregelen ook de volgende aspecten in overweging te nemen:

a) scheiding van privé- 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) toegang verschaffen tot bedrijfsinformatie alleen nadat gebruikers een eindgebruikersovereenkomst hebben ondertekend waarin zij hun verplichtingen bevestigen (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 geautoriseerd zijn. Dit beleid moet rekening houden met de privacywetgeving

C.2.7. Telewerken en thuiswerken

Beheersmaatregel

Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen. (ISO 6.2.2)

Zie ook Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein (ISO 11.2.6)

Implementatierichtlijn

Organisaties die telewerken toestaan, behoren een beleid uit te vaardigen dat de voorwaarden en beperkingen definieert voor het telewerken. Waar van toepassing geacht en wettelijk toegestaan, behoort rekening te worden gehouden met de volgende zaken:

a) de bestaande fysieke beveiliging van de telewerklocatie, waarbij rekening wordt gehouden met de fysieke beveiliging van het gebouw en de lokale omgeving

b) de voorgestelde fysieke telewerkomgeving;

c) de beveiligingseisen die voor communicatie gelden, waarbij rekening wordt gehouden met de behoefte aan toegang op afstand tot de interne systemen van de organisatie, de gevoeligheid van de informatie die wordt benaderd en via de communicatiekoppeling wordt doorgegeven en de gevoeligheid van het interne systeem;

d) het verlenen van virtuele desktoptoegang waardoor het verwerken en opslaan van informatie op privéapparatuur wordt voorkomen;

e) de bedreiging van onbevoegde toegang tot informatie of middelen van andere gebruikers van de accommodatie, bijv. familie en vrienden;

f) het gebruik van thuisnetwerken en de eisen of beperkingen van de configuratie van draadloze netwerkdiensten;

g) beleidsregels en procedures ter voorkoming van geschillen over rechten van intellectueel eigendom die is ontwikkeld op privéapparatuur;

h) toegang tot privéapparatuur (om de veiligheid van het apparaat vast te stellen of tijdens een onderzoek), wat wetgeving mogelijk kan verhinderen;

i) softwarelicentiecontracten waardoor de organisatie aansprakelijk kan worden gesteld voor de licenties van clientsoftware op werkstations die privébezit zijn van medewerkers of van externe gebruikers;

j) beveiliging tegen malware en eisen aan de firewall.

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

a) het beschikbaar stellen van passende apparatuur en opbergmeubelen voor de telewerkactiviteiten, waarbij het gebruik van privéapparatuur die niet onder het beheer van de organisatie staat, niet is toegelaten;

b) een definitie van gedefinieerde werkzaamheden, de werktijden, de classificatie van informatie waarover men mag beschikken en de interne systemen en diensten waartoe de telewerker toegang heeft;

c) het beschikbaar stellen van passende communicatievoorzieningen, met inbegrip van methoden voor het beveiligen van de toegang op afstand;

d) fysieke beveiliging;

e) regels en richtlijnen voor toegang voor familie en bezoekers tot apparatuur en informatie;

f) het beschikbaar stellen van ondersteuning en onderhoud van hardware en software;

g) het regelen van de verzekering;

h) de procedures voor de back-up en de bedrijfscontinuïteit;

i) audit en monitoren van de beveiliging;

j) intrekking van bevoegdheid en toegangsrechten, en het inleveren van apparatuur na beëindiging van de telewerkactiviteiten.

C.2.8. Gebruik van cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit/ en/of integriteit van informatie te beschermen.

C.2.8.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel

Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. (ISO 10.1.1)

Implementatierichtlijn

Bij het ontwikkelen van een cryptografiebeleid behoren de volgende aspecten in aanmerking te worden genomen:

a) de manier waarop de directie het gebruik van cryptografische beheersmaatregelen in de gehele organisatie benadert, met inbegrip van de algemene principes die gelden voor de bescherming van de bedrijfsinformatie;

b) het vereiste beschermingsniveau behoort te worden geïdentificeerd op basis van een risicobeoordeling, rekening houdend met type, sterkte en kwaliteit van het vereiste versleutelingsalgoritme;

c) het gebruik van versleuteling ter bescherming van informatie die wordt vervoerd per draagbare of verwijderbare media-apparatuur of via communicatiekanalen;

d) de aanpak van sleutelbeheer, waaronder methoden tar bescherming van cryptografische sleutels en het herstel van versleutelde informatie in geval van verloren, gecompromitteerde of beschadigde sleutels;

e) rollen en verantwoordelijkheden, bijv. wie is verantwoordelijk voor:

1) het implementeren van het beleid;

2) het sleutelbeheer, waaronder het aanmaken van sleutels (zie ISO 10.1.2);

f) de normen die moeten worden toegepast voor een doeltreffende implementatie in de gehele organisatie (welke oplossing wordt gebruikt voor welk bedrijfsproces);

g) de impact van het gebruik van versleutelde informatie op beheersmaatregelen die zijn gebaseerd op controle van de inhoud (bijv. detectie van malware).

Bij het implementeren van het cryptografiebeleid behoort rekening te worden gehouden met de regelgeving en nationale beperkingen die kunnen gelden voor het gebruik van cryptografische technieken in verschillende delen van de wereld en met problemen met grensoverschrijdende stromen van versleutelde informatie (zie ISO 18.1.5).

Cryptografische beheersmaatregelen kunnen worden gebruikt voor verschillende informatiebeveiligingsdoelstellingen, bijv.:

a) **vertrouwelijkheid:** codering van informatie gebruiken om gevoelige of essentiële informatie, tijdens opslag of verzending, te beschermen;

b) **integriteit/authenticiteit:** digitale handtekeningen of authenticatiecodes voor berichten gebruiken om te garanderen dat of integriteit van gevoelige of essentiële informatie tijdens opslag of verzending te verifiëren;

c) **onweerlegbaarheid:** cryptografische technieken gebruiken om bewijs te verkrijgen van het al dan niet plaatsvinden van een gebeurtenis of actie;

c) **authenticatie:** cryptografische technieken gebruiken ter authenticatie van gebruikers en andere systeementiteiten die toegang vragen tot of die verrichtingen doen met systeemgebruikers, -entiteiten en -bronnen.

G.2.8.2 Beheer van cryptografische sleutels

Beheersmaatregel:

Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd. (ISO 10.1.2)

Implementatierichtlijn

Het beleid behoort eisen te bevatten voor het beheren van cryptografische sleutels tijdens hun gehele levenscyclus met inbegrip van het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van sleutels.

Cryptografische algoritmen, sleutellengte en gebruikspraktijken behoren te worden geselecteerd in overeenstemming met de "best practices". Passend sleutelbeheer omvat naleving van procedures voor het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van cryptografische sleutels.

Alle cryptografische sleutels behoren te worden beschermd tegen aanpassing en verlies. Bovendien behoren geheime en particuliere sleutels bescherming nodig tegen ongeoorloofd gebruik en tegen openbaarmaking. Apparatuur die wordt gebruikt om sleutels aan te maken, op te slaan en te archiveren behoort fysiek te worden beschermd.

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 behoren te 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 sleutels behoren te worden teruggetrokken of gedeactiveerd, 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 gecompromitteerd zijn;

i) **het back-uppen of archiveren** van sleutels;

j) **het vernietigen van sleutels**;

k) het registreren en auditen van aan sleutelbeheer gerelateerde activiteiten.

Om de kans op onjuist gebruik te verkleinen behoren de activerings- en deactiveringsdatum van sleutels te worden vastgesteld zodat de sleutels alleen kunnen worden gebruikt tijdens de periode die in het desbetreffende sleutelbeheerbeleid is vastgesteld.

Naast het zorgvuldig beheren van geheime en persoonlijke sleutels behoort ook aandacht te worden besteed aan de authenticiteit van openbare sleutels. Deze authenticiteitsprocedure kan worden uitgevoerd met gebruikmaking van openbaresleutelcertificaten, die gewoonlijk worden uitgegeven door een certificerende instantie, die een erkende organisatie behoort te zijn die beschikt over passende beheersmaatregelen en procedures om de vereiste mate van betrouwbaarheid te kunnen leveren.

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 ISO 15.2).

C.2.8.3 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel

Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving (ISO 18.1.3).

Implementatierichtlijn

Voor de naleving van relevante overeenkomsten, wet- en regelgeving behoort met de volgende punten rekening te worden gehouden:

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 is ontworpen dat er cryptografische functies aan kunnen worden toegevoegd;

c) beperkingen op de toepassing van codering;

d) verplichte of discretionaire toegang voor autoriteiten tot informatie die door hardware of software is versleuteld om de vertrouwelijkheid van de inhoud te voorzien.

Om naleving van de relevante wet- en regelgeving te waarborgen behoort juridisch advies te worden ingewonnen. Ook voordat versleutelde informatie of cryptografische beheersmaatregelen over grenzen van rechtsgebieden worden verstuurd, behoort juridisch advies te worden ingewonnen.

C.2.9. 'Clear desk' en 'clear screen'

Beheersmaatregel

Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld. (ISO 11.2.9)

Implementatierichtlijn

Bij het 'clear desk'- en 'clear screen'-beleid behoort rekening te worden gehouden met de informatieclassificatie (zie ISO 8.2), wettelijke en contractuele eisen (zie ISO 18.1) en de bijbehorende risico's en bedrijfscultuur van de organisatie.

Met de volgende richtlijnen behoort rekening te worden gehouden:

a) gevoelige of essentiële bedrijfsinformatie, bijv. op papier of op elektronische opslagmedia, behoort is een afgesloten ruimte te worden bewaard (idealiter in een kluis, een kast of een andere vorm van beveiligd meubilair) wanneer deze informatie niet vereist is, vooral als het vertrek verlaten is.

b) onbeheerde computers en terminals behoren uitgelogd of beschermd te zijn met een scherm- en toetsenbordvergrendeling met wachtwoord, token of vergelijkbare gebruikersauthenticatie; wanneer ze niet worden gebruikt behoren computers en terminals te worden beschermd door toetsvergrendeling, wachtwoorden of andere beheersmaatregelen;

c) onbevoegd gebruik van fotokopieerapparaten en andere reproductieapparatuur (bijv. scanners, digitale camera's) behoort te worden voorkomen;

d) media die gevoelige of geheime informatie bevatten, behoren na het afdrukken onmiddellijk van printers te worden verwijderd.

C.2.10. Intellectuele-eigendomsrechten

Beheersmaatregel

Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd. (ISO 18.1.2)

Implementatierichtlijn

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

a) een beleid ten aanzien van de naleving van intellectuele-eigendomsrechten publiceren dat het wettig gebruik van software en informatieproducten definieert;

b) software alleen verkrijgen bij bekende bronnen met een goede reputatie, om te waarborgen dat het auteursrecht niet wordt geschonden;

c) het bewustzijn in stand houden van het beleid voor de bescherming van intellectuele-eigendomsrechten en bekendheid geven aan het voornemen om disciplinaire maatregelen te nemen tegen personeel dat deze rechten schendt;

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, masterschijven, handleidingen enz.

f) beheersmaatregelen implementeren om te bewerkstelligen dat een maximumaantal gebruikers dat eventueel door de licentie is toegestaan niet wordt overschreden;

g) beoordelingen uitvoeren om te controleren dat alleen goedgekeurde software en in licentie gegeven producten zijn geïnstalleerd;

h) een beleid vaststellen voor het handhaven van de juiste licentievoorwaarden;

i) een beleid vaststellen voor het verwijderen van of aan anderen overdragen van software;

j) voldoen aan voorwaarden voor software en informatie verkregen van openbare netwerken;

k) niet dupliceren, naar een ander formaat converteren of een uittreksel maken van commerciële opnamen (film, audio), tenzij auteursrechtelijk toegestaan;

l) geen boeken, artikelen, rapporten of andere documenten geheel of ten dele kopiëren, tenzij auteursrechtelijk toegestaan.

C.2.11. Geheimhouding

Beheersmaatregel

Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd. (ISO 13.2.4)

Implementatierichtlijn

Vertrouwelijkheids- of geheimhoudingsovereenkomsten behoren de eis van bescherming van vertrouwelijke informatie te behandelen binnen juridisch afdwingbare voorwaarden. Vertrouwelijkheids- of geheimhoudingsovereenkomsten zijn van toepassing op externe partijen of medewerkers van de organisatie. Rekening houdend met de aard van de andere partij en de haar toegestane toegang of hantering van vertrouwelijke informatie behoren elementen van de overeenkomst te worden gekozen of toegevoegd.

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) verwachte looptijd van een overeenkomst, met inbegrip van gevallen waarin de vertrouwelijkheid mogelijk onbepaald moet worden gehandhaafd;

c) vereiste acties als een overeenkomst is beëindigd;

d) verantwoordelijkheden en acties van de ondertekenaars betreffende het vermijden van onbevoegd openbaar maken van informatie;

e) eigendom van informatie, handelsgeheimen en intellectuele eigendom, en hoe dit zich verhoudt tot de bescherming van vertrouwelijke informatie;

f) het toegestane gebruik van vertrouwelijke informatie en de rechten van de ondertekenaar om informatie te gebruiken;

g) het recht om activiteiten waar vertrouwelijke informatie bij betrokken is te auditen en te monitoren;

h) procedure voor het notificeren en melden van ongeautoriseerde openbaarmaking of lekken van vertrouwelijke informatie;

i) voorwaarden voor teruggaven of vernietigen van informatie na beëindiging van de overeenkomst;

j) verwachte acties die moeten worden ondernomen in geval van schending van de overeenkomst.

Afhankelijk van de eisen van de organisatie betreffende informatiebeveiliging behoren mogelijk nog andere elementen te worden opgenomen in een vertrouwelijkheids- of geheimhoudingsovereenkomst.

Vertrouwelijkheids- en geheimhoudingsovereenkomsten behoren te voldoen aan alle toepasselijke wetten en regelgeving voor het rechtsgebied waar zij voor gelden (zie ISO 18.1).

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

C.2.12. Bedrijfscontinuïteit

C.2.12.1 Beleid voor bedrijfscontinuïteit

Beheersmaatregel

Er is tactisch beleid voor bedrijfscontinuïteit vastgesteld, gedocumenteerd en beheerseld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van prioriteiten.

Implementatierichtlijnen

De implementatierichtlijnen staan beschreven in Deel C.

C.2.12.2 Informatiebeveiligingscontinuïteit

Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

C.2.12.2.1 Informatiebeveiligingscontinuïteit plannen

Beheersmaatregel

De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen. (ISO 17.1.1)

Implementatierichtlijn

Een organisatie behoort vast te stellen of de continuïteit van de informatiebeveiliging onder het beheerproces van de bedrijfscontinuïteit valt of onder het beheerproces van samenherstel. Informatiebeveiligingseisen behoren te worden vastgesteld als de planning voor bedrijfscontinuïteit- en ramenherstel wordt gemaakt.

Bij afwezigheid van een formele planning voor bedrijfscontinuïteit en ramenherstel behoort het

informatiebeveiligingsbeheer ervan uit te gaan dat informatiebeveiligingseisen in ongunstige situaties hetzelfde blijven als in normale uitvoeringsomstandigheden. In het andere geval kan een organisatie een bedrijfsimpactanalyse uitvoeren voor informatiebeveiligingsaspecten om de informatiebeveiligingseisen vast te stellen die van toepassing zijn op ongunstige situaties.

C.2.12.2.2 Informatiebeveiligingscontinuïteit implementeren

Beheersmaatregel

De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. (ISO 17.1.2)

Implementatierichtlijn

Een organisatie behoort ervoor te zorgen dat:

a) er een adequate beheerstructuur is die is voorbereid op een verstorende gebeurtenis, deze verzacht en erop reageert met personeel dat beschikt over de nodige autoriteit, ervaring en competentie;

b) personeel voor incidentrespons wordt aangesteld dat beschikt over de nodige verantwoordelijkheid, autoriteit en competentie om een incident te afhandelen en de informatiebeveiliging te handhaven;

c) op basis van door de directie goedgekeurde doelstellingen voor informatiebeveiligingscontinuïteit, gedocumenteerde plannen, respons- en herstelprocedures worden ontwikkeld en goedgekeurd, waarin gedetailleerd wordt omschreven hoe de organisatie een verstorende gebeurtenis zal aanpakken en haar informatiebeveiliging op een vooraf vastgesteld niveau zal handhaven (zie 17.1.1).

In overeenstemming met de eisen voor informatiebeveiligingscontinuïteit behoort de organisatie het volgende vast te stellen, te documenteren, te implementeren en te onderhouden:

a) beheersmaatregelen voor informatiebeveiliging binnen processen, procedures en ondersteunende systemen en instrumenten voor bedrijfscontinuïteit of rampenherstel;

b) processen, procedures en implementatieveranderingen om bestaande beheersmaatregelen voor informatiebeveiliging tijdens een ongunstige situatie te handhaven;

c) compenserende beheersmaatregelen voor beheersmaatregelen voor informatiebeveiliging die tijdens een ongunstige situatie niet kunnen worden gehandhaafd.

C.2.12.2.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Beheersmaatregel

De organisatie behoort de (een behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze doeltreffend en doeltreffend zijn tijdens ongunstige situaties. (ISO 17.1.3)

Implementatierichtlijn

Veranderingen betreffende de organisatie, procedures, processen of van technische aard, hetzij in een context van uitvoering, herzij van continuïteit, kunnen leiden tot veranderingen in de eisen betreffende informatiebeveiligingscontinuïteit. In dergelijke gevallen behoort de continuïteit van processen, procedures en beheersmaatregelen voor informatiebeveiliging te worden beoordeeld tegen de achtergrond van deze veranderde eisen.

Organisaties behoren de continuïteit van hun informatiebeveiligingsbeheer te verifiëren door:

a) de functionaliteit van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te oefenen en te testen om te waarborgen dat ze consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit;

b) de kennis en routine voor het uitvoeren van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te oefenen en te testen om te waarborgen dat de prestaties consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit;

c) de deugdelijkheid en doeltreffendheid van maatregelen voor informatiebeveiligingscontinuïteit te beoordelen als informatiesystemen, informatiebeveiligingsprocessen, -procedures en -beheersmaatregelen, of de procedures en oplossingen van bedrijfscontinuïteitsbeheer of rampenherstelbeheer veranderen.

C.2.13.1.4 Beschikbaarheid van informatieverwerkende faciliteiten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen. (ISO 17.2)

Beheersmaatregel

Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. (ISO 17.2.1)

Implementatierichtlijn

Organisaties behoren de bedrijfseisen voor de beschikbaarheid van informatiesystemen vast te stellen. Als de beschikbaarheid niet kan worden gegarandeerd door middel van de bestaande systeemarchitectuur, behoren redundante componenten of architecturen in overweging te worden genomen.

Indien van toepassing 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.

C.3. Tactisch beveiligingsbeheer

Doelstelling

Tactisch beveiligingsbeheer borgt op tactisch niveau het in samenhang doen treffen van beveiligingsmaatregelen in de organisatie of het organisatiedeel in overeenstemming met de normen en beheerst op operationeel niveau de toegangsverlening tot en de overige beveiligingseigenschappen van voorzieringen voor IT en huisvesting.

Toelichting

Het beheren van informatiebeveiliging omvat het uitwerken van de managementverantwoordelijkheden op dit gebied, het afstemmen van de beveiligingsmaatregelen binnen de verschillende verantwoordelijkheidsgebieden, het inzetten van deskundig beveiligingsadvies en het controleren van de naleving van de beveiligingskaders (beleid en normen).

De begrippen (tactisch, kaders, advies, toetsen en toezien) in dit proces moeten in zijn context worden gezien; het gaat bij dit beheer om het ondersteunen van het management in de verschillende lagen van een organisatie. De activiteiten in dit ondersteunende proces zijn op de verschillende niveaus van de organisatie in principe hetzelfde, de mate van abstractie van de activiteiten verschilt, evenals het hoofdaccent bij de uitvoering van de verschillende fasen in het proces.

Motivering

Beveiliging is een lijn- en soms projectverantwoordelijkheid. Beveiligingsmaatregelen worden overal getroffen in de verschillende verantwoordelijkheidsgebieden (organisatie, processen en producten). Om te bereiken dat deze beveiligingsmaatregelen een evenwichtig op elkaar afgestemd geheel vormen, wordt aan het lijn- en projectmanagement ondersteuning verleend door beveiligingsdeskundigen. Het beveiligingsbeheer op tactisch niveau is voorwaardenscheppend voor het aantoonbaar kunnen bereiken en handhaven van het gewenste/vereiste beveiligingsniveau in een organisatie. Dit proces in combinatie met de organisatie van en communicatie tussen de verschillende beveiligingsbeheerders op tactisch niveau moet de totale samenhang van de maatregelen in een organisatie borgen.

Zonder kaderstelling, advisering, toetsing en evaluatie van getroffen maatregelen en kaders wordt het risico gelopen dat het geheel van de beveiligingsmaatregelen niet goed zijn afgestemd op de risico's in een organisatie.

C.3.1. Kwaliteit beveiligingsfunctionarissen

Beheersmaatregel

Beveiligingsfunctionarissen voldoen aan eisen passend bij de beroepsuitoefening.

Implementatierichtlijn

a) Beveiligingsfunctionarissen voldoen aan het profiel van de beroepseisen, aan eisen van opleiding en permanente educatie.

b) Er worden in voldoende mate contacten onderhouden binnen de organisatie om tijdig betrokken te zijn bij de totstandkoming van beleidsstukken, architecturen en organisatieveranderingen met relevantie voor beveiliging.

c) Er worden geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties onderhouden, als middel om:

1. kennis te vergroten van beproefde werkwijzen ('best practice') en op de hoogte te blijven van de laatste stand van zaken op het gebied van beveiliging;

2. te waarborgen dat kennis en begrip van het vakgebied beveiliging volledig actueel en compleet zijn;

3. toegang te verkrijgen tot deskundig beveiligingsadvies;

4. informatie over nieuwe technologieën, producten, bedreigingen of kwetsbaarheden te delen en uit te wisselen.

C.3.2. Stellen kaders

Beheersmaatregel

Er worden kaders gesteld op het gebied van beveiliging als advies aan het management toe te richting te geven aan het treffen van beveiligingsmaatregelen in overeenstemming met wet- en regelgeving en standaards van het vakgebied.

Implementatierichtlijn

a) Afhankelijk van het niveau of verantwoordingsgebied waarvoor Tactisch Beveiligingsbeheer functioneert, worden beveiligingsomgevingskaders, methoden, technieken, hulpmiddelen en voorschriften ontwikkeld, die

1. gebaseerd zijn op wet- en regelgeving en standaards in het vakgebied, rekenschap met het strategisch beveiligingsbeleid;
2. afgestemd zijn met relevante andere kaders binnen de organisatie en afspraken met klanten of leveranciers;
3. goedgekeurd zijn door het management.

b) Voor gegevens die niet vallen onder het regiem van het Vifdd maar wel extra risico's met zich mee brengen, wordt op basis van een risicoanalyse een classificatie van (extra) maatregelen opgesteld. Het kan om klantgroepen en/of dossiers zaan met een extra vertrouwelijk karakter.

c) Jaarlijks wordt er een door het management goedgekeurd beveiligingsplan opgesteld, waarin is vastgelegd welke verbeteracties er noodzakelijk zijn om aan de normen te voldoen. Dit plan is gebaseerd op wijzigingen in het dreigingsprofiel, uitkomsten van het evaluatieproces, een analyse van eventuele risico's en de te verwachten ontwikkelingen in de verschillende verantwoordelijkheidsgebieden (processen en producten).

C.3.3. Onderhouden beveiligingskaders

Beheersmaatregel

De beveiligingskaders worden bijgesteld op basis van controles, testen en evaluaties.

Implementatierichtlijn

a) Beveiligingskaders worden onderhouden op basis van

1. de uitkomsten van C.3.5. Evalueren beveiliging;
2. wijzigingen in organisatie, technieken en processen;
3. periodieke beoordeling van het beveiligingsbeleid;
4. het actuele dreigingsprofiel

C.3.4. Adviseren beveiliging

Beheersmaatregel

Er worden deskundige adviezen gegeven om te bewerkstelligen dat het beveiligingsbeleid en de beveiligingsmaatregelen worden getroffen in overeenstemming met de kaders.

Implementatierichtlijn

a) Er worden afspraken gemaakt met het management of procseseigenaren op basis van welke criteria beveiligingsadvies zal worden ingewonnen, risicoanalyse wordt toegepast dan wel toetsing van beveiligingsmaatregelen plaatsvindt.

b) Er worden adviezen verstrekt en toetsingen verricht aan de hand van beveiligingskaders n.a.v. belangrijke vernieuwingen en wijzigingen in processen en producten en er wordt toegezien op het daadwerkelijk treffen van beveiligingsmaatregelen.

c) De opleiding, training en bewustwording van beveiliging wordt bevorderd in alle lagen van de organisatie.

C.3.5. Evalueren beveiliging

Beheersmaatregel

De beveiligingsmaatregelen en normenkaders worden geëvalueerd.

Implementatierichtlijn

a) De voortgang van het beveiligingsplan wordt geëvalueerd.

b) Er wordt toegezien op afspraken over de uitvoering van interne controles en de naleving van de kaders voor beveiliging.

c) Er wordt toegezien op het uitvoeren van controles op beveiligingsinstellingen van fysieke toegangsvoorzieningen en van IT-voorzieningen, die onderdeel uitmaken van de logische toegangspaden tot gegevens.

d) De uitkomsten van interne en externe controles/audits met beveiligingsrelevantie worden beoordeeld op hun effecten voor de opzet, het bestaan en de werking van de beveiligingsmaatregelen. Er wordt toegezien op het tijdig, juist en volledig oplossen van bevindingen dan wel het verantwoord accepteren van risico's.

e) Beveiligingsrisico's en actuele ontwikkelingen worden geëvalueerd.

f) Er vindt regelmatig en gestructureerd overleg plaats tussen de verschillende beveiligingsdisciplines waarin kaderstelling, adviezen, evaluatie en onderhoud op het gebied van beveiliging aan de orde worden gesteld.

C.3.6. Informatiebeveiligingsbeoordelingen

Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie. (ISO 18.2)

C.3.6.1 Onafhankelijke beoordeling van informatiebeveiliging

Beheersmaatregel

De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld. (ISO 18.2.1)

Implementatierichtlijn

Deze onafhankelijke beoordeling behoort door de directie te worden geïnitieerd. Een dergelijke onafhankelijke beoordeling is nodig om te waarborgen dat de organisatie continu een geschikte, toereikende en doeltreffende aanpak van het beheer van informatiebeveiliging hanteert. Deze beoordeling behoort tevens het beoordelen van verbeteringsmogelijkheden en de noodzaak om wijzigingen aan te brengen in de beveiligingsaanpak te omvatten, met inbegrip van het beleid en de beheersdoelstellingen.

Een dergelijke beoordeling behoort 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 gekwalificeerd is in dergelijke beoordelingen. Personen die deze beoordelingen uitvoeren behoren te beschikken over passende vaardigheden en ervaring.

De resultaten van de onafhankelijke beoordeling behoren te worden vastgelegd en te worden gerapporteerd aan de directie die de beoordeling heeft geïnitieerd. Deze verslagen behoren te worden bewaard.

Indien in de onafhankelijke beoordeling wordt vastgesteld dat de aanpak en de implementatie van het beheer van informatiebeveiliging van de organisatie onbevredigend zijn, bijv. gedocumenteerde doelstellingen en eisen zijn niet gehaald of niet in overeenstemming met de koers voor informatiebeveiliging zoals opgenomen in de beleidsregels voor informatiebeveiliging (zie ISO 5.1.1), behoort de directie corrigerende maatregelen te overwegen.

C.3.6.2 Naleving van beveiligingsbeleid en -normen

Beheersmaatregel

De directie behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. (ISO 18.2.2)

Implementatierichtlijn

Managers behoren vast te stellen op welke manier wordt beoordeeld of is voldaan aan informatiebeveiligingseisen zoals gedefinieerd in beleidsregels, normen en andere toepasselijke regelgeving.

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 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 punten te identificeren.

Resultaten van door managers uitgevoerde beoordelingen en getroffen corrigerende maatregelen behoren te worden geregistreerd en deze verslagen behoren te worden bewaard. Managers behoren de resultaten te rapporteren aan de personen die verantwoordelijke beoordelingen uitvoeren (zie ISO 18.2.1) wanneer een onafhankelijke beoordeling plaatsvindt binnen hun verantwoordelijkheidsgebied.

C.3.6.3 Beoordeling van technische naleving

Beheersmaatregel

Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. (ISO 18.2.3)

Implementatierichtlijn

Technische naleving behoort bij voorkeur te worden beoordeeld met behulp van geautomatiseerde instrumenten die technische rapporten vervaardigen, die vervolgens door een technisch specialist worden geïnterpreteerd. Als alternatief kunnen handmatige beoordelingen (indien nodig ondersteund door passende software-instrumenten) door een ervaren systeemtechnicus worden uitgevoerd.

Indien penetratietests of kwetsbaarheidsbeoordelingen worden toegepast is voorzichtigheid geboden omdat dergelijke activiteiten de beveiliging van het systeem kunnen compromiteren. Dergelijke tests behoren te worden gepland en gedocumenteerd en behoren herhaalbaar te zijn.

Beoordeling van technische naleving behoort uitsluitend te worden uitgevoerd door competente, bevoegde personen of onder toezicht van dergelijke personen.

C.3.6.4 Beheersmaatregelen voor audits op de technische infrastructuur

Beheersmaatregel

Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren. (ISO 12.7.1)

Implementatierichtlijn

De volgende richtlijnen behoren in acht te worden genomen:

a) auditeisen voor toegang tot systemen en gegevens behoren met de juiste managers te worden overeengekomen;

b) het toepassingsgebied van technische audittests behoort te worden afgesproken en te worden gecontroleerd;

c) audittests behoren te worden beperkt tot alleen-lezen-toegang tot software en gegevens;

c) toegang anders dan 'alleen lezen' behoort alleen te worden toegestaan voor geïsoleerde kopieën van systeembestanden, die behoren te worden verwijderd als de audit is uitgevoerd, of ze behoren adequaat te worden beschermd indien het verplicht is deze bestanden bij de vereiste auditdocumenten te bewaren;

e) eisen voor speciale of extra verwerkingsactiviteiten behoren te worden vastgesteld en overeengekomen;

f) auditsoft die de beschikbaarheid van systemen kunnen beïnvloeden, behoren buiten werkuren plaats te vinden;

g) alle toegangshandelingen behoren te worden gemonitord en vastgelegd in een logbestand om een referentietraject te produceren.

C.4. Personele veiligheid

C.4.1. Voorafgaand aan het dienstverband

Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen. (ISO 7.1)

C.4.1.1 Screening

Beheersmaatregel

Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de waargenomen risico's te zijn. (ISO 7.1.1)

Implementatierichtlijn

Verificatie behoort rekening te houden met alle relevante wetgeving op het gebied van privacy, bescherming van persoonsgegevens en arbeidswetgeving, en behoort indien toegelaten, het volgende te omvatten:

a) beschikbaarheid van positieve referenties, bijv. één zakelijke en één persoonlijke;

b) een verificatie (op volledigheid en nauwkeurigheid) van het curriculum vitae van de solliciant;

c) bevestiging van de gedeclareerde academische en beroepskwalificaties

d) onafhankelijke verificatie van de identiteit (paspoort of gelijkwaardig document);

e) meer gedetailleerde verificatie, zoals controle op kredietwaardigheid of strafblad.

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 informatie of zeer vertrouwelijke informatie, behoort de organisatie ook verder te overwegen meer gedetailleerde verificaties te overwegen.

Procedures behoren criteria en beperkingen voor controleonderzoeker te definiëren, bijv wie is competent om personen te screenen, en hoe, wanneer en waarom worden controleonderzoeken uitgevoerd.

Ook voor contractanten behoort voor een screeningprocedure te worden gezorgd. In die gevallen behoort de overeenkomst tussen de organisatie en de contractant de verantwoordelijkheden voor het uitvoeren van de screening te vermelden en de informatieprocedures die moeten worden gevolgd als de screening niet is afgemaakt of als de resultaten aanleiding geven tot twijfel of bezorgdheid.

Informatie over alle kandidaten die in aanmerking komen voor posities binnen de organisatie behoort te worden verzameld en verwerkt in overeenstemming met de relevante wetgeving aanwezig in het relevante rechtsgebied. Afhankelijk van de toepasselijke wetgeving behoren kandidaten vooraf over de screeningactiviteiten te worden geïnformeerd.

C.4.1.2 Arbeidsvoorwaarden

Beheersmaatregel

De contractuele overeenkomst met medewerkers en contractanten behandt hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. (ISO 7.1.2)

Implementatierichtlijn

De contractuele verplichtingen voor medewerkers of contractanten behelzen de beleidsregels van de organisatie voor informatiebeveiliging voor te geven, en tevens duidelijk te maken en te vormelden:

a) dat alle medewerkers en contractanten aan wie toegang wordt verleend tot vertrouwelijke informatie een vertrouwelijkheids- of geheimhoudingsovereenkomst behoren te ondertekenen voordat hun toegang wordt verleend tot informatieverwerkende faciliteiten (zie ISO 13.2.4);

b) de wettelijke verantwoordelijkheden en rechten van de medewerker of contractant, bijv. betreffende auteursrechtwetgeving of wetgeving inzake gegevensbescherming (zie ISO 18.1.2 en ISO 18.1.4);

c) verantwoordelijkheden voor de classificatie van informatie en het beheer van bedrijfsmiddelen van de organisatie die samenhangen met informatie, informatieverwerkende faciliteiten en informatiediensten die door de medewerker of contractant worden gebruikt (zie ook stuk ISO 3),

d) verantwoordelijkheden van de medewerker of contractant voor het verwerken van informatie die is ontvangen van andere bedrijven of externe partijen;

e) acties die moet worden ondernomen indien de medewerker of contractant de beveiligingseisen van de organisatie veronachtzaamt (zie ISO 7.2.3).

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

De organisatie behoort ervoor te zorgen dat medewerkers en contractanten instemmen met voorwaarden betreffende informatiebeveiliging die 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.

Waar van toepassing behoren de verantwoordelijkheden die in de arbeidsvoorwaarden staan voor een vastgestelde periode na het einde van het dienstverband van kracht te blijven (zie ISO 7.3).

C.4.2. Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen. (ISO 7.2)

C.4.2.1 Directieverantwoordelijkheden

Beheersmaatregel

De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. (ISO 7.2.1)

Implementatierichtlijn

De directie behoort ervoor te zorgen dat medewerkers en contractanten:

a) op de juiste wijze worden geïnformeerd over hun informatiebeveiligingsrollen en – verantwoordelijkheden voordat zij toegang krijgen tot vertrouwelijke informatie of informatiesystemen;

b) richtlijnen ontvangen die de verwachtingen met betrekking tot hun informatiebeveiligingsrol binnen de organisatie aangeven;

c) gemotiveerd zijn om te voldoen aan de beleidsregels met betrekking tot informatiebeveiliging van de organisatie;

d) een niveau van bewustzijn over informatiebeveiliging bereiken dat relevant is voor hun rollen en verantwoordelijkheden binnen de organisatie (zie ISO 7.2.2);

e) zich conformeren aan de arbeidsvoorwaarden, die het informatiebeveiligingsbeleid en passende werkmethoden omvatten;

f) continu beschikken over de juiste vaardigheden en kwalificaties en regelmatig worden bijgeschoold

g) via een anoniem kanaal beschikkingen van de beleidsregels of procedures met betrekking tot informatiebeveiliging kunnen melden (‘klokkenluider’).

De directie behoort te laten zien dat ze de beleidsregels, procedures en beheersmaatregelen met betrekking tot informatiebeveiliging ondersteunt, en als rolmodel te handelen.

C.4.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beheersmaatregel

Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. (ISO 7.2.2)

Implementatierichtlijn

Een bewustzijnsprogramma met betrekking tot informatiebeveiliging behoort erop gericht te zijn om medewerkers en, indien relevant contractanten, bewust te maken van hun verantwoordelijkheden voor informatiebeveiliging en de manieren waarop men zich van deze verantwoordelijkheden kan kwijten.

Een bewustzijnsprogramma met betrekking tot informatiebeveiliging behoort te worden vastgesteld in overeenstemming met de beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de informatie van de organisatie die moet worden beschermd en de beleidsregels die zijn geïmplementeerd om de informatie te beschermen. Het bewustzijnsprogramma behoort een aantal bewustwordingsactiviteiten te bevatten, zoals campagnes (bijv. een 'informatiebeveiligingsdag') en het verspreiden van boekjes of nieuwsbrieven.

Bij de opzet van het bewustzijnsprogramma behoort rekening te worden gehouden met de rollen van de medewerker in de organisatie en, indien relevant, de verwachtingen van de organisatie met betrekking tot de bewustwording van contractanten. 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 nieuwe medewerkers en contractanten deze ook meemaken. Het bewustwordingsprogramma behoort ook regelmatig te worden geactualiseerd, zodat het in overeenstemming blijft met de beleidsregels en procedures van de organisatie, en er behoort te worden voortgebouwd op de lessen die zijn getrokken uit informatiebeveiligingsincidenten.

Bewustzijnstraining behoort te worden uitgevoerd zoals vereist door het bewustzijnsprogramma inzake informatiebeveiliging van de organisatie. Bewustzijnstraining kan op verschillende manieren worden gevolgd, bijv. klassikaal, via afstandsonderwijs, via internet, in eigen tempo.

Opleiding en training met betrekking tot informatiebeveiliging behoren ook algemene aspecten te omvatten zoals:

a) het aangeven van de betrokkenheid van de directie bij informatiebeveiliging in de gehele organisatie;

b) de noodzaak om bekend te worden met en te voldoen aan de van toepassing zijnde regels en verplichtingen met betrekking tot informatiebeveiliging zoals gedefinieerd in beleidsregels, normen, wetten, 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 externe partijen;

d) basisprocedures inzake informatiebeveiliging (zoals het melden van informatiebeveiligingsincidenten) en basisbeheersmaatregelen (zoals wachtwoordbeveiliging, malwarecontroles en opgeruimde bureaus);

e) contactpunten en bronnen voor aanvullende informatie en advies over informatiebeveiligingsaangelegenheden, met inbegrip van aanvullend opleidings- en trainingsmateriaal met betrekking tot informatiebeveiliging.

Opleiding en training voor informatiebeveiliging behoort per oplek plaats te vinden. De basisopleiding en -training geldt voor personen die worden overgeplaatst naar nieuwe functies of rollen met substantieel verschillende eisen ten aanzien van informatiebeveiliging, niet alleen voor nieuwe starters, en behoort plaats te vinden voordat de rol actief wordt.

De organisatie behoort het opleidings- en trainingsprogramma te ontwikkelen ten de opleiding en training doeltreffend uit te kunnen voeren. Het programma behoort in overeenstemming te zijn met de beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de informatie van de organisatie die moet worden beschermd en de beleidsmaatregelen die zijn geïmplementeerd om de informatie te beschermen. Het programma behoort verschillende vormen van opleiding en training te bevatten, bijv. lezingen of zelfstudie.

C.4.2.3 Disciplinaire procedure

Beheersmaatregel

Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging. (ISO 7.2.3)

Implementatierichtlijn

De disciplinaire procedure behoort niet te worden gestart voordat is geverifieerd dat een inbreuk op de informatiebeveiliging heeft plaatsgevonden (zie ISO 16.1.7).

De formele disciplinaire procedure behoort te waarborgen dat medewerkers die worden verdacht van een inbreuk op de informatiebeveiliging correct en eerlijk worden behandeld. De formele disciplinaire procedure behoort te voorzien in een gegradueerd antwoord dat rekening houdt met factoren zoals de aard en ernst van de inbreuk en de impact ervan op de bedrijfsvoering, of dit een eerste of herhaalde overtreding is, of de overtreder al dan niet juist getraind was, relevante wetgeving, zakelijke contracten en, indien vereist, andere factoren.

De disciplinaire procedure behoort ook te worden gebruikt als een afschrikmiddel om te voorkomen dat medewerkers de beleidsregels en procedures met betrekking tot informatiebeveiliging overtreden en om eventuele andere inbreuken op de informatiebeveiliging te voorkomen. Bij opzettelijke inbreuken kan onmiddellijke actie vereist zijn.

C.4.3. Beëindiging en wijziging van dienstverband

Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband. (ISO 7.3)

C.4.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband

Beheersmaatregel

Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht. (ISO 7.3.1)

Implementatierichtlijn

Tot het communiceren van verantwoordelijkheden na beëindiging van het dienstverband behoren voortdurende eisen en wettelijke verantwoordelijkheden met betrekking tot informatiebeveiliging en, waar van toepassing, verantwoordelijkheden die zijn opgenomen in vertrouwelijkheidsovereenkomsten (zie ISO 13.2.4) en de arbeidsvoorwaarden (zie ISO 7.1.2) die gedurende een gedefinieerde periode na beëindiging van het dienstverband van de medewerker of contractant van kracht blijven.

Verantwoordelijkheden en plichten die van kracht blijven na beëindiging van het dienstverband behoren te worden opgenomen in de arbeidsvoorwaarden van de medewerker of contractant (zie ISO 7.1.2).

Wijzigingen in verantwoordelijkheid of dienstverband behoren te worden gemanaged 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.

C.4.4. Kritische en risicovolle functies

Beheersmaatregel

Er is een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van werknemers en ingehuurd personeel te kunnen beschikken, die kritische bedrijfsactiviteiten uitoefenen en aanvullende maatregelen te treffen voor risicovolle functies.

Toelichting

Bij kritische en risicovolle functies gaat het er om te borgen dat er geen oneigenlijk of frauduleus gebruik van de bevoegdheden wordt gemaakt en tevens dat de bedrijfscontinuïteit gehandhaafd blijft.

Implementatierichtlijn

a) Er is vastgesteld wat kritische en risicovolle functies zijn.

b) Aan medewerkers is kenbaar gemaakt dat zij een kritische en/of risicovolle functie vervullen.

c) Er is een strategie vastgesteld om blijvend over voldoende vaardige en kundige werknemers en ingehuurd personeel te kunnen beschikken voor zover het kritische functies betreft. Deze strategie is gebaseerd op een analyse van de volgende uitgangspunten/overwegingen:

1. documentatie van de wijze waarop kritische bedrijfsactiviteiten worden uitgevoerd;
2. vaardigheidstraining en opleiding;
3. scheiding van basiskwaliteiten om het risico te spreiden;
4. mogelijkheden om derde partijen in te schakelen;
5. planning van de opvolging;
6. kennisbehoud en -beheer.

d) Van medewerkers die kritische functies vervullen, worden opleiding, vaardigheden en ervaring geregistreerd.

e) Er is een strategie vastgesteld om oneigenlijk gebruik van risicogevoelige bevoegdheden te voorkomen. Deze strategie is gebaseerd op een analyse van de volgende uitgangspunten en overwegingen:

1. functieroulatie of rotatie van klantenfunctionarissen/contacten;
2. sociale controle, werken in teams;
3. werkoverleg;
4. extra interne controle.

C.5. Fysieke beveiliging en beveiliging van de omgeving

C.5.1. Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen. (ISO 11.1)

C.5.1.1 Fysieke beveiligingszone

Beheersmaatregel

Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten. (ISO 11.1.1)

Implementatierichtlijn

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

a) beveiligingszones behoren te worden gedefinieerd, en de locatie en sterkte van elke zone behoren af te hangen van de beveiligingseisen van de bedrijfsmiddelen die zich binnen de zone bevinden en van de resultaten van een risicobeoordeling;

b) de bekleding van een gebouw of locatie waarin zich informatieverwerkende faciliteiten bevinden, behoort fysiek in orde te zijn (d.w.z. er behoren geen openingen in de begrenzing te zijn en er behoren geen ruimten te zijn waar gemakkelijk kan worden ingebroken); het dak, de muren en vloer van de locatie behoren solide te zijn en alle buitendeuren behoren passend tegen onbevoegde toegang te zijn beschermd met controlemechanismen (bijv. sloten, alarmsystemen, sloten); daarom ook ramen behoren afgesloten te zijn als er niemand aanwezig is, en voor ramen, in het bijzonder die op de begane grond, behoort externe bescherming te worden overwogen;

c) er behoort een bemande receptie of andere voorziening ter controle van de fysieke toegang tot de locatie of het gebouw aanwezig te zijn; toegang tot locaties en gebouwen behoort te worden beperkt tot bevoegd personeel;

d) er behoren, indien van toepassing, fysieke hindernissen te worden aangebracht om onbevoegde fysieke toegang en vervuiling van de omgeving te voorkomen;

e) alle branddeuren in een beveiligde zone behoren te worden voorzien van alarm, te worden gemonitord en getest in overeenstemming met passende regionale, nationale en internationale normen voor vast te stellen; de werking van de deuren behoort, in overeenstemming met de plaatselijke brandcode, fail-veilig te zijn;

f) tegen indringers behoren op alle buitenceuren en toegankelijke ramen passende detectiesystemen in overeenstemming met nationale, regionale of internationale normen te worden geïnstalleerd en regelmatig getest, er behoren ruimten behoren te allen tijde te zijn voorzien van een alarmsysteem, ook andere ruimten, bijv. de computer- of communicatieruimten, behoren te worden bestreken door het alarmsysteem;

g) informatieverwerkende faciliteiten die worden beheerd door de organisatie behoren fysiek te zijn gescheiden van informatieverwerkende faciliteiten die door externe partijen worden beheerd.

C.5.1.2 Fysieke toegangsbeveiliging

Beheersmaatregel

Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. (ISO 11.1.2)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

a) datum en tijdstip van binnenkomst en vertrek van bezoekers behoort te worden geregistreerd, en op alle bezoekers behoort toezicht te worden gehouden (tenzij hun toegang vooraf is goedgekeurd; personen behoort alleen toegang te worden verleend voor specifieke, goedgekeurde doelen, en zij

behoren instructies over de beveiligingseisen van het gebied en de noodprocedures te ontvangen. De identiteit van bezoekers behoort met passende middelen te worden vastgesteld;

b) toegang tot gebieden waar vertrouwelijke informatie wordt verwerkt of opgeslagen behoort te worden beperkt tot bevoegde personen door passende toegangsbeveiligingsmaatregelen te implementeren, bijv. door het implementeren van een dubbel authenticatiemechanisme zoals een toegangskaart en een geheime pincode;

c) van elke toegang behoort een fysiek logboek of een elektronisch auditspoor te worden onderhouden en gemonitord;

d) van alle medewerkers, contractanten en externe partijen behoort te worden verlangd dat zij een bepaalde vorm van zichtbare identificatie dragen en zij behoren onmiddellijk beveiligingspersoneel te informeren als zij bezoekers zonder begeleiding en personen die geen zichtbare identificatie dragen, tegenkomen;

e) personeel van externe partijen die ondersteunende diensten verlenen, behoort alleen indien noodzakelijk beperkte toegang tot beveiligde gebieden of faciliteiten die vertrouwelijke informatie verwerken te worden verleend; deze toegang behoort te worden goedgekeurd en gemonitord;

f) toegangsrechten voor beveiligde gebieden behoren regelmatig te worden beoordeeld, geactualiseerd en indien nodig te worden ingetrokken (zie 9.2.5 en 9.2.6).

C.5.1.3 Kantoren, ruimten en faciliteiten beveiligen

Beheersmaatregel

Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. (ISO 11.1.3)

Implementatierichtlijn

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

a) belangrijke faciliteiten behoren zo te worden gesitueerd dat ze niet voor iedereen toegankelijk zijn;

b) indien van toepassing behoren gebouwen onopvallend te zijn en zo min mogelijk aanwijzingen te geven over het gebruikdoel ervan, zonder duidelijke tekenen, binnen of buiten het gebouw, die op de aanwezigheid van informatieverwerkende activiteiten duiden;

c) faciliteiten behoren zo te zijn geconfigureerd 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) adresboeken en interne telefoongidsen waarin locaties worden aangegeven met faciliteiten die vertrouwelijke informatie verwerken, behoren niet vrij toegankelijk te zijn voor onbevoegden.

C.5.1.4 Beschermen tegen bedreigingen van buitenaf

Beheersmaatregel

Tegen natuurrampen, bewuswillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast. (ISO 11.1.4)

Implementatierichtlijn

Over het vermijden van schade door brand, overstroming, aardbeving, explosie, opstand en andere vormen van natuurrampen of door personen veroorzaakte rampen behoort specialistisch advies te worden ingewonnen.

C.5.1.5 Werken in beveiligde gebieden

Beheersmaatregel

Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast. (ISO 11.1.5)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

a) personeel behoort alleen op grond van 'need-to-know' bekend te zijn met het bestaan van of de activiteiten in een beveiligd gebied.

b) zonder toezicht werken in beveiligde gebieden behoort te worden vermeden, zowel om veiligheidsredenen als om geen gelegenheid te bieden voor kwaadaardige activiteiten;

c) leegstaande beveiligde ruimten behoren fysiek te worden afgesloten en periodiek te worden geïnspecteerd

d) foto-, video-, audio- of andere opnameapparatuur, zoals camera's in mobiele apparatuur, behoort, tenzij goedgekeurd, niet te worden toegelaten.

De afspraken voor het werken in beveiligde zones bevatten beheersmaatregelen voor de medewerkers en voor externe gebruikers die in de beveiligde zone werken en bestaan alle activiteiten die in de beveiligde zone plaatsvinden.

C.5.1.6 Laad- en loslocatie

Beheersmaatregel

Toegangspunten zoals laad- en losplaatsen en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerd, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden. (ISO 11.1.6)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

a) toegang tot een laad- en loslocatie van buiten het gebouw behoort te worden beperkt tot geïdentificeerd en bevoegd personeel;

b) de laad- en loslocatie behoort zo te zijn ontworpen dat goederen kunnen worden geladen en gelost zonder dat de overlander toegang heeft tot anders delen van het gebouw;

c) de buitendeuren van een laad- en loslocatie behoren beveiligd te zijn als de binnendeuren zijn zijn;

d) inkomende materialen behoren te worden gecontroleerd en onderzocht op explosieven, chemicaliën of andere gevaarlijke materialen voordat ze vanaf een laad- en loslocatie worden overgebracht;

e) inkomende materialen behoren bij binnenkomst op de locatie te worden geregistreerd in overeenstemming met de procedures voor bedrijfsmiddelenbeheer (zie hoofdstuk ISO 8);

f) inkomende en uitgaande zendingen behoren, voor zover mogelijk, fysiek te worden gescheiden;

g) inkomende materialen behoren te worden gecontroleerd op mogelijke aanwijzingen voor vervalsing tijdens het transport. Indien vervalsing wordt ontdekt behoort dit direct aan beveiligingspersoneel te worden gemeld.

C.5.2. Apparatuur

Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen. (ISO 11.2)

C.5.2.1 Plaatsing en bescherming van apparatuur

Beheersmaatregel

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind. (ISO 11.2.1)

Implementatierichtlijn

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

a) apparatuur behoort zo te worden geplaatst dat onnodige toegang tot de werkvloer zo veel mogelijk wordt beperkt:

b) informatieverwerkende faciliteiten die gevoelige gegevens behandelen, behoren zorgvuldig te worden gepositioneerd om het risico te verkleinen dat informatie tijdens verwerking door onbevoegde personen wordt ingezien;

c) opslagfaciliteiten behoren te worden beveiligd om onbevoegde toegang te voorkomen;

d) ondersteunende apparatuur behoren te hebben, behoren te worden beveiligd zodat het algemene beschermingsniveau dat vereist is, kan worden verlaagd;

e) beheersmaatregelen behoren te worden aangenomen om het risico van potentiële fysieke bedreigingen en bedreigingen van buitenaf, bijv. diefstal, brand, explosie, rook, wateroverlast (of uitval van watervoorziening), stof, trilling, chemische resultaten, storing in de elektrische voedingsbron, of in communicatievoorzieningen, elektromagnetische straling en vandalisme, zo laag mogelijk te houden;

f) voor eten, drinken en roken in de nabijheid van informatieverwerkende faciliteiten behoren richtlijnen te worden vastgesteld;

g) omgevingsomstandigheden zoals temperatuur en vochtigheid behoren te worden gemonitord en gecontroleerd op omstandigheden die de werking van informatieverwerkende faciliteiten negatief kunnen beïnvloeden;

h) bij alle gebouwen behoort bliksembeveiliging te worden toegepast en op alle inkomende stroom- en communicatieleidingen behoren bliksembeveiligingsfilters te worden geïnstalleerd;

i) voor apparatuur in industriële omgevingen behoort de toepassing van speciale beschermingsmiddelen zoals toetsenbordfolie te worden overwogen;

j) apparatuur die vertrouwelijke informatie verwerkt, behoort te worden beschermd om het risico van wegkijken van informatie door elektromagnetische emanatie zo laag mogelijk te houden.

C.5.2.2 Nutsvoorzieningen

Beheersmaatregel

Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. (ISO 11.2.2)

Implementatierichtlijn

Nutsvoorzieningen (bijv. elektriciteit, telecommunicatie, watervoorziening, gas, riolering, ventilatie en airconditioning) behoren:

a) in overeenstemming te zijn met de technische specificaties van de fabrikant en de lokale wettelijke eisen;

b) regelmatig te worden onderzocht om te beoordelen of hun capaciteit toereikend is voor de groei van het bedrijf en de interactie met andere nutsvoorzieningen;

c) regelmatig te worden geïnspecteerd en getest om te waarborgen dat ze correct functioneren;

d) zo nodig, te worden voorzien van een alarmsysteem om disfunctionaliteiten op te sporen;

e) voor zover nodig, te beschikken over meervoudige voeding met een verschillende fysieke route.

Noodverlichting en communicatiemiddelen behoren aanwezig te zijn. Nabij noodtrappen of ruimten waar apparatuur aanwezig is, behoren noodschakelaars en knoppen te zijn waarmee stroom, water, gas of andere voorzieningen kunnen worden uitgeschakeld.

C.5.2.3 Beveiliging van bekabeling

Beheersmaatregel

Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade. (ISO 11.2.3)

Implementatierichtlijn

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

a) voedings- en telecommunicatieleidingen naar informatieverwerkende faciliteiten behoren, zo mogelijk, ondergronds te lopen, of er behoort adequate alternatieve bescherming te zijn.

b) voedingskabels behoren gescheiden te zijn van communicatiekabels om interferentie te voorkomen;

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

1) het installeren van gewapende kabelgoten en afgesloten kamers of dozen bij inspectie- en afsluitpunten;

2) het gebruik van elektromagnetische afscherming ter bescherming van de kabels;

3) het initiëren van technische schoonmaakbeurten en fysieke controles op aansluiting van niet-geautoriseerde apparaten op de kabels;

4) bevoegde toegang tot schakelpanelen en kabelruimten.

C.5.2.4 Onderhoud van apparatuur

Beheersmaatregel

Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. (ISO 1".2.4)

Implementatierichtlijn

Met de volgende richtlijnen voor onderhoud van apparatuur behoort rekening te worden gehouden:

a) apparatuur behoort te worden onderhouden in overeenstemming met de door de leverancier aanbevolen intervallen voor servicebeurten en voorschriften;

b) alleen bevoegd onderhoudspersoneel behoort reparaties en onderhoudsbeurten aan apparatuur uit te voeren;

c) er behoren registraties te worden bijgehouden van alle vermeende en daadwerkelijke fouten, en van al het preventieve en corrective onderhoud;

d) als apparatuur is ingepand voor onderhoud behoren passende maatregelen te worden geïmplementeerd, waarbij in aanmerking wordt genomen of dit onderhoud wordt uitgevoerd door personeel op locatie of buiten de organisatie; voor zover nodig behoort vertrouwelijke informatie uit de apparatuur te worden verwijderd of het onderhoudspersoneel behoort voldoende betrouwbaar te worden verklaard;

e) er behoort te worden voldaan aan alle onderhoudseisen die door verzekeringspolissen zijn opgelegd;

f) voordat apparatuur na onderhoud weer in bedrijf wordt gesteld, behoort een inspectie plaats te vinden om te waarborgen dat er niet is geknoeid met de apparatuur en dat deze niet slecht functioneert.

C.5.2.5 Verwijdering van bedrijfsmiddelen

Beheersmaatregel

Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring. (SC 11.2.5)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

a) medewerkers en gebruikers van (externe) partijen[1] die bevoegd zijn om toe te staan dat bedrijfsmiddelen van de locatie worden meegenomen behoren te worden geïdentificeerd;

b) aan de afwezigheid van bedrijfsmiddelen behoren tijdsgrenzen te worden gesteld en er behoort te worden geverifieerd of ze worden teruggebracht;

c) voor zover nodig en gepast behoort het meenemen en de terugkeer van bedrijfsmiddelen te worden

geregistreerd;

d) de identiteit, rol en connectie van iedereen die bedrijfsmiddelen hanteert of gebruikt, behoort te worden gedocumenteerd en deze documenten behoren samen met de apparatuur, informatie of software te worden geretourneerd.

C.5.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Beheersmaatregel

Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie. (ISO 11.2.6)

Implementatierichtlijn

Het buiten het terrein van de organisatie gebruiken van apparatuur waarop informatie is opgeslagen en die informatie verwerkt, behoort door de directie te worden goedgekeurd. Dit geldt voor apparatuur die eigendom is van de organisatie en voor apparatuur die persoonlijk eigendom is en ten behoeve van de organisatie wordt gebruikt.

De volgende richtlijnen behoren in overweging te worden genomen voor het beschermen van apparatuur buiten het terrein van de organisatie:

a) apparatuur en media die buiten het terrein worden gebracht behoren niet onbeheerd te worden achtergelaten in openbare ruimten;

b) voorschriften van de fabrikant voor het beschermen van de apparatuur behoren te allen tijde in acht te worden genomen, bijv. bescherming tegen blootstelling aan sterke elektromagnetische velden;

c) beheersmaatregelen voor locaties buiten het terrein, zoals locaties voor thuiswerken, telewerken en tijdelijke locaties, behoren op basis van een risicobeoordeling te worden vastgesteld, en passende beheersmaatregelen behoren voor zover relevant te worden toegepast, bijv. afsluitbare archiefkasten, 'clear desk'-beleid, toegangsbeveiligingsmaatregelen voor computers en beveiligde communicatie met het kantoor;

d) als apparatuur buiten het terrein tussen verschillende personen of externe partijen wordt overgedragen, behoort een overzicht te worden bijgehouden dat de bewakingsketen voor de apparatuur definieert, met daarin opgenomen ten minste de namen en organisaties die voor de apparatuur verantwoordelijk zijn.

Risico's, bijv. op schade, diefstal of afluisteren, kunnen sterk tussen locaties variëren, en behoren bij het vaststellen van de meest geschikte beheersmaatregelen in overweging te worden genomen.

[1] Zoals het Rijksvastgoedbedrijf

1100034 00012

C.5.2.7 Veilig verwijderen of hergebruiken van apparatuur

Beheersmaatregel

Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven. (ISO 11.2.7)

Implementatierichtlijn

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 of te worden geformatteerd, fysiek te worden vernietigd of de informatie behoort te worden vernietigd, vernield of overschreven met gebruikmaking van technieken die het onmogelijk maken de gecompromitteerde informatie terug te halen.

C.5.2.8 Onbeheerde gebruikersapparatuur

Beheersmaatregel

Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is. (ISO 11.2.8)

Implementatierichtlijn

Alle gebruikers behoren op de hoogte te worden gebracht van de beveiligingseisen en de procedures voor het beschermen van onbeheerde apparatuur, en van hun verantwoordelijkheden voor het implementeren van die bescherming. Gebruikers behoren te worden geïnformeerd dat zij:

a) actieve sessies na beëindiging afsluiten, tenzij de sessies kunnen worden beveiligd door een geschikte vergrendeling, bijv. een schermbeveiliging die door een wachtwoord wordt beschermd;

b) uitloggen uit toepassingen of netwerkdiensten die niet langer nodig zijn;

c) computers of mobiele apparatuur beveiligen tegen onbevoegd gebruik door middel van toetsvergrendeling of een vergelijkbaar middel, bijv. toegang via wachtwoord, als de apparatuur niet in gebruik is.

C.6. Beheer van bedrijfsmiddelen

C.6.1. Inventariseren van bedrijfsmiddelen

Beheersmaatregel

Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden. (ISO 8.1.1)

Implementatierichtlijn

Een organisatie behoort bedrijfsmiddelen die relevant zijn in de levenscyclus van informatie te identificeren en hun belang te documenteren. De levenscyclus van informatie behoort aanmaak, verwerking, opslag, overdracht, vernietiging en vernietiging te omvatten. Documentatie behoort te worden onderhouden in speciale of bestaande inventarislijsten indien van toepassing.

De inventarislijst van de bedrijfsmiddelen behoort nauwkeurig, actueel, consistent en in overeenstemming met andere inventarisoverzichten te zijn.

Voor alle van de geïdentificeerde bedrijfsmiddelen behoort het eigenaarschap te worden toegekend (zie C.6.2) en de classificatie te worden geïdentificeerd (zie ISO 8.2).

C.6.2. Eigendom van bedrijfsmiddelen

Beheersmaatregel

Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben (ISO 8.1.2)

Implementatierichtlijn

Personen evenals andere entiteiten die een actie de directie goedgekeurde verantwoordelijkheid hebben voor de levenscyclus van een bedrijfsmiddel, komen in aanmerking om te worden benoemd als eigenaar van een bedrijfsmiddel.

Gewoonlijk wordt een procedure 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. De eigenaar van het bedrijfsmiddel behoort verantwoordelijk te zijn voor het juiste beheer ervan voor de gehele levenscyclus van het bedrijfsmiddel.

De eigenaar van het bedrijfsmiddel behoort:

a) ervoor te zorgen dat bedrijfsmiddelen worden geïnventariseerd;

b) ervoor te zorgen dat bedrijfsmiddelen passend worden geclassificeerd en beschermd;

c) toegangsbeperkingen en classificatie van belangrijke bedrijfsmiddelen te definiëren en periodiek te beoordelen, rekening houdend met de van toepassing zijnde beleidsregels voor toegangsbeveiliging;

d) te zorgen voor een juiste gang van zaken als het bedrijfsmiddel wordt verwijderd of vernietigd.

C.6.3. Aanvaardbaar gebruik van bedrijfsmiddelen

Beheersmaatregel

Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd. (ISO 8.1.3)

Implementatierichtlijn

Medewerkers en externe gebruikers die bedrijfsmiddelen van de organisatie gebruiken of er toegang toe hebben, behoren bewust te worden gemaakt van de informatiebeveiligingseisen van de bedrijfsmiddelen van de organisatie die samenhangen met informatie en informatieverwerkende

faciliteiten en bronnen. Zij behoren verantwoordelijk te zijn voor hun gebruik van informatievoorzieningen en voor gebruik onder hun verantwoordelijkheid.

C.8.4. Teruggeven van bedrijfsmiddelen

Beheersmaatregel

Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven. (ISO 8.1.4)

Implementatierichtlijn

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

Ingeval een medewerker of een gebruiker van een externe partij apparatuur van de organisatie koopt of eigen persoonlijke apparatuur gebruikt, behoren procedures te worden gevolgd om ervoor te zorgen dat alle relevante informatie aan de organisatie wordt overgedragen en nauwkeurig van de apparatuur wordt verwijderd (zie ISO 11.2.7).

Ingeval een medewerker of externe gebruiker beschikt 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 behoort de organisatie controle uit te oefenen op ongeoorloofd kopiëren van relevante informatie (bijv. intellectueel eigendom) door medewerkers en contractanten van wie het dienstverband is opgezegd.

C.7. Leveranciersrelaties

Het begrip *leverancier* heeft niet alleen betrekking op interne leveranciers, maar ook op externe leveranciers, zoals facilitaire diensten of organisatieadviseurs. Daarnaast kan sprake zijn van een ketenpartner, die diensten in het primaire proces levert, waarbij overeenkomsten worden gesloten.

Bij het in- of extern uitbesteden van ondersteunende diensten zullen de normen van dit handboek behorend bij die diensten gehandhaafd moeten blijven, omdat de eigen verantwoordelijkheid niet anders wordt. Indien de eigen bedrijfsprocessen afhankelijk zijn van externe bedrijfsprocessen geldt in principe hetzelfde, d.w.z. dat de eigen bedrijfsvoering afhankelijk wordt van de betrouwbaarheid van derden.

C.7.1. Informatiebeveiliging in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers. (ISO 15.1)

C.7.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties

Beheersmaatregel

Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd. (ISO 15.1.1)

Implementatierichtlijn

De organisatie behoort beheersmaatregelen voor informatiebeveiliging vast te stellen en verplicht te stellen om specifiek de toegang van de leverancier tot de informatie van de organisatie beleidsmatig aan te pakken. Deze beheersmaatregelen behoren betrekking te hebben op de door de organisatie te implementeren processen en procedures, en op de processen en procedures waarvan de organisatie behoort te eisen dat de leverancier deze implementeert, met inbegrip van:

a) vaststellen en documenteren van de soorten leveranciers, bijv. IT-diensten, logistieke voorzieningen, financiële diensten, IT-infrastructuurcomponenten waarvan de organisatie de toegang tot de informatie wil toestaan;

b) een gestandaardiseerd proces en gestandaardiseerde levenscyclus voor het beheren van leveranciersrelaties;

c) definiëren van de soorten informatietoegang die verschillende soorten leveranciers wordt toegestaan, en de toegang monitoren en controleren;

c) een minimum aan informatiebeveiligingseisen voor elk soort informatie en elk soort toegang dat client als basis voor individuele leverancierscovereenkomsten, gebaseerd op de bedrijfsbehoeften en -eisen van de organisatie en haar risicoprofiel;

e) processen en procedures voor het monitoren van de naleving van vastgestelde informatiebeveiligingseisen voor elk soort leverancier en elk soort toegang, met inbegrip van beoordeling van derden en productvalidatie;

f) beheersmaatregelen betreffende nauwkeurigheid en volledigheid ter waarborging van de integriteit van de informatie of informatieverwerking die één partij biedt;

g) soorten verplichtingen die van toepassing zijn op leveranciers om de informatie van de organisatie te beschermen;

h) omgaan met incidenten en noodsituaties die verband houden met toegang voor leveranciers met inbegrip van verantwoordelijkheden van zowel de organisatie als van de leveranciers.

i) regelingen voor flexibiliteit als, ze nodig voor herstel en noodsituaties om de beschikbaarheid te waarborgen van de informatie of de informatieverwerking die door elk van de partijen wordt gebruikt;

j) bewustzijnstraining voor het personeel van de organisatie dat betrokken is bij acquisitie met betrekking tot toepasselijke beleidsregels, processen en procedures;

k) bewustzijnstraining voor het personeel van de organisatie dat contacten onderhoudt met personeel van de dienstverlener betreffende passende regels van betrokkenheid en gedrag, gebaseerd op het type leverancier en het soort toegang dat de leverancier heeft tot systemen en informatie van de organisatie;

l) voorwaarden waarop informatiebeveiligingseisen en beheersmaatregelen zullen worden gedocumenteerd in een overeenkomst die door beide partijen wordt ondertekend;

m) beheren van de nodige transities van informatie, informatieverwerkende faciliteiten en al het andere dat moet overgaan, en waarborgen dat informatiebeveiliging tijdens de gehele transitieperiode wordt gehandhaafd.

C.7.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Beheersmaatregel

Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurcomponenten van de organisatie, of deze verwerkt, opslaat, communiceert of biedt. (ISO 15.1.2)

Implementatierichtlijn

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

Overwegen behoort te worden om de volgende voorwaarden in de overeenkomsten op te nemen om te voldoen aan de vastgestelde informatiebeveiligingseisen:

a) omschrijving van de informatie die moet worden verschaft of toegankelijk moet worden en methodes om de informatie te verschaffen of toegankelijk te maken;

b) classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie (zie ISO 8.2); zo nodig ook mapping tussen het eigen schema van de organisatie en het schema van de leverancier;

c) wettelijke en regelgevende eisen, met inbegrip van gegevensbescherming, resultaten van intellectueel eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat aan wordt voldaan;

d) verplichting van elke contractuele partij om een overeengekomen aantal beheersmaatregelen te implementeren, waaronder toegangsbeveiliging, prestatiebeoordeling, monitoren, rapporteren en auditen

e) de regels van aanvaardbaar gebruik van informatie, met inbegrip van onaanvaardbaar gebruik indien noodzakelijk;

f) hetzij een expliciete lijst van leverancierspersoneel dat gesanctioneerde toegang heeft of bevoegd is informatie van de organisatie te ontvangen, hetzij procedures of voorwaarden voor autorisatie en het intrekken van de autorisatie, tot toegang tot of ontvangst van informatie van de organisatie door leveranciers personeel.

g) beleidsregels betreffende informatiebeveiliging die relevant zijn voor het specifieke contract;

h) eisen voor incidentbeheer en -procedures (in het bij zonder notificatie en samenwerking tijdens herstel van het incident);

i) trainings- en bewustzijnseisen voor specifieke procedures en informatiebeveiligingseisen, bijv. voor incidentresponsprocedures, autorisatieprocedures;

j) relevante regelgeving voor personeelswerving, met inbegrip van de beheersmaatregelen die moeten worden gelmplementeerd;

k) relevante overeenkomstpartners, met inbegrip van een contactpersoon voor aangelegenheden betreffende informatiebeveiliging;

l) indien relevant, screeningeisen voor leveranciers personeel, met inbegrip van verantwoordelijkheden voor het uitvoeren van de screening en notificatieprocedures indien de screening niet is voltooid of de resultaten aanleiding gaven tot twijfel of bezorgdheid;

m) het recht om de processen en beheersmaatregelen van de leverancier in verband met de overeenkomst te auditen;

n) procedures voor het oplossen van defecten en conflicten;

o) verplichting van de leverancier om periodiek een onafhankelijk 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;

p) verplichting van de leverancier om te voldoen aan de beveiligingseisen van de organisatie

C.7.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Beheersmaatregel

Overeenkomsten met leveranciers behoren zicht te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie. (ISO 15.1.3)

Implementatierichtlijn

Overwogen behoort te worden de volgende onderwerpen op te nemen in leveranciersovereenkomster betreffende beveiliging van de toeleveringsketen:

a) informatiebeveiligingseisen definiëren die gelden voor acquisitie van producten of diensten op het gebied van informatie- en communicatietechnologie naast de algemene informatiebeveiligingseisen voor leveranciersrelaties;

b) met betrekking tot diensten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers de beveiligingseisen van de organisatie in de gehele toeleveringsketen bekendmaken indien leveranciers delen van diensten op het gebied van informatie- en communicatietechnologie die zij aan de organisatie leveren, uitbesteden;

c) met betrekking tot producten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers passende beveiligingspraktijken in de gehele toeleveringsketen bekendmaken indien deze producten componenten bevatten die van andere leveranciers worden betrokken;

d) een monitorproces en aanvaardbare methoden implementeren om te valideren dat geleverde producten en diensten op het gebied van informatie- en communicatietechnologie in overeenstemming zijn met verklaarde beveiligingseisen;

e) een proces implementeren voor het vaststellen van componenten van producten of diensten die essentieel zijn voor het handhaven van de functionaliteit en daardoor verhoogde aandacht en toezicht vereisen als deze buiten de organisatie worden gebouwd, in het bijzonder indien de eindleverancier delen van componenten van producten of diensten aan andere leveranciers uitbesteedt;

f) zekerheid verkrijgen dat essentiële componenten en de herkomst ervan in de toeleveringsketen kunnen worden nagespeurd;

g) zekerheid verkrijgen dat de geleverde producten op het gebied van informatie- en communicatietechnologie functioneren zoals voorzien zonder onverwachte of ongewenste verschijnselen;

h) regels definiëren voor het delen van informatie met betrekking tot de toeleveringsketen en potentiële kwesties en compromissen tussen de organisatie en leveranciers;

i) specifieke processen implementeren voor het beheren van de levenscyclus en de beschikbaarheid van de componenten van de informatie- en communicatietechnologie en samenhangende beveiligingsrisico's. Hiertoe behoort het beheren van de risico's van componenten die niet langer beschikbaar zijn doordat leveranciers niet meer bestaan of doordat leveranciers deze componenten niet meer leveren in verband met verbeterde technologie.

C.7.2. Beheer van dienstverlening van leveranciers

Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leverancierovereenkomsten handhaven. (ISO 15.2)

C.7.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

Beheersmaatregel

Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. (ISO 15.2.1)

Implementatierichtlijn

Het monitoren en beoordelen van dienstverlening van leveranciers behoort te waarborgen dat aan de voorwaarden van informatiebeveiliging wordt voldaan, en dat incidenten en problemen betreffende informatiebeveiliging op de juiste manier worden behandeld.

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

a) de prestatieniveaus van de dienstverlening te monitoren om naleving van de overeenkomsten te verifiëren;

b) de rapporten over de dienstverlening die zijn opgesteld door de leverancier te beoordelen, en regelmatig voortgangsbesprekingen te regelen voor zover door de overeenkomsten vereist;

c) audits van leveranciers uit te voeren, indien beschikbaar tezamen met de beoordeling van rapporten van onafhankelijke auditoren, en vastgestelde kwesties op te volgen.

d) informatie te verstrekken over informatiebeveiligingsincidenten en deze informatie te beoordelen voor zover vereist door de overeenkomsten en ondersteunende richtlijnen en procedures;

e) auditsporen van leveranciers en verslagen van informatiebeveiligingsgebeurtenissen, operationele problemen, weigeringen, opsporing van storingen, en onderbrekingen in verband met de geleverde dienst te beoordelen;

f) vastgestelde problemen op te lossen en te beheren;

g) informatiebeveiligingsaspecten van de relaties van de leverancier met zijn eigen leveranciers te beoordelen;

h) de 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 hoofdstuk ISO 17).

De verantwoordelijkheid voor het beheer van leveranciersrelaties behoort te worden toegewezen aan een daarvoor aangewezen persoon of dienstverleningsbeheerteam. De organisatie behoort verder ervoor te zorgen dat leveranciers verantwoordelijkheden toewijzen voor het bewerkstelligen van de naleving en het dwingend uitvoeren van de eisen van de overeenkomsten. Om te monitoren dat de eisen van de overeenkomst, in het bijzonder de informatiebeveiligingseisen, worden nageleefd, behoren voldoende technische vaardigheden en middelen beschikbaar te worden gesteld. Als tekortkomingen in de dienstverlening worden waargenomen behoort passende actie te worden ondernomen.

De organisatie behoort voldoende algehele controle over en zicht te houden op alle beveiligingsaspecten betreffende gevoelige of essentiële informatie of informatieverwerkende faciliteiten die toegankelijk zijn voor, worden verwerkt of beheerd door een leverancier. De organisatie behoort van gedefinieerde rapportageprocedure zicht te houden op beveiligingsactiviteiten zoals wijzigingsbeheer, vaststellen van kwetsbaarheden en rapporteren van en respons op informatiebeveiligingsincidenten.

C.7.2.2 Beheer van veranderingen in dienstverlening van leveranciers

Beheersmaatregel

Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's. (ISO 15.2.2)

Implementatierichtlijn

De volgende aspecten behoren in overweging te worden genomen:

a) veranderingen in leverancierscontracten;

b) veranderingen die door de organisatie zijn aangebracht ter implementatie van:

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 organisatie;

4) nieuwe of gewijzigde beheersmaatregelen om informatiebeveiligingsincidenten op te lossen en om de veiligheid te verbeteren.

c) veranderingen in diensten van de leverancier ter implementatie van:

1) veranderingen en verbeteringen van netwerken;

2) gebruik van nieuwe technologieën;

3) aanvaarding van nieuwe producten of nieuwe versies/releases;

4) nieuwe ontwikkelinstrumenten en omgevingen;

5) veranderingen in fysieke locatie van dienstverleningsfaciliteiten;

6) verandering van leverancier,

7) onderaannemer bij een andere leverancier.

C.8. Beveiliging bedrijfsvoering

C.8.1. Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. (ISO 12.1)

C.8.1.1 Gedocumenteerde bedieningsprocedures

Beheersmaatregel

Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. (ISO 12.1.1)

Implementatierichtlijn

Voor bedieningsactiviteiten die samenhangen met informatieverwerkende en communicatiefaciliteiten, zoals de procedures voor het starten en afsluiten van de computer, back-up, onderhoud van apparatuur, behandeling van media, beheer en veiligheid van computerruimte en postverwerking behoren gedocumenteerde procedures te worden opgesteld.

In de bedieningsprocedures behoren de bedieningsvoorschriften te zijn opgenomen, onder andere voor:

a) de installatie en configuratie van systemen;

b) verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig;

c) back-up (zie ISO 12.3);

d) eisen ten aanzien van de planning, met inbegrip van onderlinge verbondenheid met andere systemen, tijdstip waarop de eerste taak begint en tijdstip van afronding van de laatste taak;

e) voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen ten aanzien van het gebruik van systeemhulpmiddelen (zie ISO 9.4.4);

f) ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden;

g) voorschriften voor de behandeling van speciale uitvoer en media, zoals het gebruik van speciale kantoorbenodigdheden of het beheer van vertrouwelijke uitvoer, waaronder procedures voor veilig verwijderen van uitvoer van mislukte taken (zie ISO 8.3 en ISO 11.2.7);

h) procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen;

i) het beheren van audit- en systeemlogbestandinformatie (zie 12.4);

j) procedures voor het monitoren van een activiteit.

Bedieningsprocedures en de gedocumenteerde procedures voor systeemactiviteiten behoren te worden behandeld als formele documenten en wijzigingen behoren door de directie te worden goedgekeurd. Indien technisch haalbaar behoren informatiesystemen consistent te worden beheerd, met gebruikmaking van dezelfde procedures, instrumenten en hulpmiddelen.

C.8.1.2 Wijzigingsbeheer

Beheersmaatregel

Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. (ISO 12.1.2)

Implementatierichtlijn

In het bijzonder met de volgende aspecten behoort rekening te worden gehouden:

a) identificatie en registratie van significante veranderingen;

b) plannen en testen van veranderingen;

c) de potentiële impact van dergelijke veranderingen beoordelen, waaronder de impact van de informatiebeveiliging;

d) formele goedkeuringsprocedure voor voorgestelde veranderingen;

e) verificatie dat is voldaan aan de eisen van informatiebeveiliging;

f) communicatie van veranderingsdetails aan alle betrokken personen;

g) uitwijkprocedures, waaronder procedures en verantwoordelijkheden voor het afbreken en herstellen van niet-geslaagde veranderingen en onvoorziene gebeurtenissen;

h) voorzien in een noodveranderingsproces om veranderingen die nodig zijn om een incident op te lossen snel en beheerst te implementeren (zie ISO 16.1)

Verantwoordelijkheden en procedures voor beheer behoren formeel te worden vastgelegd om afdoende beheersing van alle veranderingen te waarborgen. Als de veranderingen hebben plaatsgevonden behoort een auditlogbestand te worden bewaard.

G.8.1.3 Capaciteitsbeheer

Beheersmaatregel

Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen. (ISO 12.1.3)

Implementatierichtlijn

Capaciteitseisen behoren te worden gedefinieerd, rekening houdend met de bedrijfskritikaliteit van het betrokken systeem. Het systeem behoort te worden afgestemd en gemonitord om de beschikbaarheid en doelmatigheid van systemen te waarborgen en zo nodig te verbeteren. Om problemen vroegtijdig veel 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.

Speciale aandacht behoort te worden gegeven aan middelen met een lange levertijd of hoge kosten; beheerders behoren daarom het gebruik van belangrijke systeemmiddelen te monitoren. Ze bel oren trends in het gebruik te signaleren, vooral in relatie tot bedrijfstoepassingen of beheerinstrumenten voor informatiesystemen.

Beheerders behoren deze informatie te gebruiken voor het signaleren en vermijden van potentiële knelpunten en afhankelijkheid van be angrijk personeel die een bedreiging kunnen vormen voor de systeembeveiliging en dienstbe, en behoren passende actie te plannen.

Voldoende capaciteit kan worden verkregen door de capaciteit te verhogen of door de vraag te verlagen. De capaciteitsbehoefte kan onder meer worden beheerst door:

a) verouderde gegevens te verwijderen (schijfruimte);

b) toepassingen, systemen, databases of omgevingen buiten gebruik te stellen;

c) batchprocessen en -schema's te optimaliseren;

d) toepassingslogica of databasequeries te optimaliseren;

e) de bandbreedte voor diensten die veel energie verbruiken te weigeren of te beperken als deze niet van overwegend bedrijfsbelang zijn (bijv. videostreaming).

Voor systemen die belangrijk zijn voor de missie behoort voor de capaciteit een gedocumenteerd beheersplan te worden overwogen.

C.8.1.4 Scheiding van ontwikkel-, test- en productieomgevingen

Beheersmaatregel

Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. (ISO 12.1.4)

Implementatierichtlijn

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) voor het muteren van software van de ontwikkel- naar de operationele status behoren regels te worden gedefinieerd en gedocumenteerd;

b) ontwikkelsoftware en operationele software behoren op verschillende systemen of computerprocessors te draaien en in verschillende domeinen of directory's;

c) veranderingen aan productiesystemen en toepassingen behoren te worden getest in een test- of gefaseerde omgeving voordat ze in productiesystemen worden toegepast;

d) behoudens uitzonderlijke omstandigheden, behoren tests niet in productiesystemen te worden uitgevoerd (zie ook C.12.3. Testgegevens);

e) compilers, editors en andere ontwikkelinstrumenten of systeemhulpmiddelen behoren, indien ze niet nodig zijn, niet toegankelijk te zijn vanuit productiesystemen;

f) gebruikers behoren voor operationele en testsystemen verschillende gebruikersprofielen te gebruiken, en menu's behoren passende identificatieboodschappen te tonen om het risico op fouten te verlagen;

g) gevoelige gegevens behoren niet in de omgeving van het testsysteem te worden gekopieerd, tenzij voor het testsysteem equivalente beheersmaatregelen zijn getroffen (zie ISO 14.3).

C.8.2. Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.

C.8.2.1 Beheersmaatregelen tegen malware

Beheersmaatregel

Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. (ISO 12.2.1)

Implementatierichtlijn

Bescherming tegen malware behoort te zijn gebaseerd op software die malware opspoort en op herstelsoftware, bewustzijn ten aanzien van informatiebeveiliging en passende beheersmaatregelen met betrekking tot systeemtoegang en wijzigingsbeheer. De volgende richtlijnen behoren in acht te worden genomen:

a) een formeel beleid vaststellen dat het gebruik van ongeautoriseerde software verbiedt (zie ISO 12.6.2 en ISO 14.2);

b) beheersmaatregelen implementeren die het gebruik van ongeautoriseerde software voorkomen of opsporen (bijv. een witte lijst voor toepassingen opstellen);

c) beheersmaatregelen implementeren die het gebruik van bekende of verdachte kwaadaardige websites voorkomen of opsporen (bijv. een zwarte lijst opstellen);

d) een formeel beleid vaststellen ter bescherming tegen risico's die samenhangen met het verkrijgen van bestanden en software, hetzij van het/of via externe netwerken of een ander medium, waarbij wordt aangegeven welke beschermende maatregelen behoren te worden genomen;

e) kwetsbaarheden verminderen die kunnen worden geëxploiteerd door malware, bijv. via beheer van technische kwetsbaarheden (zie ISO 12.6);

f) regelmatig beoordelingen uitvoeren van de software en gegevensinhoud van systemen die kritische bedrijfsprocessen ondersteunen; de aanwezigheid van niet-goedgekeurde bestanden of ongeautoriseerde wijzigingen behoort formeel te worden onderzocht;

g) installeren en regelmatig updaten van software die malware opspoort, en van hersteisoftware, waarbij computers en media als voorzorgsmaatregel of routinematig worden gescand; die uitgevoerde scan behoort te omvatten:

1) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen;

2) bijlagen en downloads vóór gebruik op malware scannen; deze scan behoort op verschillende plaatsen te worden uitgevoerd, bijv. op elektronische mailservers, op desktopcomputers en bij de toegang tot het netwerk van de organisatie;

3) internetpagina's op malware scannen;

h) ter bescherming tegen malware op systemen procedures en verantwoordelijkheden definiëren, het gebruik ervan trainen, aanvallen van malware melden en herstellen;

i) passende bedrijfscontinuiteitsplannen voorbereiden voor het herstel na malwareaanvallen, met inbegrip van de nodige back-up van gegevens en software en herstelprocedures (zie ISO 12.3);

j) procedures implementeren om regelmatig informatie te verzamelen, zoals een abonnement op mailinglijsten of het nagaan van websites die informatie over nieuwe malware geven;

k) procedures implementeren om informatie in verband met malware te verifiëren en waarborgen dat waarschuwingsberichten nauwkeurig en informatief zijn; beheerders behoren ervoor te zorgen dat gekwalificeerde bronnen, bijv. goed aangeschreven staande kranten, betrouwbare internetpagina's of leveranciers van antimalwaresoftware, worden gebruikspleegd om te differentiëren tussen een hoax en echte malware; alle gebruikers behoren te worden geïnformeerd over het probleem van hoaxen en wat te doen na ontvangst van een hoax;

l) omgevingen isoleren als catastrofale impact dreigt.

C.8.3. Maken van back-ups

Doelstelling: Beschermen tegen het verlies van gegevens. (ISO 12.3)

C.8.3.1 Back-up van informatie

Beheersmaatregel

Regelmatig bekeren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest, in overeenstemming met een overeengekomen back-upbeleid. (ISO 12.3.1)

Implementatierichtlijn

Om de eisen van de organisatie voor het back-uppen van informatie, software en systemen te definiëren behoort een back-upbeleid te worden vastgesteld.

Het back-upbeleid behoort de eisen voor het bewaren en beschermen te definiëren.

Er behoort te worden voorzien in adequate back-upfaciliteiten, om te waarborgen dat alle essentiële informatie en software na een calamiteit of na falen van media kan worden hersteld.

Bij het opstellen van een back-upplan, behoren de volgende punten in overweging te worden genomen:

a) er behoren nauwkeurige en volledige registers van de back-upkopieën en gedocumenteerde herstelprocedures aanwezig te zijn;

b) de omvang (bijv. een volledige back-up of alleen van de wijzigingen) en de frequentie van de back-ups behoren in overeenstemming te zijn met de bedrijfseisen van de organisatie, de beveiligingseisen van de betrokken informatie en de kritikaliteit van de informatie voor de voortzetting van de bedrijfsuitvoering van de organisatie;

c) de back-ups behoren in een afgelegen locatie te worden bewaard, op een voldoende afstand om niet te worden beschadigd door een calamiteit op de hoofdlocatie

d) aan back-upinformatie behoort een passend niveau van fysieke en omgevingsbescherming te worden gegeven (zie hoofdstuk 11) consistent met de normen die op de hoofdlocatie worden toegepast;

e) back-upmedia behoren regelmatig te worden getest om te waarborgen dat ze betrouwbaar zijn als ze in noodgevallen nodig zijn; dit behoort te worden gecombineerd met een test van de herstelprocedures en van de tijd die voor herstel nodig is. Of de back-upgegevens kunnen worden hersteld, behoort te worden getest op speciaal daarvoor aangewezen testmedia, niet door de originele media te overschrijven omdat het back-up- of herstelproces kan mislukken en onherstelbare schade aan of verlies van gegevens kan veroorzaken;

f) in gevallen waarin vertrouwelijkheid belangrijk is, behoren back-ups te worden beschermd door ze te coderen.

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 back-upbeleid te waarborgen

Back-upprocedures voor individuele systemen en diensten behoren regelmatig te worden getest om te waarborgen dat ze voldoen aan de eisen van de bedrijfscontinuïteitsplannen. In geval van kritische systemen en diensten behoren back-upprocedures betrekking te hebben op de informatie, toepassingen en gegevens van alle systemen die nodig zijn om het gehele systeem na een calamiteit te herstellen.

Voor belangrijke bedrijfsinformatie behoort de bewaartermijn te worden vastgesteld, rekening houdend met eisen voor archiefkopieën die permanent moeten worden bewaard.

C.8.4. Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen. (ISO 12.4)

C.8.4.1 Gebeurtenissen registreren

Beheersmaatregel

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. (ISO 12.4.1)

Implementatierichtlijn

Logbestanden van gebeurtenissen behoren, voor zover relevant, te bevatten:

a) gebruikersidentificaties;

b) systeemactiviteiten,

c) data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen;

d) identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie;

e) registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem;

f) registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie.

g) systeemconfiguratiewijzigingen;

h) gebruik van speciale bevoegdheden;

i) gebruik van systeemhulpmiddelen en -toepassingen;

j) bestanden die zijn geopend en het type toegang dat is verkregen;

k) netwerkadressen en -protocollen;

l) alarmen die worden afgegeven door het toegangsbeveiligingssysteem;

m) activering en deactivering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen;

n) verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.

C.8.4.2 Beschermen van informatie in logbestanden

Beheersmaatregel

Logvoorzieningen en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. (ISO 12.4.2)

Implementatierichtlijn

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) overschrijden van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen worden vastgelegd of eerder vastgelegde gebeurtenissen worden overschreven.

Als onderdeel van het beleid voor het bewaren van verslagen of in verband met eisen om bewijsmateriaal te verzamelen en te bewaren kan het nodig zijn om bepaalde auditlogbestanden te archiveren (zie ISO 15.1.3).

C.8.4.3 Logbestanden van beheerders en operators

Beheersmaatregel

Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld. (ISO 12.4.3)

Implementatierichtlijn

Houders van een bevoegd account zijn mogelijk in staat om de logbestanden op informatieverwerkende faciliteiten die onder hun directe beheer staan te manipuleren. Daarom is het nodig de logbestanden te beschermen en te beoordelen om te handhaven dat speciale gebruikers rekenschap afleggen

C.8.4.4 Kloksynchronisatie

Beheersmaatregel

De klokken van alle te overige informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron. (ISO 12.4.4)

Implementatierichtlijn

Externe en interne eisen voor weergave, synchronisatie en nauwkeurigheid van tijd behoren te worden gedocumenteerd. Dergelijke eisen kunnen wettelijke, regelgevende of contractuele eisen zijn, naleving van normen of eisen voor interne monitoring. Er behoort een standaard referentietijd voor gebruik binnen de organisatie te worden gedefinieerd.

De aanpak van de organisatie om een referentietijd op basis van externe bron(nen) te verkrijgen en hoe interne klokken betrouwbaar te synchroniseren behoort te worden gedocumenteerd en geïmplementeerd.

C.3.5. Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen. [ISO 12.5]

C.5.5.1 Software installeren op operationele systemen

Beheersmaatregel

Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd. (ISO 12.5.1)

Implementatierichtlijn

De volgende richtlijnen behoren in overweging te worden genomen om de installatie van software op operationele systemen te beheersen:

a) het updaten van de productiesoftware, -toepassingen en -programmabibliotheken behoort alleen te worden uitgevoerd door gekwalificeerde beheerders en na de juiste goedkeuring van de directie (zie ISO 6.1.6);

b) productiesystemen behoren alleen goedgekeurde uitvoerbare codes te bevatten en geen ontwikkelcodes of compilers;

c) toepassingen en bestuursgsysteemsoftware behoren pas te worden geïmplementeerd na uitgebreide en succesvolle tests; de tests behoren betrekking te hebben op bruikbaarheid, beveiliging, effecten op andere systemen en gebruiksvriendelijkheid, en behoren te worden uitgevoerd op geschikten systemen (zie ISO 12.1.4); gewaarborgd behoort te worden dat alle corresponderende broncodebibliotheken zijn geüpdatet;

d) om alle geïnstalleerde software en systeemdocumentatie te beheersen behoort een configuratiebeheersysteem te worden toegepast;

e) voordat veranderingen worden doorgevoerd behoort een strategie voor het terugdraaien van de veranderingen te zijn vastgesteld;

f) van alle updates van bedrijfsgegevensbestanden behoort een auditlogboekend te worden bijgehouden

g) oudere versies van toepassingssoftware behoren te worden bewaard voor noodgevallen;

h) oude versies van software behoren te worden gearchiveerd samen met alle vere ste informatie en parameters, procedures, configuratiedetails en ondersteunende software, zolang er gegevens in het archief worden bewaard.

Software van leveranciers die in productiesystemen wordt gebruikt behoort te worden ondersteund 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.

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, d.w.z. de introductie van nieuwe informatiebeveiligingsfunctionaliteit of het aantal en de ernst van informatiebeveiligingsproblemen die zich bij deze versie voordoen. Softwarepatches behoren te

worden toegepast als ze kunnen bijdragen aan het verwijderen of verminderen van zwakke plekken in de informatiebeveiliging (zie ISO 12.6).

Fysieke of logische toegang behoort alleen te worden verleend aan leveranciers wanneer dit noodzakelijk is voor ondersteuningsdoeleinden en met toestemming van de directie. De activiteiten van de leverancier behoren te worden gemonitord (zie ISO 15.2.1).

Computersoftware kan soms steunen op extern geleverde software en modules, die behoren te worden gemonitord en beheerst om onbevoegde veranderingen te vermijden, die zwakke plekken in de beveiliging kunnen introduceren.

C.8.6. Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen. (ISO 12.6)

C.8.6.1 Beheer van technische kwetsbaarheden

Beheersmaatregel

Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. (ISO 12.6.1)

Implementatierichtlijn

Een actuele en volledige inventaris van bedrijfsmiddelen (zie hoofdstuk ISO 8) is een voorwaarde voor een doeltreffend beheer van technische kwetsbaarheden. Tot de specifieke informatie die nodig is om beheer van technische kwetsbaarheden te ondersteunen behoren informatie over de softwareleverancier, versienummers, huidige toepassingsstatus (bijv. welke software is geïnstalleerd op welke systemen) en de persoon of personen in de organisatie verantwoordelijk voor de software.

Als reactie op de identificatie van potentiële technische kwetsbaarheden behoort passende en tijdige actie te worden ondernomen. Om een doeltreffend beheerproces voor technische kwetsbaarheden vast te stellen behoren de volgende richtlijnen te worden gevolgd:

a) de organisatie behoort de rollen en verantwoordelijkheden in samenhang met het beheer van technische kwetsbaarheden te definiëren en vast te stellen, met inbegrip van het monitoren van de kwetsbaarheden, een risicobeoordeling van de kwetsbaarheden, het installeren van herstelprogramma's (patching), het traceren van bedrijfsmiddelen en de vereiste coördinatieverantwoordelijkheden;

b) informatiemiddelen die worden gebruikt om relevante technische kwetsbaarheden te bepalen en om het bewustzijn hierover levend te houden, behoren te worden vastgesteld voor software en andere technologie (op basis van de inventarislijst van bedrijfsmiddelen, zie ISO 8.1.1); deze informatiemiddelen behoren te worden geactualiseerd op basis van veranderingen in de inventarislijst of als andere nieuwe of nuttige middelen zijn gevonden;

c) een tijdpad behoort te worden gedefinieerd waarbinnen moet worden gereageerd op aankondigingen van potentieel relevante technische kwetsbaarheden;

d) als een potentieel technische kwetsbaarheid is geïdentificeerd, behoort de organisatie de samenhangende risico's en de te ondernemen acties vast te stellen; een dergelijke actie kan patching van kwetsbare systemen inhouden, of het toepassen van andere beheersmaatregelen.

e) afhankelijk van hoe urgent een technische kwetsbaarheid moet worden aangepakt behoort de te ondernemen actie te worden uitgevoerd in overeenstemming met de beheersmaatregelen in verband met wijzigingsbeheer (zie ISO 12.1.2) of door responsprocedures voor informatiebeveiligingsincidenten te volgen (zie ISO 16.1.5);

f) indien een patch uit een legitieme bron beschikbaar is, behoren de risico's die verbonden zijn aan het installeren van de patch te worden beoordeeld (de risico's die worden gevormd door de kwetsbaarheid behoren te worden vergeleken met het risico van het installeren van de patch);

g) patches behoren te worden getest en geëvalueerd voordat ze worden geïnstalleerd om te waarborgen dat ze doeltreffend zijn en niet resulteren in bijverschijnselen die niet kunnen worden getolereerd; indien geen patch beschikbaar is, behoren andere beheersmaatregelen te worden overwogen, zoals:

1) diensten of capaciteiten in verband met de kwetsbaarheid uitschakelen;

2) toegangsbeveiligingsmaatregelen aanpassen of toevoegen, bijv. firewalls, rond de grenzen van netwerken (zie ISO 13.1);

3) vaker monitoren om werkelijke aanvallen op te sporen;

4) bewustzijn vergroten over de kwetsbaarheid (weer);

h) over alle procedures behoort een auditlogbestand te worden bijgehouden;

i) het beheerproces met betrekking tot de technische kwetsbaarheid behoort regelmatig te worden gemonitord en geëvalueerd om de doeltreffendheid en doelmatigheid ervan te waarborgen;

j) systemen met een hoog risico behoren eerst te worden aangepakt;

k) om gegevens over kwetsbaarheden te communiceren aan de functie die moet reageren op het incident en om te voorzien in uit te voeren technische procedures in geval van een incident, behoort een doeltreffend beheerproces met betrekking tot de technische kwetsbaarheid te worden afgestemd op incidentbeheeractiviteiten;

l) een procedure definiëren om de stappen aan te pakken waar een kwetsbaarheid is geïdentificeerd maar waar geen passende tegenmaatregel voorhanden is. In deze situatie behoort de organisatie risico's in verband met de bekende kwetsbaarheid te evalueren en passende opsporings- en corrigerende maatregelen te definiëren.

C.8.8.2 Beperkingen voor het installeren van software

Beheersmaatregel

Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd. (ISO 12.6.2)

Implementatierichtlijn

De organisatie behoort een strikt beleid te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers mogen installeren.

Het principe van 'minimale voorrech' behoort te worden toegepast. Indien aan gebruikers bepaalde voorrechten worden verleend, kunnen zij over de mogelijkheid beschikken om software te installeren. 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 met oog voor de rollen van de betrokken gebruikers.

C.8.7. Beheer van netwerkbeveiliging

Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen. (ISO 13.1)

C.8.7.1 Beheersmaatregelen voor netwerken

Beheersmaatregel

Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. (ISO 13.1.1)

Implementatierichtlijn

Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en aangesloten diensten tegen onbevoegde toegang te beschermen. Met de volgende aspecten behoort in het bijzonder rekening te worden gehouden:

a) er behoren verantwoordelijkheden en procedures voor het beheer van netwerkapparatuur te worden vastgesteld;

b) operationele verantwoordelijkheid voor netwerken behoort voor zover van toepassing te worden gescheiden van computerbewerkingen (zie ISO 6.1.2);

c) 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 behoren speciale beheersmaatregelen te worden vastgesteld (zie hoofdstuk ISO 10 en ISO 13.2); er kunnen ook speciale beheersmaatregelen vereist zijn om de beschikbaarheid van de netwerkdiensten en aangesloten computers te handhaven;

d) om acties die van invloed kunnen zijn op of relevant zijn voor de informatiebeveiliging te kunnen vastleggen en opsporen behoren passende maatregelen voor registreren en monitoren te worden toegepast;

e) beheeractiviteiten behoren nauwgezet te worden gecoördineerd, zowel om de dienstverlening voor de organisatie te optimaliseren als om te waarborgen dat beheersmaatregelen consistent in de hele informatieverwerkende infrastructuur worden toegepast;

f) systemen in het netwerk behoren te worden geauthentiseerd;

g) er behoort een beperking te gelden voor het aantal systemen dat met het netwerk verbonden is.

C.3.7.2 Beveiliging van netwerkdiensten

Beheersmaatregel

Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten. (ISO 13.1.2)

Implementatierichtlijn

De kundigheid van de aanbieder van de netwerkdienst om de overeengekomen diensten veilig te beheren behoort te worden vastgesteld en regelmatig te worden gemonitord, en het recht om een audit uit te voeren behoort te worden overeengekomen.

De beveiligingsprocedures die nodig zijn voor bepaalde diensten, zoals beveiligingskenmerken, dienstverleningsniveaus en beheerseisen, behoren te worden vastgesteld. De organisatie behoort ervoor te zorgen dat aanbieders van netwerkdiensten deze maatregelen implementeren.

C.3.7.3 Scheiding in netwerken

Beheersmaatregel

Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden. (ISO 13.1.3)

Implementatierichtlijn

Een van de methoden om de beveiliging van grote netwerken te beheren is ze te verdelen in gescheiden netwerkdomeinen. De domeinen kunnen worden gekozen op basis van betrouwbaarheidsniveaus (bijv. openbaar toegankelijk domein, bureaubladdomein, serverdomein), naast organisatieafdelingen (bijv. personeelszaken, financiën, marketing) of een combinatie (bijv. serverdomein verbonden met meerdere afdelingen van de organisatie). De scheiding kan tot stand worden gebracht door hetzij fysiek verschillende netwerken, hetzij verschillende logische netwerken te gebruiken (bijv. virtueel particulier netwerken).

De perimeter van elk domein behoort goed te worden gedefinieerd. Toegang tussen elkaarvolgende zones is toegelaten maar behoort bij de perimeter te worden beheerst door een gateway te gebruiken (bijv. een firewall, een filterende router). De criteria voor het scheiden 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 toegangsbeveiligingsbeleid (zie ISO 9.1.1), de toegangseisen, voor de een classificatie van verwerkte informatie en behoort ook rekening te houden met de relatieve kosten en de gevolgen voor de prestaties van het inbrengen van gatewaytechnologie.

Draadloze netwerken vereisen een speciale behandeling in verband met de slecht gedefinieerde netwerkperimeter. Voor gevoelige omgevingen behoort te worden overwogen om alle draadloze toegang te behandelen als externe verbinding en een deze toegang te scheiden van interne netwerken totdat de toegang een gateway is gepasseerd, in overeenstemming met het netwerkautorisatiebeleid (zie ISO 11.1.1), alvorens toegang tot interne systemen wordt verleend.

De authenticatie, codering en technologie van de netwerktoegangsbeveiliging voor het gebruikers-niveau van draadloze, op internet gebaseerde draadloze netwerken zijn, indien correct geïmplementeerd, mogelijk voldoende voor directe verbinding met het interne netwerk van de organisatie.

C.8.8. Toegang tot netwerken en netwerkdiensten

Beheersmaatregel

Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. (ISO 9.1.2)

Implementatierichtlijn

Een beleid voor het gebruik van netwerken en netwerkdiensten behoort te worden geformuleerd. Dit beleid behoort te omvatten:

a) de netwerken en netwerkdiensten waartoe toegang wordt verleend;

b) autorisatieprocedures om vast te stellen wie toegang krijgt tot welk netwerk en welke netwerkdiensten;

c) beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en -diensten te beschermen;

d) de middelen die worden gebruikt om toegang te krijgen tot netwerken en netwerkdiensten (bijv. VPN of draadloos netwerk);

e) eisen voor gebruikersauthenticatie voor de toegang tot de verschillende netwerkdiensten;

f) monitoren van het gebruik van netwerkdiensten.

Het beleid voor het gebruik van netwerkdiensten behoort aan te sluiten bij het toegangsbeveiligingsbeleid van de organisatie (zie ISO 9.1.1)

C.8.9. Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen. (ISO 9.4)

C.8.9.1 Beperking toegang tot informatie

Beheersmaatregel

Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. (ISO 9.4.1)

Implementatierichtlijn

Toegangsbeperkingen behoren te worden gebaseerd op eisen voor de afzonderlijke bedrijfstoepassingen en in overeenstemming met het beleid dat voor toegangsbeveiliging is gedefinieerd.

De volgende aspecten behoren in aanmerking te worden genomen om de eisen voor toegangsbeperking te ondersteunen.

a) menu's verschaffen om de toegang tot systeemfuncties van toepassingen te beheersen;

b) beheersen welke gegevens voor een bepaalde gebruiker toegankelijk zijn;

c) toegangsrechten van gebruikers beheersen, bijv. lezen, schrijven, verwijderen en uitvoeren;

d) toegangsrechten voor andere toepassingen beheersen;

e) de informatie in output beperken;

f) zorgen voor fysieke of logische toegangsbeveiligingsmaatregelen voor het isoleren van gevoelige toepassingen, toepassingsgegevens of systemen.

C.8.9.2 Beveiligde inlogprocedures

Beheersmaatregel

Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure (ISO 9.4.2).

Implementatierichtlijn

Om de geclaimde identiteit van een gebruiker te bewijzen behoort een passende authenticatietechniek te worden gekozen.

Ingeval krachtige verificatie en authenticatie van de identiteit is vereist behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals cryptografische middelen, digitale kaarten, tokens of biometrische middelen.

De procedure om in een systeem in te loggen behoort zo te worden ontworpen dat de kans op onbevoegde toegang zo klein mogelijk wordt gemaakt. Om te voorkomen dat het een onbevoegde gebruiker gemakkelijk wordt gemaakt te bepalt de inlogprocedure zo min mogelijk informatie over het systeem of de toepassing openbaar te maken. Een goede inlogprocedure behoort:

a) geen systeem- of toepassingsidentificatoren te tonen voordat het inlogproces met succes is afgerond;

b) een algemene waarschuwing te tonen dat de computer alleen toegankelijk is voor bevoegde gebruikers;

c) tijdens de inlogprocedure geen hulpboodschappen weer te geven waarmee onbevoegde gebruikers hun doel kunnen bereiken;

d) de inloginformatie pas na invoer van alle gegevens te valideren. Indien zich een fout voordoet, behoort het systeem niet aan te geven welk deel van de gegevens juist of onjuist is;

e) bescherming te bieden tegen inlogpogingen die met brute middelen worden uitgevoerd;

f) niet-succesvolle en succesvolle pogingen te registreren;

g) een informatiebeveiligingsgebeurtenis te initiëren als een poging tot of een succesvolle schending van de inlogbeheersmaatregelen is vastgesteld;

h) de volgende informatie te tonen 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 dat wordt ingevoerd niet weer te geven;

j) geen ongecodeerde wachtwoorden via een netwerk te versturen;

k) inactieve sessies na een bepaalde tijd van inactiviteit te beëindigen, vooral op locaties met een hoog risico, zoals openbare of externe locaties die buiten het beveiligingsbeheer van de organisatie vallen, of op mobiele apparaten;

l) de verbindingstijd te beperken om extra beveiliging te bieden voor toepassingen met een hoog risico en de mogelijkheden voor onbevoegde toegang te verkleinen.

C.8.9.3 Systeem voor wachtwoordbeheer

Beheersmaatregel

Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. (ISO 9.4.3)

Implementatierichtlijn

Een systeem voor wachtwoordbeheer behoort:

a) het gebruik van individuele gebruikersidentificaties en wachtwoorden af te dwingen om de toerekenbaarheid te handhaven;

b) gebruikers de mogelijkheid te bieden hun eigen wachtwoord te kiezen en te wijzigen, en een bevestigingsprocedure te bevatten die rekening houdt met foutieve invoer;

c) de keuze voor sterke wachtwoorden af te dwingen;

d) gebruikers te dwingen hun wachtwoord bij het eerste inloggen te wijzigen;

e) wijziging van het wachtwoord periodiek en telkens wanneer dat nodig is af te dwingen;

f) een registratie van eerder gebruikte wachtwoorden bij te houden en te voorkomen dat deze opnieuw worden gebruikt;

g) wachtwoorden niet op het scherm te tonen als ze worden ingevoerd;

h) wachtwoordbestanden apart van systeemgegevens van toepassingen op te slaan;

C.8.9.4 Speciale systeemhulpmiddelen gebruiken

Beheersmaatregel

Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. (ISO 9.4.4)

Implementatierichtlijn

Voor het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoren de volgende richtlijnen te worden overwogen:

a) gebruik van identificatie-, authenticatie- en autorisatieprocedures voor systeemhulpmiddelen;

b) scheiding van systeemhulpmiddelen en toepassingssoftware;

c) beperking van het gebruik van systeemhulpmiddelen tot het laagste aantal betrouwbare bevoegde gebruikers dat praktisch haalbaar is (zie ISO 9.2.3);

d) autorisatie voor ad-hocgebruik van systeemhulpmiddelen;

e) beperking van de beschikbaarheid van systeemhulpmiddelen, bijv. voor de duur van een geautoriseerde wijziging;

f) registreren van alle gebruik van systeemhulpmiddelen;

g) definiëren en documenteren van autorisatieniveaus voor systeemhulpmiddelen;

h) verwijderen of onbruikbaar maken van alle onnodige systeemhulpmiddelen

i) niet beschikbaar stellen van systeemhulpmiddelen aan gebruikers die toegang hebben tot toepassingen op systemen waarbij scheiding van taken vereist is.

C.9.9.5 Toegangsbeveiliging op programmabroncode

Beheersmaatregel

Toegang tot de programmabroncode behoort te worden beperkt. (ISO 9.4.5)

Implementatierichtlijn

Toegang tot programmabroncodes en samenhangende items (zoals ontwerpen, specificaties, verificatie- en validatieschema's) behoort strikt te worden beheerst om de introductie van onbevoegde functionaliteit te en om onbedoelde wijzigingen te voorkomen, alsmede om de vertrouwelijkheid van waardevolle intellectueel eigendom te handhaven. Met betrekking tot de programmabroncode kan dit worden bereikt door de code gecontroleerd centraal op te slaan, bij voorkeur in de broncodebibliotheek. De volgende richtlijnen behoren dan te worden overwogen om de toegang tot dergelijke broncodebibliotheken te beheersen en zo de kans op corruptie van computerprogramma's te verkleinen.

a) waar mogelijk, behoren broncodebibliotheken niet in operationele systemen te worden opgeslagen;

b) de programmabroncode en de broncodebibliotheek behoren te worden beheerd in overeenstemming met vastgestelde procedures;

c) ondersteunend personeel behoort geen onbeperkte toegang tot broncodebibliotheken te hebben;

d) het updaten van broncodebibliotheken en samenhangende items en het verstrekken van broncodes aan programmeurs behoort alleen plaats te vinden na ontvangst van een passende autorisatie;

e) programma-listbladen behoren in een beveiligde omgeving te worden bewaard;

f) van elke toegang tot broncodebibliotheken behoort een auditlogbestand te worden bijgehouden;

g) onderhouden en kopieren van broncodebibliotheken behoren aan strikte procedures voor wijzigingsbeheer te worden onderworpen (zie ISO 14.2.2).

Indien het de bedoeling is dat de programmabroncode wordt gepubliceerd behoren aanvullende beheersmaatregelen die bijdragen aan het waarborgen van de integriteit ervan (bijv. een digitale handtekening) in werking overwogen.

C.9. Beheer van informatiebeveiligingsincidenten

C.9.1. Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. (ISO 16.1)

C.9.1.1 Verantwoordelijkheden en procedures

Beheersmaatregel

Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. (ISO 16.1.1)

Implementatierichtlijn

Met betrekking tot het beheer van informatiebeveiligingsincidenten behoren de volgende richtlijnen voor directieverantwoordelijkheden en -procedures in overweging te worden genomen:

a) er behoren directieverantwoordelijkheden te worden vastgesteld om te bewerkstelligen dat de volgende procedures adequaat binnen de organisatie worden ontwikkeld en gecommuniceerd:

1) procedures voor incidentresponsplanning en -voorbereiding;

2) procedures voor het monitoren, opsporen, analyseren en rapporteren van informatiebeveiligingsgebeurtenissen en -incidenten;

3) procedures voor de verslaglegging van beheeractiviteiten betreffende incidenten;

4) procedures voor het omgaan met forensisch bewijs;

5) procedures voor het beoordelen van en beslutvorming over informatiebeveiligingsgebeurtenissen en beoordeling van zwakke plekken in de informatiebeveiliging;

6) responsprocedures met inbegrip van procedures voor escalatie, beheerst herstel van een incident en communicatie aan in- en extern personeel of organisaties.

b) vastgestelde procedures behoren te bewerkstelligen dat:

1) competent personeel de kwesties behandelt die verband houden met informatiebeveiligingsincidenten binnen de organisatie;

2) een contactpunt voor het opsporen en rapporteren van beveiligingsincidenten wordt geïmplementeerd;

3) passende contacten worden onderhouden met instanties, externe belangengroepen of fora die aangelegenheden behandelen die verband houden met informatiebeveiligingsincidenten.

c) rapportageprocedures behoren de volgende aspecten te omvatten:

1) formulieren voorbereiden voor het rapporteren van informatiebeveiligingsgebeurtenissen ter ondersteuning van de rapportageactie en om te bewerkstelligen dat de rapporterende persoon aan alle redelijke acties denkt die in geval van een informatiebeveiligingsgebeurtenis moeten worden verricht;

2) de procedures die in geval van een informatiebeveiligingsgebeurtenis moeten worden uitgevoerd, bijv. onmiddellijk alle details notaren zoals aard van niet-naleving of overtreding, optredende storing, berichten op het scherm, en onmiddellijk rapporteren aan het contactpunt en alleen gecoördineerde acties ondernemen;

3) verwijzing naar een vastgestelde disciplinaire formele procedure voor het omgaan met medewerkers die beveiligingsovertredingen begaan;

4) passende feedbackprocedures om te bewerkstelligen dat de personen die informatiebeveiligingsgebeurtenissen melden, worden geïnformeerd over de resultaten nadat de kwestie is behandeld en afgesloten.

De doelstellingen voor het beheer van informatiebeveiligingsincidenten behoren met de directie 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.

C.9.1.2 Rapportage van informatiebeveiligingsgebeurtenissen

Beheersmaatregel

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. (ISO 16.1.2)

Implementatierichtlijn

Alle medewerkers en contractanten behoren bewust te worden gemaakt van hun verantwoordelijkheid om informatiebeveiligingsgebeurtenissen zo snel mogelijk te rapporteren. Zij behoren ook te worden geïnformeerd over de procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen en het centrale punt waaraan de gebeurtenissen behoren te worden gerapporteerd.

Met betrekking tot het rapporteren van informatiebeveiligingsgebeurtenissen behoort rekening te worden gehouden met de volgende situaties:

a) niet-doeltreffende beveiligingsbeheersmaatregelen;

b) schending van informatie-integriteit, vertrouwelijkheid of aanwezige verwachtingen;

c) menselijke fouten;

d) niet-naleving van beleidsregels of richtlijnen;

e) schending van fysieke beveiligingsregelingen;

f) onbeheerste systeemveranderingen;

g) storingen in soft- of hardware;

h) overtredingen van de toegangsregeling.

C.9.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Beheersmaatregel

Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermoede zwakke plekken in de informatiebeveiliging registreren en rapporteren. (ISO 16.1.3)

Implementatierichtlijn

Alle medewerkers en contractanten behoren deze zaken zo snel mogelijk aan het contactpunt te rapporteren om informatiebeveiligingsincidenten te voorkomen. Het rapporteringsmechanisme behoort zo eenvoudig, toegankelijk en beschikbaar te zijn als mogelijk is.

C.9.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Beheersmaatregel

Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten. (ISO 16.1.4)

Implementatierichtlijn

Het contactpunt behoort elke informatiebeveiligingsgebeurtenis te beoordelen op basis van het overeengekomen classificatieschema voor gebeurtenissen en incidenten betreffende informatiebeveiliging, en te besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen.

In gevallen waarin de organisatie beschikt over een medewerker voor informatiebeveiligingsincidenten (CSIRT/SOC), kunnen de beoordeling en het besluit hier naar worden doorgestuurd voor bevestiging of herbeoordeling.

Resultaten van de beoordeling en het besluit behoren in detail in een verslag te worden vastgelegd ten behoeve van toekomstige verwijzing en verificatie.

C.3.1.5 Respons op informatiebeveiligingsincidenten

Beheersmaatregel

Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. (ISO 16.1.5)

Implementatierichtlijn

Op informatiebeveiligingsincidenten behoort te worden gereageerd door een aangewezen contactpunt en andere relevante personen van de organisatie of externe partijen (zie ISO 16.1.1).

De respons behoort de volgende aspecten te omvatten:

a) zo snel mogelijk na de gebeurtenis bewijs verzamelen;

b) indien vereist, forensische analyse van de informatiebeveiliging uitvoeren (zie ISO 16.1.7);

c) escaleren indien vereist;

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 communiceren aan anders in- en externe personen of organisaties met een need-to-know;

f) behandelen van de zwakke plek(ken) in de informatiebeveiliging waarvan is vastgesteld dat deze het incident heeft/hebben veroorzaakt of eraan heeft/hebben bijgedragen;

g) het incident formeel afsluiten en verslaglegging bijhouden zodra het incident met succes is behandeld.

Om de bron van het incident te identificeren behoort postincidentanalyse plaats te vinden.

C.3.1.6 Lering uit informatiebeveiligingsincidenten

Beheersmaatregel

Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. (ISO 16.1.6)

Implementatierichtlijn

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gemonitord. De informatie die is verkregen uit de evaluatie van informatiebeveiligingsincidenten behoort te worden gebruikt om terugkerende of ingrijpende incidenten te identificeren.

C.3.1.7 Verzamelen van bewijsmateriaal

Beheersmaatregel

De organisatie behoort procedures te definiëren en die te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. (ISO 16.1.7)

Implementatierichtlijn

Bij het omgaan met bewijs ten behoeve van disciplinaire en wettelijke actie behoren interne procedures te worden ontwikkeld en gevolgd.

In het algemeen behoren deze bewijsprocedures processen in te houden voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs in overeenstemming met de verschillende soorten media, apparaten en de status van de apparaten, bijv. in- of uitgeschakeld. De procedures behoren rekening te houden met de:

a) bewakingsketen;

b) veiligheid van bewijs;

c) veiligheid van personeel;

d) rollen en verantwoordelijkheden van het betrokken personeel;

e) competentie van personeel;

f) documentatie;

g) instructie

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

Forensisch 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 forensisch bewijs te verzamelen. De eisen van verschillende rechtsgebieden behoren ook in aanmerking te worden genomen om de kans zo groot mogelijk te maken dat het bewijs wordt toegelaten in de relevante rechtsgebieden.

C.10. Informatiebeheer

Doelstelling

Informatiebeheer ontwerpt en beheert bedrijfsprocessen op functioneel niveau en verleent operationele ondersteuning aan gebruikers en beheerre van een bedoeldware informatievoorziening.

Toelichting

Bedrijfsprocessen worden zodanig ontworpen dat de opgeleverde bedrijfsmiddelen aan beveiligingseisen voldoen en dat door bedrijfsfouten bij dit proces veiligende transparantie en beheersbaarheid gehouden wordt. Het voortbrengingsproces van software wordt ingedeeld in fases. In elke fase worden producten opgeleverd, zoals gespecificeerde opdrachtenportefeuille, globaal en detail ontwerp.

Motivering

In het proces informatiebeheer worden vanuit de bedrijfsactiviteiten (de "business") eisen voor beveiliging van de bedrijfsprocessen vastgesteld en tijdig de voorwaarden geschapen voor het opnemen van geprogrammeerde controles in applicaties (application controls) en daarop aansluitende maatregelen van ADBC (user controls) in de handmatige delen van de processen. Voorts wordt in dit proces centraal voor de organisatie vastgesteld welke informatie onder welke beveiligingsvoorwaarden wordt uitgewisseld met andere organisaties.

Afbakening

De normen in deze paragraaf hebben betrekking op bedrijfsprocessen en de daarbij ondersteunende applicaties. De normen van de paragrafen C.10.1 t/m/ vormen functioneel ontwerp en implementatie. C.10.2 Kwaliteitsbeheer als zodanig is algemeen geformuleerd, zodat deze ook gebruikt kunnen worden voor het functioneel ontwerp en de implementatie van de technische infrastructuur.

C.10.1. Sturen functioneel ontwerp en implementatie

Beheersmaatregel

Het informatiebeheer kan voldoende sturing geven aan het functioneel ontwerp, onderhoud en implementatie van IT-voorzieningen.

Implementatierichtlijn

a) Er zijn criteria vastgesteld op grond waarvan voor de besturing van vernieuwing en onderhoud een aparte projectorganisatie wordt ingesteld. Deze criteria kunnen betrekking hebben op het middelenbeslag, aantal betrokken organisatieeenheden, gebruik nieuwe technologie e.d.

b) Er zijn criteria vastgesteld op grond waarvan projecten niet te omvangrijk worden (daarmee slecht bestuurbaar) en op grond waarvan er met deelprojecten wordt gewerkt.

c) Ingeval een aparte projectorganisatie noodzakelijk wordt geacht, wordt een stuurgroep ingesteld met vertegenwoordigers vanuit alle belanghebbende (in- en externe) organisatieeenheden met voldoende mandaat en kennis over de inhoud en voortgang te beslissen.

d) Er zijn criteria opgesteld op grond waarvan verplicht advies wordt ingewonnen van beveiligingsadviseurs, faseproducten daar hen worden gereviewd en onafhankelijke beveiligingstesting plaatsvindt (bijv. door in- of externe IT auditors) bij de onderscheiden faseproducten.

e) Het management van het ontwerpproces maakt afspraken over het tijdig en onafhankelijk toetsen van geplande faseproducten aan beveiligingsnormen en het rapporteren daarover.

f) De besluitvorming over acceptatie van faseproducten vindt op voldoende hoog managementniveau plaats.

g) Het detailontwerp, op grond waarvan realisatie plaatsvindt wordt goedgekeurd door representatieve vertegenwoordigers van gebruikers, functioneel en technisch beheerders op basis van testrapporten en op basis van aspectcriteria van kwaliteitsbeheer (zie C.10.2.).

h) Er is functiescheiding tussen gebruikers, functionele ontwerpers, technisch ontwerpers en bouwers en exploitatiemedewerkers.

C.10.2. Kwaliteitsbeheer

Beheersmaatregel

De kwaliteitseisen voor het ontwerpen en onderhouden van processen en IT-voorzieningen zijn vastgesteld en worden intern bewaakt op naleving.

Implementatierichtlijn

a) Het ontwerp en de realisatie wordt volgens standaard Methoden, Technieken, Hulpmiddelen en Voorschriften (MTHV's) uitgevoerd.

b) De MTHV's bevatten een inventarisatie van risico's voor het slagen van het project, waarin aandacht wordt besteed aan afhankelijkheden, randvoorwaarden, beperkingen, ervaring met toe te passen procesmatige, organisatorische en technische vernieuwingen.

c) De MTHV's geven aan wie welke mijlpaalproducten oplevert en wie deze goedkeuren voordat ze naar een volgende fase overgaan.

d) De MTHV's bevatten acceptatiecriteria voor geraakte aspecten als COPAFINITH of PIOFACH inclusief bevestiging t.o. de productnormen volgens de paragrafen **Fout! Verwijzingsbron niet gevonden.**Fasedocumenten en IT-voorzieningen, evenals de procesnormen C.11.1 Procesinrichting en C.11.4 Rapporteren over het proces zijn het gaat om het ontwerpen van processen.

e) Afwijkingen van de opdracht, uitgangsdocumentatie, kaders en aanvullende afspraken worden gemotiveerd in de opgeleverde fasedocumenten.

f) De fasedocumenten worden bewaard overeenkomstig de vastgestelde bewaartermijnen.

g) Er is een systeem van onafhankelijke kwaliteitstoetsing ter borging van de standaard MTHV's.

h) Over de resultaten van de kwaliteitstoetsing wordt gerapporteerd aan het project- en informatiemanagement.

i) De standaard MTHV's worden periodiek geëvalueerd met alle betrokkenen en zo nodig bijgesteld.

C.10.3. Fasedocumenten ontwerp en invoering IT

Doelstelling

Fasedocumenten voor het ontwerp en invoeren van IT scheppen de voorwaarden voor een betrouwbare informatieverwerking, voor zover dat afhankelijk is van IT-voorzieningen.

C.10.3.1 Beveiligingsparagraaf procesontwerp

Beheersmaatregel

In de faseproducten van het ontwerp en onderhoud van processen en applicaties wordt in een beveiligingsparagraaf aangegeven op welke wijze de normen voor beveiliging zijn geïmplementeerd.

Implementatierichtlijn

a) Er wordt een beveiligingsparagraaf in de fasedocumenten opgenomen, waarbij de hiernavolgende richtlijnen – per fase in toenemende mate van detail - worden uitgewerkt.

b) In een zo vroeg mogelijk ontwerpstadium wordt vastgesteld:

1. of er sprake is van afwijkingen van het basis beveiligingsniveau;
2. of er door of aan derden beveiligingseisen worden gesteld i.v.m. externe insourcing of uitbesteding van primaire- en/of ondersteunende;
3. of de bestaande beveiligingsuitgangspunten dan wel -maatregelen aanpassing behoeven door nieuwe ontwikkelingen en het gebruik van technologie dan wel ander gebruik daarvan;
4. of er sprake is van de specifieke invoerings- en conversieproblematiek.

Bij afwijkingen wordt advies gevraagd aan beveiligingsfunctionarissen.

c) Er zijn criteria opgesteld op grond waarvan een risicoanalyse wordt toegepast, die mede richtinggevend is voor de implementatie van de beveiligingsmaatregelen. Criteria zijn onder meer:

geheel nieuwe processen van significante bekendheid, samenwerking bij primaire processen, gebruik nieuwe technologie of aar te schaffen nieuwe IT-voorzieningen al dan niet met bekende kenmerkwaarden

d) Wanneer applicaties met een hoger beveiligingsniveau in een gemeenschappelijke omgeving worden uitgevoerd, worden de applicaties waarmee de zone in de technische infrastructuur wordt gedeeld, vastgesteld en goedgekeurd door de procesbeheerder van die applicatie.

e) Geaccepteerde (restrisico's worden expliciet vastgelegd met een motivering waarom hiervoor (nog) geen beveiligingsmaatregelen worden getroffen.

f) Er is vastgesteld of de uitgangspunten van de bedrijfscontinuiteitsplannen nog van toepassing zijn in de nieuwe of gewijzigde situatie. Het betreft:

1. de maximaal tolerabele uitvaldatuur (MTU);

2. het maximaal toegestane digitaal gegevens verlies (MGV);

3. aanvullende maatregelen als 1 en 2 niet gehaald met de aanwezig mogelijkheden van Beheer en Exploitatie IT-voorzieningen worden ingevuld:

4. reconstructie niet digitale informatie.

g) Er wordt vastgesteld of voldaan moet worden aan het melden van de privacyaspecten aan de privacyfunctionaris.

h) Het verwerken van informatie aan andere informatiesystemen en derden voldoet aan het doelbindingsbeginsel voor de privacybescherming.

i) De bewaartijden van informatiebronnen en registraties (papier, digitaal) zijn vastgesteld in een bewaarschema.

j) Maatregelen van beveiliging worden getroffen op basis van de paragraaf C.11.1 "Procesinrichting, C.11.4 Rapporteren over het proces.

C.10.3.2 Implementatieplan processen en applicaties

Beheersmaatregel

Bij de invoering van nieuwe of gewijzigde processen en applicaties wordt een implementatieplan gemaakt.

Implementatierichtlijn

a) In het implementatieplan worden de volgende onderdelen uitgewerkt:

1. benodigde mens- en middelencapaciteit voor de invoering bij alle betrokken partijen;

2. voorlichting en training in het gebruik van het informatiesysteem;

3. conversietraject;

4. interne controle bij conversie van gegevens op de juistheid en volledigheid van de overgang van de oude naar de nieuwe gegevensbestanden);

5. continuïteit van de operationele werkzaamheden;

6. wijze waarop zo nodig kan terug worden gevallen op de oude situatie of op bijzondere hiervoor ontworpen handmatige procedures (fall-back procedure);

7. welke overgangsmaatregelen moeten worden genomen voor, tijdens en na de invoering van de voorgenomen situatie.

8. te ondernemen acties bij het uitlopen van de invoeringsplanning;

9. aanstellen van deskundige aanspreekpunten per betrokken organisatieonderdeel en behoeve van de algehele voorbereiding, coördinatie, samenhang en afstemming.

b) De impact en complexiteit van de nieuwbouw en het onderhoud alsmede van conversie- of migratieactiviteiten is bepalend voor de gefaseerde invoering. De mogelijkheden om terug te keren naar vorige situaties en de mate waarin wordt schadevergoedend als deze mogelijkheden voor bestaan.

C.10.3.3 Beveiligingsparagraaf fasedocumenten technische infrastructuur

Beheersmaatregel

In de beveiligingsparagraaf van de fasedocumenten voor het ontwerp en de inrichting van IT-voorzieningen van de technische infrastructuur wordt de inrichting van de beveiliging gedocumenteerd in overeenstemming met externe en interne normen.

Toelichting

In een beveiligingsparagraaf van de fasedocumenten voor het ontwerp en de inrichting van IT-voorzieningen van de technische infrastructuur wordt de inrichting van de beveiliging gedocumenteerd in overeenstemming met externe en interne normen. In de beveiligingsparagraaf kan worden volstaan met het – per fase in voorkomende mate van detail – verwijzen naar de desbetreffende in- en externe beveiligingsnormen als ze geen verduidelijking nodig hebben, aangevuld met eventuele gemotiveerde afwijkingen daarop.

Implementatierichtlijnen

a) In een zo vroeg mogelijk ontwerpstadium wordt vastgesteld:

1. in hoeverre er sprake is van afwijkingen van het basis beveiligingsniveau
2. welke beleiddocumenten en ontwerpcriteria van toepassing zijn;
3. of de bestaande beveiligingsuitgangspunten dan wel –maatregelen aanpassing behoeven door relevante ontwikkelingen op het gebied van technologie;
4. in hoeverre de leveranciersinstructies voor het inrichten van de aspecten van beveiliging gebaseerd zijn op de facto beveiligingsrichtlijnen van erkende normeninstituten als NIST;
5. in hoeverre er sprake is van de invoerings- en conversieproblematiek en welke oplossingsrichting wordt voorgesteld.

b) In een risicoanalyse worden de specifieke eigenschappen van de IT-voorziening in beschouwing genomen en de beveiligingsinrichting vastgesteld voorzover die niet voldoende is geadresseerd in de productnormen van IT-voorzieningen en de facto beveiligingsrichtlijnen van erkende normeninstituten als NIST.

c) Bij het uitvoeren van een risicoanalyse zijn ten minste de functioneel beheerder, systeembeheerder, deskundigen en beveiligingsspecialisten betrokken.

d) Geaccepteerde (rest)risico's worden expliciet vastgelegd met een motivering waarom hiervoor geen beveiligingsmaatregelen worden getroffen.

e) In de opgeleverde systeemdocumentatie wordt de beveiligingsparametrisering vastgelegd in overeenstemming met de leveranciersinstructies en de facto beveiligingsrichtlijnen van erkende normeninstituten als NIST.

f) Voor IT-voorzieningen met een bijzonder belang voor de logische toegang tot de gegevens is in de beveiligingsparagraaf aangegeven:

1. met welke frequentie en welke geautomatiseerde hulpmiddelen beveiligingsinstellingen gecontroleerd worden;
2. welk type security violations gesignaleerd moeten worden met welke frequentie en welke tooling.

In de signaleringen wordt onderscheid gemaakt naar signalen, die in de gebruikersorganisatie moeten worden afgehandeld en signalen die betrekking hebben op Technisch Beheer en exploitatie;

3. welke uitgangspunten er worden gehanteerd voor de groepering van autorisaties opdat de dynamiek in IT-dienstverlening, processen, functies en organisaties niet tot onaanvaardbare, extra ondernemersrisicokosten kunnen leiden.

g) De beveiligingsdocumentatie van IT-voorzieningen met een bijzonder belang voor de logische toegang tot (medische)gegevens wordt goedgekeurd door het beveiligingsbeheer.

C.11. Algemeen beheer van handmatige processen

Algemeen procesbeheer bevat de normen voor het beheersen van de handmatige verwerking (de ADAPO), die per proces uitgewerkt wordt als complement en sluitstuk op de geautomatiseerde processen en daarin opgenomen controles dan wel als uitsluitend handmatig proces.

Toelichting

Het algemeen procesbeheer is in hoofdzaak op de integriteit van informatie gericht. De andere aspecten beschikbaarheid en vertrouwelijkheid worden veelal geborgd door andere (specifieke) processen in dit normenkader. Het werkingsgebied is ruimer dan een informatiesysteem, omdat in een proces meerdere (soms zelfs vele) informatiesystemen kunnen worden gebruikt.

Motivering

Het beheersen van processen in het algemeen en met name het handmatige deel daarin, is een randvoorwaarde voor het borgen van de procesmatige beveiligingsnormen en kan niet los daarvan worden beschouwd.

Afbakening

Deze normen zijn als aanvulling te beschouwen op elk in dit normenkader voorkomend proces. Ter voorkoming van herhalingen worden deze normen als apart proces hier éénmalig beschreven.

C.11.1. Procesinrichting

Beheersmaatregel

Handmatige handelingen voldoen aan eisen van beveiliging.

Implementatierichtlijn

a) Taken, bevoegdheden en verantwoordelijkheden van functierollen zijn actueel en volledig vastgesteld.

b) Per proces/applicatie is aangegeven welke taken/profielen onverenigbaar zijn uit hoofde van functiescheiding.

c) Bij conflicterende functie- of roltoervulling (bijvoorbeeld onvoldoende functiescheiding) worden compenserende maatregelen getroffen.

d) Bij de procesinrichting is vastgesteld of er sprake is van gegevens, waarvoor extra maatregelen van beveiliging van toepassing zijn en in hoeverre de volgende overweging gelden:

1. de analyse van de aspecten van vertrouwelijkheid, integriteit en beschikbaarheid;
2. wie toegang heeft tot het gebruiken of bewerken van de informatie;
3. op welke wijze de informatie wordt: ontvangen, vastgelegd, bewaard, verzonden en vernietigd moet worden.

e) Papieren invoerdocumenten worden gecontroleerd op ongeautoriseerde wijzigingen (voor alle wijzigingen in invoerdocumenten wordt toestemming gegeven).

f) Bij de uitwisseling van verplaatsbare opslagmedia of basisbeschikken, die betekenis hebben voor de integriteit en/of vertrouwelijkheid van de gegevens(verwerking) met of aan andere organisaties of organisatieonderdelen wordt gebruik gemaakt van gevoeligheidslijsten waarop in tabellen (aantallen, bedragen) de zending is aangegeven. Het verzenden en ontvangen van deze lijsten gebeurt via aparte kanalen en wordt vastgelegd. De totalen op de gevoeligheidslijsten worden o.a.m. na ontvangst afgestemd met de daarbij behorende aangeleverde mediabestanden.

g) Signalen en fouthandelingen op grond van invoer- en uitvoercontroles worden juist, volledig en tijdig afgehandeld. Uit de vastleggingen blijkt: wie welke posten wanneer heeft afgehandeld.

h) Bij hoge risico-posten worden de ingevoerde gegevens op plausibiliteit gecontroleerd.

i) Bij gegevens met een bijzondere betekenis voor het proces wordt een periodieke beoordeling gedaan van de actualiteit van sleutelvelden of gegevensbestanden om hun geldigheid en integriteit te bevestigen.

j) Intern ontstane brondocumenten, die alleen voor intern gebruik zijn bedoeld, zoals werkopdrachten, verwerkingsverslagen, mutatie- en signaallijsten worden minimaal twee jaar na afloop van het jaar waarin de opdrachten zijn afgesloten bewaard ten behoeve van controlemogelijkheden. Dit laat onverlet dat er andere redenen kunnen zijn om interne documenten langer te bewaren.

k) De distributie van uitvoerlijsten wordt vastgelegd.

l) Bij vervangings- of functiemutatieregelingen worden de functiescheidingen niet doorbroken.

m) Bij nood- of escalatieregelingen mogen de functiescheidingen alleen worden doorbroken door de hogere managementlaag, waarbij dit onverwijld schriftelijk wordt vastgelegd. Na afloop van de calamiteit wordt analytisch van de uitvoering vastgesteld of er de gegevensverwerking niet gecompromitteerd heeft of de functionaliteit van volledig hersteld is.

n) Als preventieve, calamiteiten e.d. alleen opgelost kunnen worden door het tijdelijk opheffen of vervroegen van bovenstaande beveiligingsmaatregelen, wordt dit goedgekeurd door het verantwoordelijke management en worden aanvullende maatregelen getroffen. Door het management wordt toegezien op naleving van deze maatregelen.

C.11.2. Aansturen operationele IT

Beheersmaatregel

Vastgesteld wordt dat de geautomatiseerde delen van het proces integer hebben gewerkt.

Toelichting

Dit onderdeel is ook extra te beschouwen als een productnorm voor het (proces van het) inrichten van processen. De productverantwoordelijkheid voor de inrichting kan een andere zijn dan die voor de procesverantwoordelijkheid voor de naleving.

Implementatierichtlijn

a) Dagelijks wordt vastgesteld dat de batchverwerkingen hebben plaatsgevonden volgens het draaiboek.

b) Door verwerkingslijsten gevoende controletellingen worden gebruikt om vast te stellen dat de geautomatiseerde verwerking juist en volledig heeft plaatsgevonden. In voorkomende gevallen wordt vastgesteld dat de beginstanden aansluiten op eindstanden van de voorgaande verwerking en periodiek dat stellingen van gegevensverzamelingen aansluiten op de vanuit de mutaties opgebouwde eindstanden.

c) Bij bestandsuitwisseling met systeemvreemde omgevingen worden de totalen van ontvangen en verzonden bestanden met de brondocumenten (geleidelijsten, verwerkingsverslagen) afgestemd.

d) Ve schillen die geconstateerd worden bij periodieke bestandsvergelijkingen worden tijdig geanalyseerd en opgelost, waarbij structurele problemen aan informatiemanagement worden doorgegeven.

e) Uitvoerlijsten worden gecontroleerd op volledigheid.

f) Variabelen/parameters in tabellen van applicaties worden periodiek gecontro eerd.

g) Er is functiescheiding tussen vaststelling, invoer en periodieke controle van (wijzigingen van) variabelen/parameters in tabellen van applicaties.

C.11.3. Verwerken gegevens op basis van vraagtaken

Beheersmaatregel

De gegevensverwerking op basis van vraagtaken (queries, Business Intelligence systemen volgens aan steun van beveiliging.

Implementatierichtlijn

a) Bij het verstrekken van informatie uit vraagtaken worden de uitgangspunten voor de logische toegangsbeveiliging en doelbinding vanuit de optiek van privacybescherming niet doorbroken.

b) Bij het samenstellen van programma's op basis van vraagtaken wordt ervoor zoggedragen dat door middel van controletellingen kan worden vastgesteld dat de juiste en volledige

gegevensverzameling wordt gebruikt, tenzij daarover andere zekerheden bestaan. Controletellingen kunnen bijvoorbeeld aansluiten op eerdere totaaltellingen volgens verwerkingsverslagen dan wel op tellingen of saldi vanuit andere gegevensverzamelingen met overeenkomstige gegevens, zoals het grootboek.

c) De bij vraagtalen gebruikte selectie- en zoekcriteria worden op het verwerkingsverslag weergegeven, teneinde controle op de juistheid van de verwerking achteraf mogelijk te maken.

c) De controle op volledigheid en juistheid van de selectie door middel van vraagtalen vindt plaats in functie gescheiden van de ontwikkeling en productie van de output.

C.11.4. Rapporteren over het proces

Beheersmaatregel

Op basis van rapportage vindt sturing van het proces plaats.

Toelichting

Dit onderdeel is ook extra te beschouwen als een productnorm voor het (proces van het) inrichten van processen. De productverantwoordelijkheid voor de inrichting kan een andere zijn dan die voor de procesverantwoordelijkheid voor de naleving.

Implementatierichtlijn

a) Per proces wordt periodiek gerapporteerd over Key Performance Indicatoren (KPI's), onder andere over de naleving van de beveiligingsnormen, de voortgang van de jaarplanning en procesverbeteringen.

b) Naast de rapportage-items gedurende de rapportageperiode, wordt er bij voorkeur ook een trendmatig overzicht over de huidige en daaraan voorafgaande periodes weergegeven.

c) Bij gebruik van kengetallen is vermeld hoe deze zijn berekend en zijn gehanteerde begrippen eenduidig gedefinieerd.

d) Afwijkingen ten opzichte van de norm en/of trendbreuken worden geanalyseerd en in de rapportage toegelicht, waarbij tevens wordt vermeld welke acties in gang zijn gezet om de procesgang naar het gewenste niveau terug te brengen.

e) De juistheid en volledigheid van de gerapporteerde cijfers zijn controleerbaar.

C.11.5. Beheersen en evalueren van het proces

Beheersmaatregel

De opzet en uitvoering van het proces wordt intern beheerst en geëvalueerd.

Implementatierichtlijn

a) Per proces wordt door onafhankelijke interne controleurs volgens een Intern Controle Programma controle op naleving van de normen van C.11. Algemeen beheer van handmatige processen uitgeoefend.

b) De frequentie van de uitvoering van de interne controle wordt mede bepaald door risicoanalyse.

c) De uitvoering van de interne controles wordt gepland en geregistreerd.

d) Van de uitvoering en conclusies van de interne controle is een audit trail met bewijsstukken beschikbaar.

e) Over de resultaten van de controlewerkzaamheden i.c. geconstateerde afwijkingen van de normen, wordt periodiek gerapporteerd aan het verantwoordelijk lijn- en procesmanagement.

f) Over het tijdig oplossen van negatieve bevindingen worden afspraken gemaakt, voortgangsbewaking ingesteld en verantwoording afgelegd.

g) In het werkoverleg of daarop gerichte periodieke sessies wordt nagegaan of de inrichting van het proces nog optimaal is. Daaraan kunnen ideeënbussen, risicoanalyses, proces- en interne controlerapportages een bijdrage leveren. Wensen tot verbetering worden doorgegeven aan de procesbeheerder.

C.12. Ontwikkelen van applicaties en informatiesystemen

C.12.1. Beveiligingseisen voor informatiesystemen

Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken. (ISO 14.1)

C.12.1.1 Analyse en specificatie van informatiebeveiligingseisen

Beheersmaatregel

De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. (ISO 14.1.*)

Implementatierichtlijn

Informatiebeveiligingseisen behoren te worden vastgesteld met gebruikmaking van verschillende methoden zoals het afleiden van nalevingseisen van beleidsregels en regelgeving, dreigingsmodellering, beoordelingen van kwetsbaarheden of het gebruiken van kwetsbaarheidsdrempels. Resultaten van de identificatie behoren te worden gedocumenteerd en beoordeeld door alle belanghebbenden.

Informatiebeveiligingseisen en beheersmaatregelen behoren een afspiegeling te zijn van de waarde van de betrokken informatie voor het bedrijf (zie 8.2) en de potentiële schade voor het bedrijf als gevolg van een gebrek aan adequate beveiliging.

Het vaststellen en beheren van informatiebeveiligingseisen en samenhangende processen behoort te worden geïntegreerd in een vroeg stadium van informatiesysteemprojecten. Vroegtijdige overweging van informatiebeveiligingseisen, bijv. in het ontwerpstadium, kan leiden tot oplossingen die doeltreffender en goedkoper zijn.

Met betrekking tot informatiebeveiligingseisen behoren ook de volgende aspecten in overweging te worden genomen:

a) de vereiste mate van betrouwbaarheid ten opzichte van de beweerde identiteit van gebruikers om authenticatie-eisen voor gebruikers af te leiden;

b) procedures voor het verlenen van toegang en autorisatie, voor zakelijke en voor bevoorrechte of technische gebruikers;

c) gebruikers en operators informeren over hun plichten en verantwoordelijkheden;

d) de vereiste beschermingsbehoeften van de betrokken bedrijfsmiddelen, in het bijzonder met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit;

e) eisen die zijn afgeleid van bedrijfsprocessen, zoals registreren en monitoren van transacties, eisen voor onweerlegbaarheid;

f) eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging, bijv. interfaces voor het registreren en monitoren of systemen voor het opsporen van lekken van gegevens.

Voor toepassingen die diensten verlenen via openbare netwerken of die transacties implementeren, behoren de beheersmaatregelen ISO 14.1.2 en ISO 14.1.3 in overweging te worden genomen.

Bijv. het kopen van producten behoort een formele test- en acquisitieprocedure te worden gevolgd. In de contracten met de leveranciers behoren de vastgestelde beveiligingseisen te zijn opgenomen. Als de beveiligingsfunctionaliteit in een voorgesteld product niet voldoet aan de voorgeschreven eis,

behoren het geïntroduceerde risico en de daarmee samenhangende beheersmaatregelen te worden heroverwogen voordat het product wordt gekocht.

Beschikbare richtlijnen voor de beveiligingsconfiguratie van het product die in overeenstemming zijn gebracht met de uiteindelijke software/dienstverlening van dat systeem behoren te worden geëvalueerd en geïmplementeerd.

Criteria voor het accepteren van producten behoren te worden gedefinieerd, bijv. in de zin van hun functionaliteit, wat zekerheid verschaft dat aan de geïdentificeerde beveiligingseisen is voldaan. Voordat producten worden gekocht behoren ze te worden geëvalueerd tegen deze criteria. Om te waarborgen dat de producten geen onacceptabele extra risico's introduceren, behoort extra functionaliteit te worden beoordeeld.

C.12.1.2 Toepassingen op openbare netwerken beveiligen

Beheersmaatregel

Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging. (ISO 14.1.2)

Implementatierichtlijn

Overwegingen betreffende informatiebeveiliging voor toepassingen die zich over openbare netwerken bewegen, behoren de volgende aspecten te bevatten:

a) de mate van betrouwbaarheid die beide partijen eisen van elkaars beweerde identiteit, bijv. via authenticatie;

b) autorisatieprocedures voor wie de inhoud van belangrijke transactiedocumenten mag goedkeuren, belangrijke transactiedocumenten in circulatie mag brengen of mag ondertekenen;

c) bewerkstelligen dat communicatiepartners volledig zijn geïnformeerd over hun bevoegdheden om de dienst te verschaffen of te gebruiken;

d) vaststellen van en voldoen aan eisen ten aanzien van vertrouwelijkheid, integriteit, bewijs van verzending en ontvangst van belangrijke documenten en de onweerlegbaarheid van contracten, bijv. in samenhang met inschrijvings- en contractprocedures;

e) de vereiste mate van vertrouwen in de integriteit van belangrijke documenten;

f) de eisen ten aanzien van bescherming van vertrouwelijke informatie;

g) de vertrouwelijkheid en integriteit van ordertransacties, betalingsinformatie, gegevens betreffende afleveringsadressen en ontvangstbevestigingen;

h) de mate van verificatie die passend is voor controle van betalingsinformatie die door een klant is verstrekt;

i) de keuze van de meest geschikte betalingsvorm ter bescherming tegen fraude;

j) het vereiste beschermingsniveau om de vertrouwelijkheid en integriteit van orderinformatie te handhaven;

k) vermijding van verlies van of vermenigvuldiging van transactie-informatie;

l) aansprakelijkheid in verband met frauduleuze transacties;

m) eisen met betrekking tot verzekering.

Veel van bovengenoemde aspecten kunnen worden aangepakt door toepassing van cryptografische beheersmaatregelen (zie hoofdstuk ISO 10), waarbij rekening wordt gehouden met naleving van wettelijke eisen (zie hoofdstuk ISO 18, zie in het bijzonder ISO 18.1.5 voor wetgeving betreffende cryptografie).

Regelingen tussen partners betreffende toepassingen behoren te worden ondersteund door een schriftelijke overeenkomst die beide partijen bindt aan de overeengekomen voorwaarden van de diensten, met in begrip van afspraken over autorisaties (zie bovenstaand punt b).

Elken betreffende wetgeving aanvallen behoren te worden overwogen; hierbij kan worden gedacht aan elken ter beschikking van de betrokken toepassingssystemen of het waarborgen van de bedrijfsbaarheid van onderlinge netwerkverbindingen die nodig zijn om de dienst te leveren.

C.12.1.3 Transacties van toepassingen beschermen

Beheersmaatregel

Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegde vermenigvuldiging of afspelen. (ISO 14.1.3)

Implementatierichtlijn

Overwegingen betreffende informatiebeveiliging voor transacties van toepassingen behoren de volgende aspecten te behelzen:

a) het gebruik van elektronische handtekeningen door alle partijen die bij de transactie betrokken zijn;

b) alle aspecten van de transactie, d.w.z. waarborgen dat:

1) geheime authenticatie-informatie van gebruikers van alle partijen geldig en geverifieerd is;

2) de transactie vertrouwelijk blijft;

3) de privacy van alle betrokken partijen behouden blijft.

c) versleuteling van de communicatiepaden tussen alle betrokken partijen;

d) beveiliging van protocollen die worden gebruikt om te communiceren tussen alle betrokken partijen;

e) beveiligingen dat de opslaglocatie van transactiegegevens zich buiten een publiek toegankelijke omgeving bevindt, bijv. op een opslagplatform op het intranet van de organisatie, en niet wordt bewaard en gehandhaafd op een opslagmedium dat direct vanuit internet toegankelijk is;

f) 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 certificaathandtekeningen.

C.12.2. Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling: Beveiligingen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen. (ISO 14.2)

C.12.2.1 Beleid voor beveiligd ontwikkelen

Beheersmaatregel

Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast. (ISO 14.2.1)

Implementatierichtlijn

Beveiligd ontwikkelen is een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem. In een beleid voor beveiligd ontwikkelen behoren de volgende aspecten in overweging te worden genomen:

a) beveiliging van de ontwikkelomgeving

b) richtlijnen betreffende beveiliging in de levenscyclus van softwareontwikkeling;

1) beveiliging in de softwareontwikkelmethodologie;

2) beveiligdecoderingrichtlijnen voor elke programmeertaal die wordt gebruikt

c) beveiligingseisen in de ontwikkelfase;

d) beveiligingsoorlogspunten binnen de rijlijnen van het project;

e) beveiligde informatiecentra;

f) beveiliging van de versiebeheer;

g) vereiste kennis over toepassingsbeveiliging;

h) het vermogen van de ontwikkelaar om kwetsbaarheden te vermijden, te vinden en te repareren.

Technieken voor beveiligd programmeren behoren zowel te worden gebruikt voor nieuwe ontwikkelingen als in scenario's voor hergebruik van codes waarvan de normen die voor de ontwikkeling zijn toegepast niet bekend zijn of niet consistent waren met de huidige 'best practices'. Toepassing van beveiligdecoderingsnormen behoort te worden overwogen en indien relevant verplicht te worden gesteld. Ontwikkelaars behoren te worden getraind in het toepassen van codering, en het gebruik behoort te worden geverifieerd door te testen en de codes te beoordelen.

Indien ontwikkelactiviteiten worden uitbesteed behoort de organisatie zich ervan te vergewissen dat de externe partij deze regels voor veilig ontwikkelen naleeft (zie ISO 14.2.7).

C.12.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen

Behoorsmaatregel

Wijzigingen aar systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer. (ISO 14.2.2)

Implementatierichtlijn

Formele procedures voor wijzigingsbeheer behoren te worden gedocumenteerd en afgedwongen om de integriteit van het systeem, de toepassingen en producten te waarborgen, vanaf de vroegste ontwerpstadia tot en met de laatste onderhoudsactiviteiten. De introductie van nieuwe systemen en belangrijke wijzigingen aan bestaande systemen behoort een formeel proces te volgen van documentatie, specificatie, test, kwaliteitscontrole en beheerde implementatie.

Dit proces behoort een risicobeoordeling, een analyse van de gevolgen van wijzigingen en een specificatie van de nodige beveiligingsverbeteringsmaatregelen te omvatten. Dit proces behoort ook te waarborgen dat bestaande beveiligings- en beheersingsprocedures niet worden gecompromitteerd, dat programmeurs die ondersteunende werkzaamheden uitvoeren alleen toegang krijgen tot die delen van het systeem die zij voor hun werkzaamheden nodig hebben en dat voor elke wijziging formele instemming en goedkeuring is verkregen.

Waar mogelijk beheren procedures voor wijzigingsbeheer voor toepassingssoftware en voor de operationele omgeving te worden gelmegreerd (zie ISO 14.2.2). De procedures voor wijzigingsbeheer behoren te omvatten, maar niet beperkt te zijn tot:

a) verslaglegging bijhouden van overeengekomen autorisatieniveaus;

b) waarborgen dat wijzigingen worden doorgevoerd door bevoegde gebruikers

c) beheersmaatregelen en integriteitsprocedures beoordelen om te waarborgen dat deze niet worden gecompromitteerd door de wijzigingen;

d) alle software, informatie, database en hardware identificeren die wijziging behoeven;

e) beveiligingskritische codes identificeren en controleren om de waarschijnlijkheid van bekende zwakke plekken in de beveiliging zo gering mogelijk te houden;

f) formele goedkeuring voor gedetailleerde voorstellen verkrijgen voor aanvang van de werkzaamheden;

g) waarborgen dat bevoegde gebruikers de wijzigingen voorafgaand aan implementatie accepteren;

h) waarborgen dat de systeemdocumentatie na elke wijziging wordt geüpdatet en dat oude documentatie wordt gearchiveerd of vernietigd;

i) versiebeheer voor alle software-updates uitvoeren;

j) een auditspoor voor alle wijzigingsverzoeken bijhouden;

k) waarborgen dat bedieningsdocumentatie (zie ISO 12.1.1) en gebruikersprocedures indien nodig worden gewijzigd om ze toepasbaar te houden;

l) waarborgen dat het implementeren van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.

C.12.2.3 Technische beoordeling toepassingen na wijzigingen besturingsplatform

Beheersmaatregel

Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. (ISO 14.2.3)

Implementatierichtlijn

In deze procedure behoort te zijn opgenomen:

a) beoordelen van procedures voor toepassingscontrole en integriteit om te waarborgen dat ze niet zijn gecompromiteerd door de veranderingen aan het besturingsplatform;

b) waarborgen dat notificatie van veranderingen aan het besturingsplatform tijdig plaatsvindt zodat de aangewezen tests en beoordelingen voorafgaand aan implementatie plaats kunnen vinden;

c) bewerkstelligen dat de juiste veranderingen plaatsvinden aan de bedrijfscontinuïteitsplannen (zie hoofdstuk ISO 17)

C.12.2.4 Beperkingen op wijzigingen aan softwarepakketten

Beheersmaatregel

Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd. (ISO 14.2.4)

Implementatierichtlijn

Voor zover mogelijk en haalbaar behoren door aanbieders geleverde softwarepakketten ongewijzigd te worden gebruikt. 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 gecompromiteerd raken;

b) of de toestemming van de verkoper behoort te worden verkregen;

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.

Indien de veranderingen noodzakelijk zijn, behoort de originele software te worden bewaard en behoren de veranderingen aan een specifiek daarvoor bestemde kopie te worden aangebracht. 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 (zie ISO 12.6.1). 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.

C.12.2.5 Principes voor engineering van beveiligde systemen

Beheersmaatregel

Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle werkzaamheden betreffende het implementeren van informatiesystemen. (ISO 14.2.5)

Implementatierichtlijn

Procedures voor de engineering van beveiligde informatiesystemen, gebaseerd op principes voor beveiligde engineering, behoren te worden vastgesteld, gedocumenteerd en toegepast op interne engineeringactiviteiten met betrekking tot informatiesystemen. Beveiliging behoort te worden ontworpen in alle lagen van de architectuur (commercieel, gegevens, toepassingen en technologie), waarbij de behoefte aan informatiebeveiliging behoort te worden afgewogen tegen de behoefte aan toegankelijkheid. Nieuwe technologie behoort te worden geanalyseerd op veiligheidsrisico's en het ontwerp behoort te worden beoordeeld aan de hand van bekende aanvalspatronen.

Deze principes en de vastgestelde engineeringprocedures behoren regelmatig te worden beoordeeld om te waarborgen dat zij doeltreffend bijdragen aan verbeterde normen voor beveiliging binnen het engineeringproces. Ze behoren ook regelmatig te worden beoordeeld om ervoor te zorgen dat ze actueel blijven in de zin dat ze nieuwe potentiële bedreigingen afwenden en toepasbaar blijven bij verbeteringen die worden toegepast in de technologieën en oplossingen.

De voor engineering vastgestelde beveiligingsprincipes behoren indien van toepassing te worden toegepast op uitbesteede informatiesystemen via de contracten en andere bindende overeenkomsten tussen de organisatie en de leverancier aan wie de organisatie uitbesteedt. De organisatie behoort te bevestigen dat de strikte toepassing van de beveiligingsprincipes voor engineering vereist/waar is met het gebruik in de eigen organisatie.

C.12.2.6 Beveiligde ontwikkelomgeving

Beheersmaatregel

Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. (ISO 14.2.6)

Implementatierichtlijn

Een beveiligde ontwikkelomgeving omvat personen, processen en technologie die in verband staan met systeemontwikkeling en integratie.

Organisaties behoren risico's te beoordelen die samenhangen met individuele verrichtingen betreffende systeemontwikkeling en beveiligde ontwikkelomgevingen vast te stellen voor specifieke verrichtingen op het gebied van systeemontwikkeling, rekening houdend met:

a) de gevoeligheid van de gegevens die door het systeem worden verwerkt, opgeslagen en verstuurd;

b) toepasselijke externe en interne eisen, zoals van regelgeving of beleidsregels;

c) beheersmaatregelen voor beveiliging die al voor de organisatie zijn geïmplementeerd ter ondersteuning van systeemontwikkeling;

d) betrouwbaarheid van personeel dat in de omgeving werkt (zie ISO 7.1.1);

e) de graad van uitbesteding met betrekking tot systeemontwikkeling;

f) de behoefte aan scheiding tussen verschillende ontwikkelomgevingen

g) toegangsbeveiliging voor de ontwikkelomgeving;

h) monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes;

i) de beheersmaatregel dat back-ups worden bewaard op veilige externe locaties;

j) controle over bewegingen van gegevens van en naar de omgeving.

Als het beschermingsniveau voor een specifieke ontwikkelomgeving is vastgesteld, behoren organisaties corresponderende processen in veilige ontwikkelprocedures te documenteren en deze beschikbaar te stellen aan alle personen die ze nodig hebben.

C.12.2.7 Uitbestede softwareontwikkeling

Beheersmaatregel

Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie. (ISO 14.2.7)

Implementatierichtlijn

Als systeemontwikkeling wordt uitbesteed behoren de volgende punten 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 uitbestede inhoud (zie ISO 18.1.2);

b) contractuele eisen voor beveiligde ontwikkel-, coderings- en testpraktijken (zie 14.2.1);

c) het goedgekeurde dreigingsmodel aan de externe ontwikkelaar beschikbaar stellen;

d) acceptatietests voor de kwaliteit en nauwkeurigheid van de leveringen;

e) bewijs leveren dat beveiligingsdrempels zijn gebruikt om minimumacceptatieniveaus voor de veiligheid en kwaliteit van privacy toe te passen;

f) bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de opzettelijke of 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) regelingen voor het deponeren van de broncode, bijv. indien de broncode niet langer beschikbaar is;

i) contractueel recht om ontwikkelprocessen en beheersmaatregelen te auditen;

j) doeltreffende documentatie van de gebouwde omgeving die wordt gebruikt om af te leveren producten te creëren;

k) de organisatie blijft verantwoordelijk voor naleving van toepasselijke wetten en verificatie van de doelmatigheid van de controle.

C.12.2.8 Testen van systeembeveiliging

Beheersmaatregel

Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. (ISO 14.2.8)

Implementatierichtlijn

Tijdens de ontwikkelprocessen zijn voor nieuwe en geactualiseerde systemen uitvoerige tests en verificatie nodig, met inbegrip van het opstellen van een gedetailleerd schema van activiteiten en tests van inputs en verwachte outputs onder diverse omstandigheden. Voor interne ontwikkelactiviteiten behoren dergelijke tests in eerste instantie te worden uitgevoerd door het ontwikkelteam. Vervolgens behoren onafhankelijke tests te worden uitgevoerd (zowel voor interne als voor uitbestede ontwikkelactiviteiten) om te bewerkstelligen dat het systeem uitsluitend werkt zoals voorzien (zie ISO 14.1.1 en ISO 14.1.9). De omvang van het testen behoort in verhouding te staan tot de belangrijkheid en de aard van het systeem.

C.12.2.9 Systeemacceptatietests

Beheersmaatregel

Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld. (ISO 14.2.9)

Implementatierichtlijn

Het uitvoeren van systeemacceptatietests behoort reeds het testen van informatiebeveiligingseisen te omvatten (zie ISO 14.1.1 en ISO 14.1.2) en het volgen van een veilige werkwijze voor systeemontwikkeling (zie ISO 14.2.1). De tests behoren ook te worden uitgevoerd op ontvangen componenten en geïntegreerde systemen. Organisaties kunnen geautomatiseerde instrumenten inzetten zoals instrumenten om codes te analyseren of om op kwetsbaarheden te scannen, en beheren het herstel van beveiligingsgerelateerde tekortkomingen te verifiëren.

Tests behoren te worden uitgevoerd in een realistische testomgeving om te bewerkstelligen dat het systeem geen kwetsbaarheden introduceert in de omgeving van de organisatie en dat de tests betrouwbaar zijn.

C.12.3. Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt. (ISO 14.3)

C.12.3.1 Bescherming van testgegevens

Beheersmaatregel

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd. (ISO 14.3.1)

Implementatierichtlijn

Het voor testdoeleinden gebruiken van operationele databases met persoonsgegevens of enige andere vertrouwelijke informatie behoort te worden vermeden. Indien persoonsgegevens of anderszins vertrouwelijke informatie wordt gebruikt voor testdoeleinden, behoren alle gevoelige details en inhoud te worden beschermd door deze te verwijderen of te wijzigen.

De volgende richtlijnen behoren te worden toegepast om operationele gegevens te beschermen die voor testdoeleinden worden gebruikt:

a) de toegangsbeveiligingsprocedures die gelden voor besturingssystemen behoren ook te gelden voor testsystemen;

b) voor elke keer dat besturingsinformatie naar een testomgeving wordt gekopieerd, behoort een afzonderlijke autorisatie te worden verkregen;

c) besturingsinformatie behoort onmiddellijk na voltooiing van het testen uit een testomgeving te worden verwijderd;

d) van het kopiëren en gebruiken van besturingsinformatie behoort verslaglegging te worden bijgehouden om in een audittraject te voorzien.

C.13. Bijlage: IT-voorzieningen

C.13.1. Inleiding

Doel stelling

IT-voorzieningen maken geautomatiseerde informatieverwerking mogelijk.

Afbakening

De Belastingdienst hanteert de normen in dit hoofdstuk aanvullend op de NEN-ISO 27002:2013.

De normen voor IT-voorzieningen hebben geen betrekking op de inherente beveiligings- en kwaliteitsaspecten, zoals die door de leveranciers in hun producten zijn ontworpen en gebouwd. Voor dit type aspecten bestaan aparte beveiligingsnormen, de zogenaamde Common Criteria (ISO/IEC 15408). Deze normen zijn minder praktisch toepasbaar en niet echt vergelijkbaar met de normen in dit hoofdstuk.

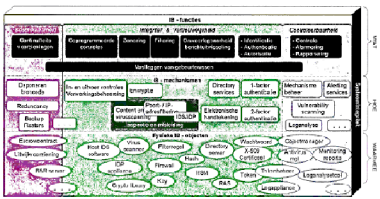
IT-voorzieningen m.u.v. bedrijfstoepassingen, worden ook wel aangeduid als technische infrastructuur en betreft hardware, besturingsprogramma's en hulpprogramma's, datanetwerkvoorzieningen. De normen voor IT-voorzieningen gaan specifiek in op de risicomogelijkheden (parameterwaarde) van de voorzieningen en op de wijze waarop die voorzieningen worden ingezet in het geheel van de technische infrastructuur, bijvoorbeeld in zones.

IB-functies

Het referentiekader voor de hier bedoelde normen wordt gevormd door het zogenaamde Model IB-functies, dat bedoeld is om te ordenen en te verbinden. Het model is in het kader van de NORA (Nederlandse Overheids Referentie Architectuur) ontwikkeld op basis van ISO-NEN 7498-2 Information processing systems – Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991.

Een IB-functie is een logische groepering van geautomatiseerde activiteiten die op een bepaald beveiligingsdoel is gericht. In samenhang worden de hagen afgebeelde beveiligingsfuncties dekkend geacht voor de informatiebeveiliging van IT-voorzieningen (zwarte functiebokken).

In het architectuurmodel zijn deze IB-functies gerepliceerd op de kwaliteitscriteria voor informatiebeveiliging: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid. In samenhang vormen ze de WAT-laag van het model.



De IB-functies met bijbehorende mechanismen en fysieke middelen zijn voor de eenvoud van afbeelding op de criteria geprojecteerd, die ze primair ondersteunen, maar de functies voor integriteit en vertrouwelijkheid dragen bijvoorbeeld ook bij aan beschikbaarheid.

De IB-mechanismen vormen de HOE-laag en zijn technische concepten (technieken) die het WAT van de IB-functies invullen. Omdat bedrijf zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden. De IB-mechanismen zijn de maatregelen waarmee IB-functies worden ingevuld. Elke maatregel kent één of meer implementatierichtlijnen.

De fysieke IB middelen vormen de WAARMEE-laag. Dit zijn IT-onderdelen, die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of applicatie, maar worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getoond. Hoewel referentiearchitecturen de HOE- en WAARMEE-laag meestal niet beschrijven, is dat hier wel gedaan om duidelijk te maken hoe en waarmee beveiligingsfuncties uiteindelijk werkzaam zijn in de IT.

De drie niveaus in de normen corresponderen niet één-op-één met de drie lagen van het architectuurmodel. Het hoogste niveau van functies loopt wel gelijk met de normbeschrijving. De twee niveaus daaronder van de normbeschrijving hebben voornamelijk betrekking op laag 2, het HOE van het architectuurmodel.

De normen zijn vooral in "enge zin" beschreven, dat wil zeggen dat er per IB-functie geen algemene, functionele eisen beschreven worden die voor alle soorten geautomatiseerde functies gelden. Voorbeelden van die algemene, functionele eisen zijn: controleerbaarheid van verandering in logon, audit trail van mutaties (parameterwijzigingen), functiescheidingen mogelijk maken, verwerkingsverslagen kunnen genereren. Deze algemene eisen maken onderdeel uit van de IB-functie Geprogrammeerde Controles. Bij die uitwerking staan echter de bedrijfsafdelingen voor ogen, zoals die in meerwerk ontwikkeld kunnen worden of als standaard pakketten worden aangeschaft.

C.13.2. Continuïteitsvoorzieningen

Doelstelling

De IT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid.

Definitie

De IB-functies die ervoor zorgen dat de juiste informatie op het juiste moment beschikbaar komt voor de dienstverlening.

Toelichting

Continuïteitsvoorzieningen voorkomen dat de dienstverlening door storingen en calamiteiten onacceptabel lang stil komt te liggen. Een voorbeeld van een maatregel in dit kader is het dubbel uitvoeren van voorzieningen, waardoor de ene voorziening de functie van de ander overneemt bij uitval.

Motivering

Deze maatregelen voorkomen dat verstoringen en calamiteiten in de IT tot gevolg hebben dat de

ciensteverlening onaanvaardbaar lang niet ondersteund wordt.

C.13.2.1 Dubbele uitvoering en spreiding van IT-voorzieningen

Beheersmaatregel

Op basis van de eisen die voortvloeien uit bedrijfseenheidsniveau wordt bepaald in hoeverre delen van de technische infrastructuur dubbel worden uitgevoerd om single-points-of-failure te verwijderen.

Implementatierichtlijnen

a) Bij het vermijden van single-points-of-failure kunnen de volgende maatregelen worden getroffen:

1. dubbele uitvoering van voorzieningen: CPU's, de productieversie van de software, gegevensopslag zoals HA/L op fileservers en databaseservers, hot of cold standby van beheervoorzieningen, clustering technologie van servers, fysieke verbindingen m.u.v. bekabeling binnen kantoorruimte;
2. zodanige plaatsing van dubbele IT-voorzieningen dat deze niet op één fysieke plaats zijn samengebracht (gescheiden kabels niet via één aansluitpunt) en dat er een veilige afstand tussen locaties bestaat;
3. IT-voorzieningen zo mogelijk geografische spreiden en op dezelfde technologie baseren;
4. ariele beschikbaarheid van reserve-voorzieningen;
5. uitwijkcontracten.

C.13.2.1.0 Herstelbaarheid van verwerking

Beheersmaatregel

Verwerkingen zijn herstelbaar.

Implementatierichtlijnen

a) De bediening van IT-voorzieningen is niet gebonden aan een fysieke locatie

b) Datacommunicatievoorzieningen beschikken over automatisch werkende alternatieve routeringsmechanismen om uitval van bijvoorbeeld verbindingen op te vangen.

c) Systemen met hogere beschikbaarheidseisen dan het basisniveau beschikken over voorzieningen op het gebied van automatic failover en load balancing, waarbij de verwerking gespreid is over twee locaties.

d) Indien op grond van deze hogere beschikbaarheidseisen de verwerking is verspreid over twee locaties, is de afstand enerzijds zodanig groot dat de kans minimaal is dat beide locaties getroffen worden door dezelfde calamiteit, anderzijds zodanig klein dat herstel van communicatiefouten niet leidt tot nieuwe, onherstelbare fouten

e) Er zijn routines voor back-up en recovery van databestanden en software, voor herstart en foutherstel van verwerkingen.

f) Berichten, die van derden zijn ontvangen en naar derden zijn verzonden, worden minimaal gebufferd totdat er voldoende zekerheid is over de integere verwerking.

g) Er is voldoende buffering van tussenbestanden bij langere verwerkingsketens.

C.13.2.2 Bewaking en alarmering IT

Beheersmaatregel

IT-voorzieningen proberen dreigende discontinuïteit van die voorzieningen zo mogelijk te voorspellen dan wel signaleren in een zo vroeg mogelijk stadium dat deze optreden

Toelichting

Denial of service attacks (het onbereikbaar maken van een dienst door een overvloed aan berichten te sturen) en controles op te grote omvang van berichten of bestanden zijn specifiek van betekenis voor de beschikbaarheid van de IT-voorzieningen, maar worden verwante de samenhang van maatregelen gezien als onderdeel van de IB-functie 'Filtering'.

Implementatierichtlijnen

a) Er worden standaard voorzieningen geïmplementeerd om de beschikbaarheid van IT-voorzieningen te bewaken op basis van aannemelijkheidsregels en gebruikersafspraken. Overschrijdingen van drempelwaarden worden doorgegeven aan een Event Console. Deze drempelwaarden kunnen een voorspelende (zoals aantal schrijffouten bij diskunits, vrije diskruimte) of een signalerende werking en is daadwerkelijk sprake van een dreiging voor de continuïteit, dan is dit is vaak hebben.

b) Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke resources (denk aan opslagcapaciteit, CPU-load, netwerkbandbreedte), zodat enkele gebruikers of een systeem niet een overmatig deel van resources kunnen opeisen en daarmee de beschikbaarheid van systemen in gevaar kunnen brengen.

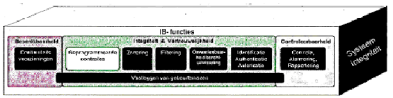
C.13.3. Geprogrammeerde controles

Doelstelling

In toepassingsprogrammatuur worden geprogrammeerde controles opgenomen, gericht op invoer, verwerking en uitvoer.

Definitie

De functies die zorgen voor hetzij geautomatiseerde controles, hetzij de levering van informatie voor het uitvoeren van handmatige controles door gebruikers of beheerders.



Toelichting

Geprogrammeerde controles in toepassingsprogrammatuur (ook wel aangeduid als Application Controls) zijn onmisbaar om de integriteit van de informatievoorziening te waarborgen. Het spreekt voor zich dat geprogrammeerde controles veel efficiënter en effectiever zijn dan handmatige controles. Geprogrammeerde controles verdienen extra aandacht bij toepassingsprogrammatuur die via Internet loopt, om het laagste beheersingsniveau van die omgeving te compenseren.

De implementatierichtlijnen van geprogrammeerde controles zijn minder integraal van toepassing dan bij de andere IB-functies. De impact van geprogrammeerde controles op de bedrijfsvoering kan aanzienlijk zijn, zodat er meer dan bij de andere IB-functies naar haalbaarheid en effectiviteit in de specifieke situatie moet worden gekeken. Bovendien zijn vele geprogrammeerde controles overlappend ten opzichte van elkaar, zodat keuzen eenvoudiger aan de orde zijn dan bij de andere IB-functies.

Niet alle geprogrammeerde controles zijn altijd van toepassing. Ook die reden is bij een aantal implementatierichtlijnen aangegeven bij welke verwerkingstypologie ze horen. Daarbij wordt er onderscheid gemaakt naar:

- Batch: verwerking van een reeks posten in één keer;
- On-line: interactieve verwerking van een post via beeldscherm door een gebruiker (ook wel on-

ineVreal-time gancemd);
- Bericht: verwerking van een individuele post afkomstig vanuit het netwerk.

Indien het onderscheid niet relevant is, zijn kruisjes opgenomen in alle kolommen achter de implementatierichtlijn.

De onder dit hoofdstuk uitgewerkte normen kunnen ook als referentiekader worden gezien voor de algemene IB-eisen voor besturingsprogramma's en (systeem) beheerpakketten die deel uitmaken van de technische infrastructuur. De normen zijn echter bedoeld voor bedrijfstoepassingen, dus zullen vele implementatierichtlijnen niet echt van toepassing zijn.

Motivering

Geprogrammeerde controles bieden de beste waarborgen dat de integriteit van de informatie(verzameling) gehandhaafd kan worden.

C.13.3.1 (Controle-technische) functie- en processcheidingen

Beheersmaatregel

Niemand in een organisatie of proces mag in staat worden gesteld om een gehele processyclus te beheersen.

Toelichting

Controle-technische functiescheiding berust op het principe van het *scheiden* van tegengestelde belangen. Kenmerkend binnen IT-omgevingen is dat deze binnen informatiesystemen moet worden afgedwongen door in de toepassing taken te scheiden en vervolgens de maatregelen van logische toegangsbeveiliging: identificatie, authentificatie en autorisatie daarop te laten aansluiten.

Implementatierichtlijnen

a) ***Taakscheidingen*** *("klassieke" functiescheiding)* (Batch, On-line, Bericht) Bewarende registrerende, uitvoerende, controlerende en beschikkende taken zijn gescheiden.

b) ***Stamgegevens versus mutaties*** (Batch, On-line Bericht) Applicatietaken voor het opvoeren van stamgegevens en het opvoeren van mutatiegegevens zijn gescheiden. Stamgegevens, ook wel vaste of referentie gegevens genoemd (geen enkel gegeven is echter helemaal vast) hebben een doorlopende betekenis in processen. Voorbeelden: rekeningen en omschrijvingen van grootboekrekeningen, stantgegevens met NAW en kredietlimiet, nummer, naam en prijs van artikelen, etc.

c) ***Scheiding bij massale invoer*** (Batch) Bij massale data-invoerprocessen worden eerste invoer, controle-invoer en het aanbrengen van correcties naar aanleiding van afgevoerde applicatiecontroles of -signaleringen als afzonderlijke (applicatie)taken onderkend. Controle-invoer kan zich bezighouden met kritische gegevens.

d) ***Aparte taak voor goedkeuren*** (On-line) Bij gegevens met een algemeen belang voor de integriteit van de gehele verwerking of bij het vaststellen van gegevens met een aanzienlijk financieel belang, wordt een aparte applicatietaak voor het goedkeuren gecreëerd om de beschikkende functie beter te ondersteunen. De verwerking van de ingevoerde gegevens vindt pas plaats, nadat goedkeuring (door een andere gebruiker) heeft plaatsgevonden.

e) ***Scheiding per zaak*** (On-line) Als applicaties bestemd zijn voor gebruikersorganisaties, waarin kort-cyclische taakrelaties aan de orde is, worden de historie van gebruikersID's en afgevoerde applicatietaken per "zaak" (dossier) vastgelegd en op onveranderbaarheid van taken gecontroleerd voordat een taak voor een bestaande "zaak" voor een gebruiker ter beschikking komt. Workflow Management Systemen zijn speciaal ingericht om deze richtlijn te realiseren.

f) ***Scheiding naar inhoud van gegevens*** (On-line) Indien verschillende behandelgroepen binnen een centrale gegevensverzameling zijn te onderscheiden, worden de applicatietaken afhankelijk gemaakt door de identificatie van deze groepen te controleren met behulp van de gegevens. Bijvoorbeeld, letter groepen van klanten, regionaal onderscheid.

g) ***Beheer versus gebruik*** (Batch, On-line, Bericht) Systeem- en applicatiebeheertaken zijn gescheiden van de overige gebruikerstaken. Muteren van rekenregels en variabelen (algemene rentepercentages, selectiecriteria) zijn als beheertaken te zien.

h) ***Scheiden en afhankelijk maken van processtappen*** (Batch, On-line, Bericht) Voor de betrouwbaarheid van processen en de gegevensverwerking kan het noodzakelijk zijn dat bepaalde processtappen in een bepaalde volgorde plaatsvinden en niet anders. Voorbeelden kunnen dit principe verduidelijken: - voor het verkrijgen van vergunning moet eerst een betaling zijn ontvangen voordat de vergunning wordt verstuurd. - voor het verkrijgen van een gewaarmerkte authenticatie voor een gebruikerscode moet eerst een activeringscode worden ingegeven, die na aanvraag wordt toegestuurd naar het officieel bekende huisadres.

i) ***Eenduidige mutatieverantwoordelijkheden*** (On-line) Om de verantwoordelijkheden voor gegevens eenduidig in een organisatie te kunnen toewijzen, is voor het muteren van gegevens een zodanig consistente set applicatietaken aanwezig, dat mutatiebevoegdheden eenduidig binnen één organisatiedeel van gebruikers toegewezen kunnen worden. Alleen een batchgewijze eerste opvoer vanuit een andere applicatie of een systeemvreemde omgeving mag hierop, in de audit trail herkenbaar, inbreuk maken. Bijvoorbeeld: de personeelsadministratie is verantwoordelijk voor de gegevens die over de medewerkers in de Active Directory worden opgenomen; is men niet daarin opgenomen dan krijgt men geen account.

j) ***Dezelfde gegevens in meerdere gegevensverzamelingen*** (Batch, On-line) Indien dezelfde gegevens in meer gegevensverzamelingen voorkomen (zodat in beginsel sprake is van redundantie), worden mutaties altijd vanuit één gebruikersorganisatie in één gegevensverzameling gemuteerd, waarbij die mutaties automatisch, batchgewijs en als zodanig herkenbaar in de audit trail, worden overgebracht (gekopieerd) naar de andere gegevensverzamelingen.

C.13.3.2 Invoercontroles

Beheersmaatregel

Alle ingevoerde gegevens vanuit een systeemvreemde omgeving worden op juistheid (J), tijdigheid (T) en volledigheid (V) gecontroleerd voordat verdere verwerking plaatsvindt. Bij batchgewijze verwerking heeft de controle op de volledigheid ook betrekking op het aantal posten of mutaties dat deel uitmaakt van de batch.

Toelichting

Onder een systeemvreemde, niet-vertrouwde omgeving wordt verstaan elke omgeving die niet volledig kan worden beheerst vanuit het perspectief en de samenhang van het eigen toepassingsgebied.

Implementatierichtlijnen

a) ***Onderscheid in invoeren, wijzigen en verwijderen (J)*** (On-line) Er bestaan verschillende applicatietaken voor invoeren, wijzigen en verwijderen om de juiste invoercontroles (geautomatiseerd dan wel handmatig) mogelijk te maken.

b) ***Validatie, bestaanbaarheid, relatie (J)*** (Batch, On-line, Bericht) De ingevoerde gegevens vormen een complete en consistente gegevensset in de context van de applicatie. De toegestane waarden van de ingevoerde gegevens worden op juistheid gecontroleerd om de volgende fouten te ontdekken - waarden die buiten het geldige bereik vallen; - ongeldige tekens in invoervelden; - ontbrekende of onvolledige kritische gegevens; - overschrijding van boven- en ondergrenzen voor gegevensvolumes (buffer overruns/overflows); - inconsistentie ten opzichte van andere gegevens binnen invoer dan wel in andere gegevensbestanden. Foutieve invoer wordt geweigerd, onwaarschijnlijke invoer wordt gesignaleerd.

c) ***Weigeren invoer per batch (J)*** (Batch) Voor het retourneren van batchgewijze invoer in verband met niet te verwerken posten (uitval) worden vuistregels gehanteerd, die periodiek worden geëvalueerd (bijv. bij meer dan 10 geweigerde posten, hele bestand retour afzender).

d) ***Signaleren invoer (J)*** (Batch, On-line, Bericht) Afwijkende invoer op grond van relatie- en

redelijkheidscontrole wordt aan de gebruiker gesignaleerd voordat de invoer in de applicatie wordt verwerkt.

e) ***Terugmelden omschrijving (J)*** (On-line) Indien van toepassing worden bij ingevoerde codes of sleutelgegevens de daarbij behorende omschrijving teruggemeld ter visuele controle met het invoerdocument (bijv. NAW-gegevens bij BurgerServiceNummers.)

f) ***Verplichte veldinvulling bij kritische gegevens (J)*** (On-line) Gegevenselementen die kritisch zijn voor de toepassing worden verplicht ingevuld.

g) ***Default waarden (J)*** (On-line) Vul de meest waarschijnlijke waarde van een veld al in, indien dit van toepassing is. Bijvoorbeeld: in een registratie voor tijdschrijven de code N voor normale uren versus O voor overwerk. Default waarden zijn niet toegestaan bij ***kritische*** gegevenselementen.

h) ***Controle getal (check digit) (J)*** (Batch. On-line. Bericht) Relevante code- aanduidingen of sleutelgegevens (BurgerServiceNummer, rekeningnummers, et cetera) van 4 of meer posities zijn van een check-digit voorzien aan de hand waarvan de bestaanbaarheid van de codeaanduiding door de applicatie kan worden vastgesteld.

i) ***Voorkomen dubbele invoer / controle op uniciteit (J)*** (Batch) Het opnemen van volgnummers in records of berichten en controle op uniciteit kan dubbele invoer voorkomen. Toepassing is mede afhankelijk van de mogelijkheden van de verwerkingscontroles dan wel productiecontroles dan wel de ernst van gevolgen van dubbele verwerking

j) ***Correctiemogelijkheden (J)*** (Batch, On-line, Bericht) Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen en/of te verwijderen. NB: wijzigen is verwijderen en toevoegen.

k) ***Invoer aan de bron (J)*** (Batch, On-line, Bericht) In een keten van verwerkingen (door meerdere organisaties) worden invoercontroles zoveel mogelijk bij de eerste verwerking (bij de bron) uitgevoerd, omdat daar de meeste kennis over die gegevens bestaat.

l) ***Voorinvullen e-formulieren (J)*** (Batch, Bericht) De invoervelden van elektronische formulieren worden zoveel mogelijk tevoren ingevuld met reeds vastgestelde gegevens.

m) ***Terugmelden invoer klantgegevens (J)*** *(Batch, On-line, Bericht)* Ingevoerde klantgerelateerde gegevens worden aan de klant in apart proces bevestigd met het verzoek de gegevens te controleren en meteen te (later) wijzigen bij fouten.

n) ***Klant inschakelen (J)*** (Batch, On-line, Bericht) Klanten hebben inzage in hun eigen gegevens en worden gestimuleerd hun gegevens op eigen initiatief te wijzigingen indien nodig. Hiervoor worden functionaliteiten aangeboden.

o) ***Volledigheid (en juistheid) inzending berichten (J en V)*** (Bericht) Bij onregelmatige inzending van berichten wordt aan de verzender duidelijk gemaakt dat er meteen een bevestiging van ontvangst moet worden verkregen, zo mogelijk gecombineerd met de resultaten van de (eerste) verwerking. Hierdoor kan de inzender worden ingeschakeld bij het constateren dat de post (juist) is aangekomen.

p) ***Vastleggen verwerkingsdatum (T)*** (Batch, On-line, Bericht) Ten behoeve van de controle op tijdigheid van ontvangst en verdere verwerking wordt per verwerking de datum vastgelegd op basis van de systeemdatum.

q) ***Voortgangscontrole (T)*** (Batch, On-line, Bericht) Door vergelijking van de verschillende (verwerkings)datums wordt voortgangscontrole op de verwerking uitgeoefend.

r) ***Volledigheid invoer /volgorde controle (V)*** (Batch, Bericht) Door het opnemen van volgnummers in berichten of invoerrecords kan de volledige ontvangst worden vastgesteld, mits het aantal invoerbronnen beperkt is.

s) ***Batch- en hashtotals (V)*** (Batch, Bericht) Door middel van het inbrengen van voortellingen van batch-(aantallen/bedragen) en -/hashtotals van invoerdocumenten / geleidelijsten in de applicatie wordt de volledigheid van massale invoer gecontroleerd.

1100035 00013

C.13.3.3 Uitvoercontroles

Beheersmaatregel

De uitvoerfuncties van programma's maken het mogelijk om de juistheid, tijdigheid en/of volledigheid van de gegevens te kunnen vaststellen.

Implementatierichtlijnen

a) ***Uitvoer alleen van noodzakelijke gegevens (J)*** (Batch, On-line, Bericht) De uitvoer (elektronisch of op papier) bevat alleen die gegevens die nodig zijn voor de doeleinden van de ontvanger (ook: client). Elektronische uitvoer wordt niet pas op de bestemming gefilterd.

b) ***Maken afdruk van gegevens van een post/zaak (J)*** (On-line) Het maken van een afdruk van gegevens mag alleen plaatsvinden via een applicatietaak en niet via een generieke hardcopy (print screen) functie van de werkstations. Toelichting: het maken van schermafdrukken is een te beïnvloeden functie, die geen bewijs kan opleveren van een geautoriseerde processtap.

c) ***Wettelijke eisen (J)*** (Batch, On-line, Bericht) Automatisch gegenereerde bescheiden voor klanten voldoen aan de wettelijke vereiste vormvoorschriften.

d) ***Afdrukken selectiecriteria bij uitvoerlijsten (J)*** (Batch) Bij variabele instelmogelijkheden worden de selectiecriteria, die gebruikt zijn om de uitvoer te bepalen, op de desbetreffende uitvoerlijsten afgedrukt.

e) ***Geleidelijsten (J en V)*** (Batch) Uitvoerbestanden die op verplaatsbare media worden uitgewisseld, zijn voorzien van geleidelijsten met (hash) totalen van ***kritische*** gegevens en bedragen. Deze (hash)totalen komen ook voor in het bestand (voorloop- of sluitrecord)

f) ***Volledigheid verzending berichten (V)*** (Bericht) Bij verzending van berichten, waarbij risico's op juridische geschillen mogelijk zijn, worden voorzieningen getroffen die volledige verzending kunnen aantonen. Mogelijkheden: (automatische) terugmelding van ontvangst; – tijdige signalering van het niet-tijdig reageren op het verzonden bericht; toekennen volgnummers aan berichten, waarbij er zekerheid moet zijn dat er volgnummercontrole plaatsvindt bij de ontvangende partij.

g) ***Volledigheid uitvoer (V)*** (Batch) Als een batchproces geen uitvoer produceert, wordt een nihilverslag of nihilbestand aangemaakt. Hierdoor is het voor de volgende processen duidelijk dat er terecht geen uitvoer is. Kritische uitvoerlijsten, die niet met een vaste periodiciteit worden geproduceerd, bevatten volgnummers dan wel anderszins een verwijzing naar de laatste lijst.

h) ***Volledigheid uitvoerlijsten zelf (V)*** (Batch) Om de volledigheid van uitvoerlijsten te kunnen constateren, wordt elk verslag afgesloten met een "einde-verslag" regel of per pagina een nummering bestaande uit het paginanummer en het totale aantal pagina's van het document.

i) ***Controletellingen batchverwerking (V)*** (Batch) Batchuitvoer bevat controletellingen die zijn gebaseerd op tijdens de computerverwerking opgebouwde tellingen. Indien tellingen worden overgenomen uit bestanden, is dat kenbaar gemaakt op de uitvoerlijsten.

j) ***Voldoende mogelijkheden tot informatievoorziening (J,T,V)*** (Batch, On-line, Bericht) Het aanwezig zijn van voldoende mogelijkheden (gestructureerd, en ongestructureerd via bijv. queries) om over (geaggregeerde) informatie te beschikken, kan een bijdrage leveren aan het toetsen van de juistheid, tijdigheid en volledigheid van de informatieverwerking. De informatievoorziening maakt cijferbeoordeling, ouderdomsanalyse, voortgangsbewaking via meerdere invalshoeken e.d. mogelijk.

C.13.3.4 Verwerkingsbeheersing

Beheersmaatregel

Toepassingsprogrammatuur biedt mogelijkheden om te constateren dat alle ter verwerking aangeboden invoer juist, volledig en tijdig is verwerkt.

Implementatierichtlijnen

a) **Transactionele integriteit in lange ketens van verwerking (J)** (Bericht) De risico's van verlies

van transactionele integriteit bij het verwerken van gegevens in lange ketens wordt opgevangen op applicatieniveau als verwerkingszekerheid vereist is.

Toelichting: Het implementeren van zekerheidsstelling op systeemniveau dat berichten ook daadwerkelijk aan het eind van een keten zijn verwerkt, kost vooralsnog veel overhead en dus performance. Een methode bij raadpleging kan zijn de ketens korter te maken door kopieën van (basis)bestanden in deeltrajecten te gebruiken. Vooralsnog is het effectiever dergelijke zekerheden in het proces (de applicatie) in te bouwen. Hiervoor bestaan diverse methoden; van het zenden van een bevestigingsbericht tot het dagelijks afstemmen van verwerkingstotalen.

b) ***Informatieverstrekking aan derden (J)*** (Batch) In de verwerkingsverslagen worden bij batchgewijze informatieverstrekking aan derden naast de uitvoertellingen tevens de ontvangende instantie vermeld.

c) ***Inhoud audit trail (J)*** (Batch, On-line, Bericht) De audit trail bevat voldoende gegevens om achteraf te kunnen herleiden welke essentiële handelingen wanneer door wie of vanuit welk systeem met welk resultaat zijn uitgevoerd. Tot essentiële handelingen worden in ieder geval gerekend: opvoeren en afvoeren posten, statusveranderingen met wettelijke, financiële of voor de voortgang van het proces, de zaak of de klant beslissende gevolgen.

d) ***Raadpleegbaarheid audit trail (J)*** (Batch, On-line, Bericht) Alle ingevoerde, gemuteerde of vervallen posten die onderdeel uitmaken van de audit trail, zijn op doelmatige wijze naar verschillende gezichtspunten raadpleegbaar ten behoeve van het oplossen van vragen en problemen alsmede voor het uitoefenen van interne controle.

e) ***Schonen audit trail (J)*** (Batch, On-line, Bericht) Indien gegevens ten behoeve van de audit trail in databases (als occurrences) raadpleegbaar blijven, zijn er aparte applicatietaken beschikbaar voor het verwijderen van oude gegevens.

f) ***Bewaartermijn audit trail (J)*** (Batch, On-line, Bericht) De audit trail wordt tenminste twee jaar bewaard of zoveel langer als de wet bepaalt indien van toepassing.

g) ***Handmatige bestandscorrecties (J)*** (Batch, On-line, Bericht) Indien handmatige invoer ter correctie van bestandsgegevens niet te vermijden is (want dan heeft de applicatie kennelijk geen sluitend stelsel van controle- en correctiemaatregelen), worden de resultaten van deze bewerkingen in "wat wordt" verslagen vastgelegd. Speciale aandacht is dan te besteden aan de volledigheid van deze uitvoerverslagen, zie de normen hieraan voorafgaand.

h) ***Controletellingen vervolg (V)*** (Batch, On-line) De applicatie geeft door middel van controletellingen inzicht in de verwerking van de invoerstroom tot de uitvoerstroom en/of mutaties op basisregistraties. Daartoe worden op de verwerkingsverslagen controletellingen afgedrukt, die gesplitst zijn naar soort invoer, soort uitvoer of verwerking.

Toelichting: na een afgeronde cyclus van verwerkingen (meestal per dag) wordt aangegeven in hoeverre ingevoerde mutaties wel of niet verwerkt zijn. Voor zover er basisregistraties worden verwerkt, worden deze tellingen gepresenteerd in de vorm van een doorrekening (balanscontrole) in aantallen: beginstand + nieuw – vervallen = eindstand, in bedragen: beginstand + nieuw □ wijzigingen – vervallen = eindstand

Overwegingen bij een stelsel van controletellingen - Het ontwerpen van een stelsel van controletellingen, waarmee een doorrekening kan worden gemaakt, is bij complexe processen geen sinecure. Bovendien dienen de handmatige procedures hierop aan te sluiten, hetgeen een flink beslag op middelen kan betekenen. Dit moet opwegen tegen het belang van het verkrijgen van zekerheden over de volledigheid van de basisregistratie. Indien de individuele posten in een basisregistratie voldoende frequent worden gebruikt voor raadpleging en/of vergelijking met posten uit andere niet daarvan afgeleide gegevensverzamelingen, kan wellicht ook voldoende zekerheid worden verkregen over de volledigheid en mogelijk juistheid van de posten in de basisregistratie. - Een ander punt van overweging is opslag in het systeem van de tellingen (met risico van manipulatie) versus het opnieuw herberekenen en presenteren van de resultaten als afzonderlijke automatisch (maar complex) proces of het berekenen als handmatige proces. Het maken van handmatige berekeningen borgt de attentie voor het signaleren van verschillen.

i) **Toepassen logistiek model** *(V)* (Bericht) Bij berichtgeoriënteerde verwerkingen en/of meerdere batchuitwisselingen per dag met andere organisaties wordt de volledigheid en tijdigheid van de verwerking beheerst door **logistieke meetpunten en parkeerplaatsen** in het primair proces aan te brengen.

Toelichting 1: Gedurende de productie wordt een waarneming weggeschreven als een geval / zaak dat meetpunt passeert. In het kader van de volledigheidsbewaking heeft elk werkproces aan het begin en eind een **logistiek meetpunt**. Hierdoor kan waargenomen worden of een gevalsbehandeling nog in uitvoering is of afgerond of geannuleerd. Verder zijn logistieke meetpunten nodig voor tijdigheid- en juistheidsbepaling en dienstverlening. Hiervoor moeten logistieke meetpunten geplaatst worden aan het begin en eind van een voorraadpunt en handmatige behandeling van een geval. Aangezien een planning op tactisch niveau gerelateerd is aan de producten en diensten van de organisatie en dus de bedrijfsprocessen, is het ook van belang om in de logistieke meetpunten binnen de werkprocessen identificerende kenmerken van de bedrijfsprocesinstantie en de gevalsbehandeling vast te leggen. Hierdoor kan uiteindelijk de samenhang van de gevalsbehandeling op tactisch niveau zichtbaar gemaakt en bewaakt worden. **Parkeerplaatsen** zijn bewust aangebrachte punten in het proces waar werk tijdelijk vastgehouden kan worden. Vanuit deze punten kan het verloop van het proces en de capaciteitsuitnutting in het bijzonder beïnvloed worden. In het kader van volledigheid is de zendende partij verantwoordelijk voor de logistieke aflevering op de afgesproken locatie volgens de afgesproken kwaliteit tot en met het moment dat de ontvangende partij de ontvangst bevestigd heeft (functioneel, technisch of beiden). De ontvangende partij heeft hierbij ten alle tijden een afnameplicht. Hiermee is de verantwoordelijkheid rondom volledigheid bij één enkele regelkring belegd. Onder partijen verstaan we hier bedrijfsfuncties en/of uitvoerende organisatie onderdelen. Wanneer er een voorraadpunt gepositioneerd is tussen de overgang van de gevalsbehandeling, geldt dezelfde regel. De ontvangende partij is hierbij verantwoordelijk voor het voorraadpunt.

Toelichting 2: Bij programmafouten en herstelverwerkingen bestaat het risico van onvolledige verwerking, zowel bij de eigen organisatie als bij de eventuele ketenpartner. Hierbij moet kunnen worden teruggegaan naar het laatste verwerkingspunt waarover zekerheid bestaat dat de posten goed zijn verwerkt.

C.13.3.5 Bestandscontrole

Beheersmaatregel

Kritische gegevens (bijvoorbeeld identificerende en financiële gegevens), die in verschillende gegevensverzamelingen voorkomen, worden periodiek met elkaar vergeleken.

Toelichting:

Onder deze vergelijkingen vallen in ieder geval financiële gegevens in grootboek en subadministraties en financiële en sleutelgegevens in gegevensverzamelingen die op verschillende platforms voorkomen of door verschillende organisaties worden geëxploiteerd.

Implementatierichtlijn

- Er zijn meerdere alternatieven om aan deze doelstelling te voldoen:
- vergelijk dezelfde kritische gegevens in verschillende gegevensverzamelingen, waarbij verschillen worden gesignaleerd. Wellicht kan hiervoor standaard programmatuur worden gebruikt;
- indien de bestanden dezelfde metadata bevatten kan de controle plaatsvinden met hashtotalen. Bij verschillen zal op record- of occurrence-niveau vergelijking moeten plaatsvinden. De periodiciteit hangt af van de hoeveelheid verschillen, die bij eerdere vergelijkingen zijn geconstateerd dan wel de inschatting van risico's op het kunnen voorkomen van inconsistenties;
- bij afgeleide gegevensverzamelingen, die frequent en integraal worden overschreven door kopieën vanuit een basisgegevensverzameling, is deze vergelijking niet noodzakelijk.

C.13.3.6 Geprogrammeerde controles i.r.t. generieke IT-voorzieningen

Beheersmaatregel

In toepassingsprogrammatuur zijn geen functies werkzaam, waarvoor kwalitatief betere generieke voorzieningen beschikbaar zijn, zoals die voor identificatie, authenticatie, autorisatie, onweerlegbaarheid en encryptie.

Toelichting en afbakening

Deze doelstelling zal doorgaans alleen volledig haalbaar zijn bij maatwerkapplicaties. Bij standaard applicaties / programmapakketten worden dergelijke functies meestal meegeleverd en zijn niet uit te schakelen en te vervangen door eigen generieke functies, hooguit daarmee te synchroniseren. Bovendien kunnen dan tevens andere generieke IB-functies aan de orde zijn.

Implementatierichtlijnen (niet uitputtend)

a) Autorisatiebeheersysteem

Voor het beheer van autorisaties wordt zoveel mogelijk gebruik gemaakt van standaard autorisatievoorzieningen of -modules. Indien dit op onderdelen niet is te vermijden (bijv. bij gegevensafhankelijke autorisatiemechanismen) worden deze functies als aparte module uitgevoerd.

b) (Ver)sterk(t)e authenticatie

Bij het elektronisch communiceren vanuit een niet vertrouwde omgeving (bijv. vanuit de externe zone) kan het noodzakelijk zijn extra zekerheden (boven het basisniveau beveiliging) te verkrijgen omtrent de identiteit van derden. De hiervoor te treffen maatregelen worden afgestemd met het in deze gevoerde beleid en de beschikbare generieke oplossingen.

c) Onweerlegbaarheid juiste ontvanger/verzender

In situaties waar (juridische) geschillen kunnen ontstaan over het al dan niet ontvangen of verzenden van elektronische gegevens van of aan de juiste identiteit, wordt gebruik gemaakt van generieke voorzieningen van een Public Key Infrastructuur.

d) Encryptie

Als encryptie ter borging van vertrouwelijkheid en/of integriteit van gegevens binnen of ten behoeve van een applicatie wordt toegepast, dan gelden hiervoor de normen van de subparagrafen C.13.4.3 Encryptie ten behoeve van zonering, C.13.4.4 Sterkte van de encryptie, C.13.4.5 Vertrouwelijkheid en integriteit sleutels.

e) Dubbele of ontbrekende bestandsuitwisseling

Bij uitwisseling van bestanden tussen centrale en decentrale servers of met externe partijen wordt zeker gesteld dat uitwisseling niet of dubbel plaatsvindt. Een dergelijk filetransfermechanisme is bij voorkeur als generieke voorziening in te richten.

C.13.3.7 Aanvullende normen

Beheersmaatregel

Aanvullende maatregelen boven het basisniveau beveiliging kunnen noodzakelijk zijn om een hoger beveiligingsniveau te bereiken bij extra risicovolle bedrijfsprocessen.

Toelichting

Afhankelijk van de specifieke risico's die kunnen samenhangen met het desbetreffende bedrijfsproces kan het aan de orde zijn extra maatregelen te treffen. De hieronder opgesomde maatregelen zijn als suggestie bedoeld.

Implementatierichtlijnen

a) Aparte applicatietaken

Applicatietaken, die gegevens verwerken met extra (hoog) belang, kunnen van de overige transacties gescheiden worden om functiescheiding op basis van autorisatie mogelijk te maken. In dat geval worden de desbetreffende gegevens als aparte gegevensrubriek gezien, waarvan de rubricering doorwerkt bij alle transacties van de toepassing. Gegevens van te onderscheiden aard kunnen ook

worden opgenomen in aparte bestanden zodat de toegang en verwerking gedifferentieerd kunnen worden.

b) Extra audit trail

Bij applicatietaken met een omvangrijke historie kan meer uitgebreide vastlegging van uitgevoerde activiteiten in de audit trail worden overwogen. Dit kan ook het geval zijn als de applicatie mogelijkheden biedt tot oneigenlijk gebruik van raadpleegbevoegdheden.

c) Controletellingen database

Bij het online verwerken van mutaties in een database kunnen controletellingen van aantallen en bedragen apart worden bijgehouden en gerapporteerd. Frequent vanaf dan gecontroleerd of deze controletellingen in overeenstemming zijn met de daadwerkelijke toestand van de database. Voor deze controle wordt dan een aparte taak gedefinieerd.

d) Gegevenscryptie

Gegevenscryptie op applicatieniveau (database-niveau) is een extra middel om de vertrouwelijkheid en de integriteit van de gegevensuitwisseling of -opslag te waarborgen.

e) Gegevensrubricering tonen

Gegevensrubricering tonen op beeldscherm, output en verwisselbare gegevensdragers en maatregelen met elektronische gegevensuitwisseling. De gebruikers en/of ontvangers dienen op de hoogte te zijn van wat de rubricering betekent voor de behandeling van de gegevens. Organisaties die gerubriceerde gegevens uitwisselen dienen op de hoogte te zijn van de betekenis van die rubricering, hanteren de organisaties een andere naamgeving, dan dienen zij onderlinge afspraken te maken hoe de verschillende naamgevingen op elkaar aansluiten.

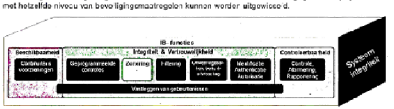
C.13.4. Zonering IT

Doelstelling

De technische infrastructuur is in zones ingedeeld om isolatie van onderdelen hiervan mogelijk te maken.

Definitie

Afbakening van een logisch geheel van de technische infrastructuur waarbinnen gegevens vrijelijk met helzelfde niveau van beveiligingsmaatregelen kunnen worden uitgewisseld.



Toelichting

Het doel van zonering is:

a) het voorkomen of beperken van risico's door isolatie van onderdelen van de technische infrastructuur;

b) het scheiden van onderdelen waaraan verschillende betrouwbaarheidseisen worden gesteld.

Informatie-uitwisseling tussen zones verloopt via koppelvlakken, die de informatiestromen controleren. Hierdoor kunnen bepaalde dreigingen in el optreden dan wel niet doorwerken van de ene zone in de andere. Hierbij gaat het er niet alleen om de interne vertrouwde zone tegen de externe,

onvertrouwde zone te beschermen, maar ook om interne zones (zoals ontwikkeling-, test-, acceptatie- en productie-omgevingen) van elkaar te scheiden.

Zonering maakt het voorts mogelijk om met verschillende beveiligingsniveaus binnen een infrastructuur te werken en informatiestromen en risicovolle beheercommando's te regelen. Zonering als middel om toegang tot voorzieningen te beperken werkt op een hoger schaalniveau dan via bijvoorbeeld toegangsbeveiliging. Zonering maakt het netwerk overzichtelijker voor beheer en dat is tevens van belang voor beveiliging.

Elke zone kent dus andere risico's, die samenhangen met de diensten of IT-voorzieningen die erin opgenomen zijn. Binnen zones kunnen met standaard maatregelen subzones (compartimentering) worden ingericht als het risicoprofiel dat vereist. Bijvoorbeeld om verschillende productieomgevingen uit elkaar te houden, die niet hetzelfde beveiligingsniveau hebben. Externe netwerken worden in dit zoneringsconcept ook als aparte zone gezien.

Aangezien het overgrote deel van de toepassingen van encryptie erop gericht zijn gegevensverlies/-verandering te voorkomen, worden dit type maatregelen onder zonering gepositioneerd.

Motivering

Door zonering kunnen risico's worden gelocaliseerd, waardoor bedreigingen en incidenten die optreden in de ene zone niet doorwerken in een andere zone.

C.13.4.1 Zonering technische infrastructuur

Beheersmaatregel

De indeling van zones binnen de technische infrastructuur vindt plaats volgens een vastgesteld inrichtingsdocument (configuratiecodes) waarin is vastgelegd welke uitgangspunten gelden voor de toepassing van zonering.

Implementatierichtlijnen

a) Er zijn aparte zones voor Ontwikkeling, Test, Acceptatie en Productie.

b) De experimenteer omgeving (laboratorium, sand box) is een fysiek gescheiden zone.

c) Beheer van zones vindt plaats vanuit een eigen zone.

d) IT-voorzieningen (zoals mobiele clients en werkstations) die buiten de fysieke toegangsbeveiliging van de gebouwen van de organisatie zijn opgesteld, worden in de externe zone (externe werkplek) gepositioneerd.

e) Dataservers waarvoor een hoger beveiligingsniveau geldt dan het basisniveau, kunnen in een eigen zone worden opgenomen.

f) Van werkstations wordt bepaald welke onderdelen tot welke zone behoren, ge et op de risico's van het samenvoegd ontsluiten van data via de verschillende soorten poorten. Om deze reden kan lokale opslag van gegevens op de vaste schijven van werkstations (b.v. laptops) en opslag op verwijderbare opslagmedia worden gefaciliteerd.

g) Interne systemen wisselen gegevens uit met ketenpartners en klanten via een centrale interne zone (DMZ) en een vertrouwde, externe zone.

h) Voor de uitwisseling van gegevens met derden (niet openbare gegevens) worden besloten externe zones (vertrouwde derden) gebruikt.

i) In een DMZ worden alleen openbare gegevens van een organisatie opgeslagen, die in het uiterste geval verloren mogen gaan.

j) Vitale bedrijfsgegevens worden in een aparte zone geplaatst.

C.13.4.2 Eisen te stellen aan zones

Beheersmaatregel

Zones zijn voor beveiliging en beheer als eenheid gedefinieerd.

Implementatierichtlijnen

a) Elke zone heeft een vastgesteld, uniek beveiligingsdoel.

b) Elke zone wordt slechts beheerd onder verantwoordelijkheid van één beheerinstantie (m.u.v. onvertrouwde derden)

c) Een zone heeft een gedefinieerd beveiligingsniveau, d.w.z. kent een gedefinieerd stelsel van samenhangende beveiligingsmaatregelen.

d) De maatregelen van logische toegangsbeperking zijn van toepassing op alle IT-voorzieningen in een zone.

e) Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.

f) Zones kunnen worden onderscheiden door gebruikmaking van routering van datastromen verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding.

g) Poorten, die zien op soortgelijke voorzieningen geïnstalleerd op een computer of netwerkvoorziening, die niet specifiek vereist zijn voor de bedrijfsvoering, worden uitgeschakeld of verwijderd.

C.13.4.3 Encryptie ten behoeve van zonering

Beheersmaatregel

De communicatie en de opslag van gegevens die buiten de invloedsfeer van de logische en fysieke toegangsbeveiliging maar wel binnen de eigen beheeromgeving valen of waarvoor deze maatregelen onvoldoende zijn, zijn door encryptie beschermd.

Implementatierichtlijnen

a) Encryptie dient te worden toegepast in de volgende situaties:

1. bij verplaatsbare mediadragers indien deze buiten een beschermde zone worden bewaard (denk bijvoorbeeld aan externe opgeslagen back-up tapes, diskettes, DVD's, CD-ROM's en USB-sticks);

2. het extern geheugen van mobiele apparatuur (denk aan harde schijven van portable workstations en geheugenkaarten in PDA's/smartphones)

3. bij beheersessies over het eigen netwerk (met encryptievoorzieningen binnen de beheertools of gebruikte protocollen);

4. bij datatransport over onvertrouwde netwerkwerken (Internet) of om een hoger beveiligingsniveau te bereiken.

5. bij datatransport via mobiele datadragers buiten de reikwijdte van de fysieke toegangsbeveiliging van een organisatie;

6. bij draadloze datacommunicatie;

7. wachtwoorden, die worden opgeslagen of verzonden;

8. end-to-end encryptie als aanvullende beveiligingsmaatregel kan alleen binnen een zone gebruikt worden ter voorkoming van doorgeven van ongewenste soft- of malware van de ene zone naar de andere. Uitzondering hierop vormt de communicatie tussen werkstations en dataservers.

b) Er is in het kader van de naleving van de relevante overeenkomsten, wetten en voorschriften

rekening gehouden met de beperkingen op de import en/of export van computerapparatuur en -programmatuur die zij in netwerken dat er cryptografische functies aan kunnen worden toegevoegd;

c) Er is in het kader van de naleving van de relevante overeenkomsten, wetten en voorschriften rekening gehouden met de beperkingen op het gebruik van versleutelingstechnieken;

C.13.4.4 Sterkte van de encryptie

Doelstelling

De sterkte van de encryptiemechanismen voldoet aan de eisen van de tijd.

Implementatierichtlijnen

a) De gebruikte cryptografische algoritmen zijn als open standaard per soort toepassing gedocumenteerd en staan als robuust bekend.

b) Hardware-oplossingen (bijv. smart card- en Hardware Security Module producten) zijn gecertificeerd volgens daartoe strekkende standaards.

c) De sleutellengte is instelbaar en voldoende groot om ook in de afzienbare toekomst bestand te zijn tegen succesvolle pogingen om de sleutels te laten achterhalen met inachtneming van het belang van de gegevens, die ermee worden beschermd.

C.13.4.5 Vertrouwelijkheid en integriteit a.u.t.e.l.s

Beheersmaatregel

De vertrouwelijkheid en integriteit van geheime cryptografische sleutels is gewaarborgd tijdens het gehele proces van generatie, transport, opslag en vernietiging van de sleutels.

Implementatierichtlijnen

a) Cryptografische sleutels en certificaten kennen een geldigheidstermijn die is afgestemd op het kritische gehalte van de toepassing met een maximum van 1 jaar.

b) Sessie encryptie met een unieke sessiesleutel heeft de mogelijk de voorkeur boven encryptie met periodiek te wijzigen sleutels. Deze sessiesleutel wordt random gegenereerd, is bij voorkeur symmetrisch en wordt bij voorkeur uitgewisseld met een asymmetrisch algoritme.

c) Generatie en restitutie van private keys, master keys en root certificates vinden plaats binnen een beschermde omgeving van cryptohardware.

d) Deze cryptohardware is tamper-resistant. Dit betekent dat er bijzondere voorzieningen zijn getroffen tegen onbevoegde kennisname van de opgeslagen cryptosleutels bij een fysieke inbreuk op de hardware.

e) Instructieve bediening van cryptohardware vindt plaats volgens het vier-ogen-principe (meerdere personen nodig voor één handeling). Denk hierbij aan installatie, wijzigingen in configuratie en generatie van master keys.

C.13.5. Filtering

Doelstelling

Op het kopvlak tussen zones zijn filterfunctie's gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet toegestane gegevens worden tegengehouden.

Definitie

Controle van informatiestromen op communicatiegedrag, vorm (protocol) en of inhoud van gegevens, afhankelijk van de aard van de informatiestromen en de zones of netwerkknooppunten waar ze vandaan komen of naar toe gaan.

Toelichting

Filtering beschermt zones tegen aanvallen, indringers, ongewenste inhoud en virussen, waardoor diensten onbereikbaar worden of onrechtmatige toegang tot gegevens of systemen wordt verkregen. Filtering controleert geen identiteiten van individuele gebruikers.

De communicatie tussen twee zones kan worden getoetst op ongewenste eigenschappen. Daarvoor wordt een elektronisch profiel vastgelegd van de zenders in de betrokken zones. Van het communicatiegedrag wordt elektronisch een 'reputatie score' vastgelegd, die enerzijds wordt vergeleken met het desbetreffend inrichtingsdocument (configuratiedossier) voor het doorlaten van communicatie en anderzijds met bekende patronen van ongewenste communicatie.

In de situatie dat end to end beveiliging wordt toegepast op berichten of documenten, zal minder filtering noodzakelijk zijn, maar dat tast het zonerings- en filteringsconcept niet aan; het kan wel tot een andere invulling leiden.

In deze versie van document is nog niet gestreefd naar een echt uitgewerkte normering van de filterfunctie, gezien het complexe karakter daarvan. Wel zijn de elementen ervan benoemd. Naar verwachting zal het ontwikkelen van IB-patronen aanleiding vormen de normering aan te passen.

Motivering

Filterfuncties zijn onlosmakelijk verbonden aan de IB-functie 'Zonering' en ontlenen daaraan ook hun motivering.

C.13.5.1 Controle op communicatiegedrag

Beheersmaatregel

Ongewenst communicatiegedrag wordt opgemerkt en geblokkeerd.

Implementatierichtlijnen

a) De filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol en richting van de communicatie. Niet toegestane verbindingen worden geblokkeerd c.q. er wordt verhinderd dat deze tot stand komen.

b) In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en te kunnen blokkeren die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is (denial of service attacks).

c) Al het gegevensverkeer vanuit externe of onvertrouwde zones wordt real-time inhoudelijk geïnspecteerd op inbraakpogingen. Een update van aanvalspatronen vindt frequent plaats.

C.13.5.2 Controle op gegevensuitwisseling

Beheersmaatregel

De gegevensuitwisseling tussen zones wordt naar vorm en inhoud gecontroleerd, waarbij ongewenste gegevens worden geblokkeerd.

1100035 00013

Implementatierichtlijnen

a) De uitvoer van toepassingssystemen waarmee gevoelige informatie wordt verwerkt, wordt alleen verzonden naar computerterminals en locaties met een autorisatie.

b) Versleutelde gegevensstromen van en naar de externe zone worden ontsleuteld voor inhoudelijke controles.

c) E-mail berichten met bijlagen worden uitsluitend doorgelaten op basis van geformaliseerde afspraken over de coderingsvorm (extensie) van de bijlage. Gecontroleerd wordt of de aanduiding van de coderingsvorm klopt met de werkelijke coderingsvorm van de bijlage.

d) Berichten en bestanden met een omvang boven een vastgestelde grenswaarde worden geblokkeerd om problemen wegens onbeschikbaarheid te voorkomen.

e) Er is antivirusprogrammatuur actief die e-mail berichten en webpagina's blokkeert met kwaadaardige code (virussen, wormen, trojans, spyware, etc.) in zowel ontvangen als verzonden e-mails. Een update van antivirusdefinities vindt frequent plaats.

f) Er is een (spam) filter geactiveerd voor zowel ontvangen als verzonden berichten. Een update van het spamfilter vindt frequent plaats.

g) Op alle werkstations en daarvoor in aanmerking komende servers is antivirusprogrammatuur resident actief. Een update van virusdefinities en/of antivirusprogrammatuur kan op ieder moment (handmatig) uitgevoerd worden en vindt periodiek of bij concrete dreigingen geautomatiseerd plaats.

h) In een keten van zones binnen een organisatie wordt antivirusprogrammatuur van verschillende leveranciers toegepast.

C.10.6. Onweerlegbaarheid berichtuitwisseling

Doelstelling

Bij berichtuitwisseling wordt de onweerlegbaarheid van verzending en ontvangst geborgd.

Definitie

Onweerlegbaarheid van elektronische berichtuitwisseling houdt in dat:

- De zender van een bericht niet kan ontkennen een bepaald bericht verstuurd te hebben;
  - De ontvanger van een bericht niet kan ontkennen het bericht van de zender in de oorspronkelijke staat te hebben ontvangen.

Toelichting

De onweerlegbaarheid kan op twee wijzen verkregen worden:

- over een onvertrouwd netwerk: d.m.v. een Public Key Infrastructure (PKI);
- over een besloten netwerk via een betrouwbare berichtendienst.

De onweerlegbaarheid via PKI kan verkregen worden door middel van wederzijdse authenticatie van zender en ontvanger aangevuld met controle op de integriteit van het bericht. Hiermee wordt een bericht onweerlegbaar verstuurd. Dit wordt ook wel non-repudiation genoemd. Dit kan met behulp van een zogenoemde elektronische handtekening, die toepasbaar is als wettelijk bewijs mits voldaan

wordt aan eisen in de Wet Elektronische Handtekening (WEH).

In het algemeen valt het "zetten" van de digitale handtekening uiteen in twee delen, die tot een unieke relatie leidt tussen het bericht in de handtekening:

Vastleggen van de unieke kenmerken van het bericht (in een "hash").

Verbinden van de unieke identiteit van de zender aan de hash.

Het zetten van een digitale handtekening kan plaatsvinden met verschillende methoden, waarvan de twee bekendste zijn:

- Symmetrische cryptografische sleutels = vooraf uitgedeeld door regiepartij.
- Asymmetrische cryptografie o.b.v. PKI = uitgedeeld door vertrouwde derde.

Bij een Public Key Infrastructure (PKI) worden twee encryptiesleutels toegepast: een publieke sleutel en een geheime, private sleutel. De publieke sleutel wordt opgenomen in het certificaat, uitgegeven door een (derde) vertrouwde partij. De private sleutel wordt bewaard en gebruikt door de persoon of instelling, van wie het certificaat is. Deze sleutels zijn nodig voor versleuteling én ontsleuteling. Deze sleutels hebben een unieke wiskundige relatie met elkaar. Hierdoor kunnen ze in combinatie met de betreffende certificaten gebruikt worden voor authenticatie en het versturen van geheime (sleutel-) informatie over een onvertrouwd netwerk.

Motivering

Als er geen specifiek daarop afgestemde maatregelen zijn, wordt het risico gelopen dat een ontvanger van een bericht kan ontkennen ooit een bericht te hebben ontvangen of kan ontkennen een bericht te hebben ontvangen met de inhoud zoals deze door de verzender is verstuurd. In het elektronisch berichtenverkeer zijn aanmerkelijk meer risico's in deze te onderkennen dan in het fysieke postverkeer.

Beheersmaatregel

Bij berichtuitwisseling waaruit rechten en plichten ontstaan tussen partijen bestaat de zekerheid dat het ontvangen bericht afkomstig is van de verzender en dat de inhoud niet door derden is beïnvloed.

Implementatierichtlijnen

Onweerlegbaarheid kan worden verkregen op twee verschillende wijzen:

a) Een betrouwbare berichtendienst in het besloten netwerkverkeer, waarbij verzending en ontvangst van berichten bevestigd wordt door de berichtendienst dan wel hiervoor in de applicaties extra functies op te nemen.

Of bij een onvertrouwd netwerk:

b) Een PKI voldoet aan de daarvoor geldende standaarden, bij de overheid die van de PKI-Overheid.

c) De elementen die het bewijs vormen van een elektronische handtekening, worden in de vorm van een juridisch logbestand zodanig samen met de originele data bewaard, dat datzelfde bewijs in de normale werkstroom van het bedrijfsproces altijd weer is te reproduceren.

d) De ontvangen berichten worden onmiddellijk na ontvangst in de juridische logging vastgelegd, voordat enige bewerking met toepassingssoftware aan de orde is.

e) De verzonden berichten worden in de laatste fase van verwerking onmiddellijk voordat verzending plaatsvindt in de juridische logging vastgelegd.

f) Voor de juridisch logging gelden dezelfde implementatierichtlijnen als voor logging.

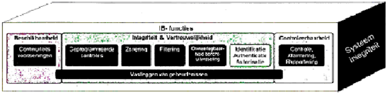
C.13.7. Identificatie, Authenticatie en Autorisatie

Doelstelling van de IB-functie

Logische toegangscontrole vindt plaats voordat IT-voorzieningen kunnen worden gebruikt.

Definities

Logische toegangscontrole door middel van Identificatie, Authenticatie, Autorisatie draagt ervoor zorg dat een persoon, organisatie of IT-voorziening uitsluitend gebruik kan maken van geautomatiseerde functies, waarvoor deze door middel van een aanvraagproces toegangsrechten heeft verkregen.



Toelichting

Deze functie bestaat uit drie afzonderlijke subfuncties en wordt in samenhang met de hier niet-beschouwde Beheersmaatregelen ook wel aangeduid met Identity and Access Management (IAM)

De begrippen voor de drie subfuncties zijn als volgt toe te lichten:

- Identificatie is het bekend maken van de identiteit van personen, organisaties of IT-voorzieningen: wie ben je?
- Authenticatie is het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft: ben je het ook echt? Authenticatie noemt men ook wel verificatie van de identiteit.
- Autorisatie is het controleren van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in IT-voorzieningen: mag je de gevraagde functies of gegevens wel benaderen en wat mag je ermee doen: uitvoeren, raadplegen of ook muteren?

Identificatie en Authenticatie wordt vrijwel altijd in combinatie met elkaar gebruikt. Autorisatie is een meer op zichzelf staande subfunctie, die qua implementatie in de IT geheel eigen consequenties heeft.

Motivering

Het kunnen handhaven van functiescheiding, de herleidbaarheid van handelingen en het beperken van de toegang tot gegevens behoren tot de belangrijkste maatregelen van informatiebeveiliging. Identificatie, authenticatie en autorisatie zijn de functies waarmee aan deze doeleinden invulling kan worden gegeven.

C.13.7.1 Identificatie

Beheersmaatregel

Alle toegangsvragers (gebruikers) tot een geheel van IT-voorzieningen zijn uniek herleidbaar tot één natuurlijk persoon, organisatie of IT-voorziening.

Implementatierichtlijnen

a) Natuurlijk personen, organisaties of IT-voorzieningen worden geïdentificeerd door een unieke identificatie.

b) Vrijgesteld van identificatie zijn gebruikers met toegang tot systemen die alleen publieke of binnen een organisatie algemeen toegankelijke informatie ontsluiten.

c) Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.

d) IT-systemen bieden de mogelijkheid dat beheerders beheerwerkzaamheden uitvoeren onder hun eigen persoonsgebonden gebruikersnaam. In de operatie worden beheerwerkzaamheden en werkzaamheden als gewone gebruiker onder twee verschillende gebruikersnamen uitgevoerd.

e) Het gebruik van speciale beheer accounts (root, administrator) is uitgeschakeld, als gebruik ervoor volledig is meet herleidbaarheid, doelbinding en onweerlegbare logging gecombineerd toegepast worden.

G.13.7.2 Authenticatie

Beheersmaatregel

Alvorens een systeem toegang verleent, wordt de identiteit van de gebruiker of ander subject dat om toegang vraagt, vastgesteld door middel van authenticatie.

Implementatierichtlijnen

a) Bij het intern gebruik van IT-voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.

b) In de volgende situaties vindt authenticatie van gebruikers plaats op basis van cryptografische technick, 'hardware tokens' of een 'challenge/response'-protocol:

1. Single Sign On;
2. toegang vanuit een onvertrouwde omgeving;
3. bij beheer van kritische beveiligingsvoorzieningen (denk bijvoorbeeld aan Hardware Security Modules, firewalls, Intrusion Detection and Prevention Systems en routers).

c) Bij het niet-dagelijks beheer van kritische beveiligingsvoorzieningen vanuit een vertrouwde omgeving is het vier ogen principe een alternatief voor 2.b (dat wil zeggen: dat er altijd twee functionarissen nodig zijn om een handeling uit te voeren).

d) Een mobiel apparaat (zoals een laptop, handheld computer, smartphone, PDA) vraagt om een pincode of wachtwoord bij het inschakelen.

e) Bij telewerken, beheer op afstand en mobiel werken (een mobiel apparaat dat draadloze verbindingen met IT-voorzieningen van de organisatie) wordt vastgesteld tot vaarf een voor dit doelsinde beschikbaar gestelde werkplek wordt gewerkt.

f) Wachtwoordbestanden worden gescheiden opgeslagen van gegevens van de toepassing.

G.13.7.3 Wachtwoordconventies

Beheersmaatregel

Bij authenticatie op basis van kennis dwingt het systeem het toepassen van sterke wachtwoordconventies af.

Implementatierichtlijnen

a) Wachtwoorden voldoen aan de volgende wachtwoordconventies:

1. minimaal acht tekens;
2. minimaal één hoofdletter;
3. minimaal 4 kleine letters;
4. minimaal 1 cijfer en/of één vreemd teken;
5. nieuw wachtwoord moet in minimaal twee tekens verschillen met het vorig wachtwoord.

b) Wachtwoorden van gebruikersaccounts moeten minimaal elke 90 dagen gewijzigd worden.

c) Wachtwoorden van functionele accounts worden minder frequent gewijzigd, namelijk minimaal eens per jaar en ten minste elke nieuwe release van de IT service, maar daarentegen zijn de wachtwoorden langer, namelijk minimaal 20 posities, met willekeurig gekozen cijfers, tekens en speciale tekens.

d) De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij gebuik

het volgende:

1. Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd;

2. Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure;

3. Alvorens een nieuw wachtwoord wordt gewijzigd, wordt geautomatiseerd gecontroleerd of het nieuwe wachtwoord aan de vereiste conventies voldoet.

e) De default en installatiewachtwoorden worden tijdens of direct na installatie verwijderd of gewijzigd.

f) Initiële wachtwoorden en wachtwoorden die gereset zijn, voldoen aan bovenstaande wachtwoordconventie en daarbij wordt door het systeem afgedwongen dat bij het eerste gebruik dit wachtwoord wordt gewijzigd.

C.13.7.4 Instellingen aanmelden op een IT-voorziening

Beheersmaatregel

Instellingen met betrekking tot het aanmelden op een IT-voorziening zijn er op gericht te voorkomen dat iemand werkt onder een andere dan de eigen gebruikersnaam.

Implementatierichtlijnen

a) Er wordt zoveel mogelijk voorkomen dat gebruikers zich op de verschillende IT-voorzieningen in dezelfde keten opnieuw aan moeten melden. Als dit niet mogelijk is, dan wordt het aanmeldproces zo veel mogelijk enkelvoudig ingericht.

b) Expiratiedatums van accounts zijn afgestemd op de einddatum van de contracten van de medewerkers.

c) Op het aangebruikte platform wordt gebruik gemaakt van schermbeveiligingsprogrammatuur (een screensaver) die na 30 minuten alle informatie op het beeldscherm onleesbaar maakt. Het is toegestaan dat het systeem zo geconfigureerd wordt, dat binnen een toegestane periode van enkele seconden de gebruiker door een muisbeweging of toetsenbordaanslag kan verhinderen dat de schermbeveiliging wordt geactiveerd. Het systeem biedt de gebruiker ook zelf de mogelijkheid om de schermbeveiliging op eenvoudige wijze te activeren. Het systeem is zo ingesteld dat na het activeren van de schermbeveiliging de gebruiker zich opnieuw moet authenticeren (de identificatie mag zichtbaar blijven).

d) Nadat voor een gebruikersnaam 6 keer een foutief wachtwoord is gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Ind en er geen lock-out periode ingesteld kan worden, den wordt het account geblokkeerd, totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te wijzigen.

e) Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven van het wachtwoord. Het is wel gebruikelijk dat toetsaanslagen worden weergegeven door sterretjes of bullets.

f) Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.

g) Voor het inloggen vanuit een niet-vertrouwd netwerk wordt een maximumtijd van 10 minuten en een minimumtijd van 10 seconden vastgesteld, indien deze tijd wordt overschreden, betekent het systeem het inlogproces.

h) Netwerksessies worden na een vastgestelde periode van inactiviteit afgesloten. De duur van de periode tot de time out is afgestemd op de vertrouwdheid van de zone (intern of extern), de gevoeligheid van de informatie die wordt verwerkt en de toepassingen die worden gebruikt.

i) Voordat een geslaagde aanmelding op een systeem heeft plaatsgevonden toont het systeem uitsluitend informatie die noodzakelijk is voor de aanmelding, bij een foutieve aanmelding wordt niet vermeld of de gebruikersnaam bestaat, maar slechts dat de combinatie gebruikersnaam en

wachtwoord onjuist was, nadat alle gegevens voor het inloggen zijn ingevuld. Er wordt bovendien geen geheugensteun voor het wachtwoord getoond.

j) Zodra een inlogproces succesvol is voltooid, worden de datum en tijd van de voorgaande succesvolle login getoond.

k) Automatisch aanmelden is niet toegestaan voor interactieve gebruikers. Hier wordt bedoeld dat automatisch wordt ingelogd zonder dat binnen de sessie door een gebruiker een wachtwoord wordt ingegeven (bijvoorbeeld het gebruik van 'Windows Auto Log-on mag dus niet, waarbij door het aanzetten van een PC een gebruiker automatisch wordt ingelogd onder een vooraf opgegeven gebruikersnaam met een vooraf opgegeven wachtwoord). Alleen systeemprocessen met functionele accounts mogen binnen een zone geautomatiseerd aanloggen.

C.13.7.5 Autorisatie

Beheersmaatregel

Autorisaties zijn ingesteld op basis van ontwerp- of systeemdocumentatie, waarin aangegeven is welke rechten in welke gebruikersgroepen worden ondergebracht.

Toelichting en afbakening

De IB-subfunctie autorisatie wordt hier beschouwd vanuit het perspectief van de verantwoordelijkheid van de technisch beheerder. De feitelijke inhoud van de autorisaties is een verantwoordelijkheid van procesontwerpers en functioneel beheerders, rollenbeheerders, ondersteunende functies bij het aanvragen van autorisaties door lijnmanagers.

Implementatierichtlijnen

a) De technische implementatie van autorisaties naar autorisatiegroepen is in overeenstemming met de ontwerp- of systeemdocumentatie.

b) Speciale (systeem)bevoegdheden zijn in aparte autorisatiegroepen opgenomen.

c) Bij het koppelen van gebruikers aan autorisatiegroepen kunnen aangegeven onverenigbaarheden worden gesignaleerd.

C.13.7.6 Minimaliseren rechten

Beheersmaatregel

IT-voorzieningen zijn met zo min mogelijk toegangsrechten ingesteld.

Implementatierichtlijnen

a) In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden. De toegangsregels worden zo fijnmazig als mogelijk ter beschikking gesteld, afhankelijk van de mogelijkheden van de IT-voorziening en de daardoor veroorzaakte beheerslast. Zo kunnen bij schrijfrechten vaak rechten voor creëren (zoals create/insert/generate), wijzigen (zoals update/change/alter) en verwijderen (zoals delete/drop/purge) separaat worden toegekend. Standaard gebruikers krijgen geen execute-rechten.

b) De toekenning van rechten aan processen en bestanden is zo minimaal mogelijk. Bijvoorbeeld:

1. als het platform toestaat om gescheiden executie- en leesrechten toe te kennen, dan worden voor programmabestanden geen leesrechten toegekend;
2. tijdelijke (spool)bestanden (bijv. printgegevens) zijn alleen voor systeembeheer toegankelijk;
3. er worden geen of anders zo weinig mogelijk rechten gegeven aan standaard groepen en accounts, zoals "guest", "public" of "everyone".

c) Toepassingen mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user). Denk

bijvoorbeeld aan een daemon die onder root een poort opent en daarna terugschakelt naar usernveau. Een ander voorbeeld is het gebruik het Substitute User commando. Dit wordt alleen gebruikt voor die delen van een proces die bijdelijk onder hogere rechten draaien om te voorkomen dat beheerders voortdurend met de hoogste systeemrechten moeten werken

c) De taken die met (tijdelijk) hogere rechten uitgevoerd worden, vormen niet onderbroken of afgebroken worden met als gevolg dat deze hogere rechten voor andere doeleinden gebruikt kunnen worden (feitelijk misbruikt kunnen worden).

C.13.7.7 Tegengaan onbedoeld gebruik autorisaties

Beheersmaatregel

Er zijn maatregelen getroffen die onbedoeld gebruik van toegekende autorisaties voorkomen.

Implementatierichtlijnen

a) Gebruikers krijgen geen algemene commando-omgeving tot hun beschikking (bijvoorbeeld een Dos-prompt of Unix-shell).

b) Beheertaken verlopen zoveel mogelijk via een menusysteem en gestandaardiseerde werkwijzen (scripts).

c) Bij het overnemen van werkstations door beheerders om te kunnen meekijken op het werkstation wordt technisch afgedwongen dat hiervoor eerst toestemming aan de gebruiker wordt gevraagd. De gebruiker kan op elk moment de verleende toestemming intrekken.

d) Systeemdata, programmatuur en toepassingsgegevens zijn van elkaar geschaden, dat wil zeggen dat de bestanden zoveel mogelijk in eigen directory's of partities geplaatst worden.

e) Er zijn in productiezones geen hulpmiddelen toegankelijk die het systeem en logische toegangsbeveiliging doorbreken of de integriteit van de productieverwerking kunnen aantasten, zoals ODEC, bestandsviewers, editors, ontwikkelcode, compilers, tekstverwerkingsprogramma's en **eventuele andere systeemhulpmiddelen.**

f) Gebruikers hebben verschillende gebruiksprofielen voor operationele en proefsystemen, en de menu's tonen de juiste identificatieboodschappen om het risico van fouten te verminderen.

g) Wachtwoorden worden versleuteld over een netwerk verzonden.

h) Opgeslagen wachtwoorden worden altijd met een one-way hashfunctie versleuteld.

i) Besturingsprogrammatuur heeft de mogelijkheid zowel programma-, netwerk- als gebruikerssessies af te sluiten.

j) Er worden vooraf gedefinieerde perioden ('time slots') gebruikt, bijvoorbeeld voor overdracht van groepen bestanden ('batch file transfer') of met regelmatig tusserpoozen terugkerende interactieve sessies van korte duur.

k) Authentificatieprocedures worden herhaald op basis van het **hiervoor** opgestelde **beleid.**

l) Werkstations die niet in gebruik zijn, worden tegen **onbevoegd** gebruik beveiligd met behulp van een toetsvergrendeling of vergelijkbare beveiliging, bijvoorbeeld een wachtwoord.

C.13.7.8 Beheersbaarheid autorisaties

Beheersmaatregel

Verleende toegangsrechten zijn inzichtelijk en beheersbaar.

Implementatierichtlijnen

a) De registratie van gebruikers en verleende toegangsrechten is zoveel mogelijk centraal geregeld (single-point-of-administration)

b) Toegangsrechten worden zoveel mogelijk via groeperingmechanismen (bijv. t.b.v. RBAC)

toegekend (dus niet rechtstreeks aan individuele gebruikers). Uitzonderingen vergen extra aandacht bij het beheer.

c) Voor groeperingsmechanismen geldt een naamgevingsconventie, die aansluit op zo stabiel mogelijke uitgangspunten (dus zo min mogelijk afdelingsgebonden als er regelmatig organisatiewijzigingen plaatsvinden).

C.13.7.8 Volledigheid toegangsbeveiliging

Beheersmaatregel

Op alle IT-voorzieningen is toegangsbeveiliging van toepassing.

Implementatierichtlijnen

a) Toegangsbeveiliging is geïmplementeerd op alle middelen die gegevens bevatten of verwerken. Dit betreft onder meer de volgende middelen:

1. platforms (vaste en mobiele werkplek, server, mainframe): bestanden, directory's, services en aanvullingsmateriaal (denk aan USB-devices op de werkplek);
2. ondersteunende systemen: services;
3. primaire systemen: taken/functies in applicaties, stored procedures, gegevensbeheersing in databases (views, tabellen, velden, records);
4. beheer: beheer van appliances en firmware van hardware voorzover dit kan. Mogelijk is er geen functionaliteit om de toegang tot firmware met een rechtenstructuur te beveiligen. We dient in ieder geval een wachtwoord te zijn ingesteld.

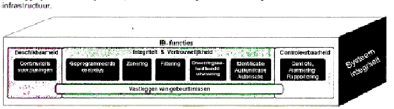
C.13.8. Vastleggen van gebeurtenissen

Doelstelling van de IB-functie

Handelingen in en meldingen van IT-voorzieningen in de technische infrastructuur worden vastgelegd in logging.

Definitie

Vastlegging van handelingen van personen en meldingen met betrekking tot de technische infrastructuur.



Toelichting

Een andere term voor het vastleggen van gebeurtenissen van de technische infrastructuur is logging. Voorbeelden van handelingen door natuurlijke personen zijn het wijzigen van parameters. Een foutmelding door een voorziening van de technische infrastructuur is een voorbeeld van een gebeurtenis.

Het terugvindbaar vastleggen van gebeurtenissen is noodzakelijk om achteraf controle te kunnen uitoefenen en/of fouttoestanden te kunnen uitzoeken. Het vastleggen is tevens noodzakelijk als bewijsmiddel voor private of strafrechtelijke vordering.

Veel gebeurtenissen die voor het beheer van de technische infrastructuur van belang zijn, hebben tevens betekenis in het kader van informatiebeveiliging.

Logging moet niet verward worden met het begrip audit trail, dat betrekking heeft op het vastleggen van het verwerkingsproces door toepassingsprogrammatuur. Dit begrip wordt verder uitgewerkt bij de IO-functie 'Deprogrammeerde controles'.

Motivering

Het vastleggen van meldingen van besturingsprogramma's en andere systemen in de technische infrastructuur is noodzakelijk om achteraf controle te kunnen uitoefenen en/of foutsituaties te kunnen uitvoeken. Het vastleggen is tevens noodzakelijk als bewijsmiddel voor private- of strafrechtelijke vordering.

C.13.8.1 Aanmaken logbestanden

Beheersmaatregel

In de logging wordt informatie vastgelegd waarmee is te produceerbaar is wie waar en wanneer welke handelingen heeft verricht.

Toelichting

Logbestanden bevatten vaak een grote hoeveelheid informatie, waarvan een groot deel irrelevant is voor de controle van de beveiliging. Om gebeurtenissen te identificeren die significant zijn voor de controle van beveiliging, wordt overwogen het juiste type berichten automatisch naar een tweede logbestand te verplaatsen, en/of bepaalde systeemhulpprogramma's of audit-hulpmiddelen voor bestandsonderzoek en -rationalisatie te gebruiken.

Implementatierichtlijnen

a) De volgende uitgevoerde handelingen worden in ieder geval opgenomen in de logging:

1. gebruik van technische beheerfunctie en systeemhulpmiddelen, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore, (tijdelijke) toekenning en uitoefening van hogere dan gebruikelijk rechten (incl. van collega's verricht met gepriviligieerde accounts, zoals root, supervisor, praddos etc.);

2. gebruik van functionele beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit; ingrepen in gegevenssets waarender databases;

3. handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels;

4. beveiligingsovertredingen (zoals de constatering van een virus, worm, Trojans paard of andere malware, een pentest of testen op zwakheden, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services);

5. verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken bijkans uitvoering van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen);

6. handelingen van gebruikers, zoals verleende toegangsrechten, gebruik van on-line transacties en toegang tot bestanden door systeembeheerders.

b) In een te schrijven logregel wordt in ieder geval weggeschreven:

1. de naar een natuurlijke persoon herleidbare gebruikersnaam die verzocht een handeling uit te voeren;

2. het soort handeling, het gegevan commando met de parameters;

3. waar mogelijk de identiteit van het werkstation of de locatie;

4. het middel waarop de handeling werd uitgevoerd of waar een event optrad;
5. het resultaat van de handeling indien dit niet uit het soort handeling is af te leiden;
6. de datum en het tijdstip van een handeling of event;
7. de severity-aanduiding: het beveiligingsbelang, waarop selectie t.b.v. de analyse kan plaatsvinden.

c) Systeemklokken worden tijdens openstelling gesynchroniseerd en worden gelijk gezet met een atoomklok op basis van het Network Time Protocol (NTP), zodat de juiste tijd in het logbestand vastgelegd kan worden. Een indicatie voor de synchronisatiefrequentie is 4 uur. De maximale afwijking ten opzichte van de standaardtijd is 100 milliseconden.

c) In een te schrijven logregel worden in geen geval gegevens opgenomen waardoor de beveiliging doorbroken kan worden (zoals wachtwoorden, pincodes).

C.13.8.2 Integriteit logbestanden

Beheersmaatregel

De integriteit van opgeslagen logbestanden is gewaarborgd.

Implementatierichtlijnen

a) Bij het schrijven en opslaan van logregels wordt zoveel mogelijk gebruik gemaakt van hiervoor ingerichte generieke beveiligingsvoorzieningen.

b) Bij het aanleggen van logbestanden wordt zo mogelijk gebruik gemaakt van "write once"-technologie.

c) De volledigheid van de logging kan worden vastgesteld, bijvoorbeeld met behulp van opeenvolgende nummers per log-event.

d) Uitsluitend geautoriseerde processen (operationeel onder een functioneel account) mogen logregels schrijven.

e) Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers, waarbij de toegang is beperkt tot leesrechten.

f) Beheerders zijn niet in staat de instellingen van de logging te wijzigen of logbestanden te verwijderen, tenzij het specifiek hiervoor bevoegde beheerders zijn. Wanneer een systeem een specifieke rol voor auditdoeleinden kent, dan wordt hiervan gebruik gemaakt bij het raadplegen.

C.13.8.3 Beschikbaarheid logbestanden

Beheersmaatregel

De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht.

Implementatierichtlijnen

a) Loginformatie wordt bewaard totdat de bewaartermijnen verstreken zijn. Een indicatie voor de bewaartermijn is:

1. een transactie log wordt bewaard totdat is vastgesteld dat de juiste en volledige verwerking van de (batch) transactie(s) heeft plaatsgevonden of totdat de mogelijkheid om een roll-back uit te voeren is verstreken, veelal maximaal één dag;
2. een technische log wordt bewaard totdat is vastgesteld dat er zich geen verstoring in het systeem heeft voorgedaan, veelal maximaal enkele dagen tot een week;
3. logging die van belang is voor auditing en onderzoek naar onelgenlijk gebruik wordt 2 jaar bewaard en wel zolang als de gerechtelijke procedure duurt waarvoor de loggegevens als bewijsmateriaal dienen.

b) Er zijn query- en analysetools aanwezig voor het kunnen ontsluiten van loginformatie.

c) Het overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.

d) Het vollopen van het opslagmedium voor de logbestanden wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie; bij kritische toepassingen leidt het vollopen van het logbestand tot het stilzetten van de verwerking totdat nieuwe ruimte voor loggegevens beschikbaar is. Het volgelopen opslagmedium wordt pas weer vrijgegeven nadat de logbestanden zijn zekergesteld (op een ander medium).

e) Bij onderhoud op analyse- en raadpleegvoorzieningen voor een logbestand wordt achterwaartse compatibiliteit afgedwongen. Dit wil zeggen dat ook de eerder aangelegde logbestanden binnen de bewaartermijn van het logbestand met de nieuwe of gewijzigde voorziening ontsloten kunnen worden.

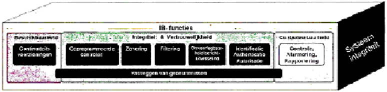
C.13.9. Controle, alarmering en rapportering

Doelstelling

In de technische infrastructuur zijn signaleringsfuncties werkzaam ter controle op vastgestelde inrichtingsdocument (configuratiedossier).

Definitie

Functies die erop gericht zijn te kunnen vaststellen dat de IT-voorzieningen overeenkomstig het vastgestelde inrichtingsdocument (configuratiedossier) functioneren en die signaleren wanneer dit niet het geval is of kan worden.



Toelichting

De tooling die in de markt verkrijgbaar is, maakt het mogelijk al deze functies geïntegreerd te behandelen. Zonder integratie zijn deze functies niet effectief te beheersen. Om die reden worden de hier bedoelde signaleringsfuncties als één geheel behandeld.

De signaleringsfuncties zijn als volgt afzonderlijk toe te lichten:

- Controle is de toets of een IT-voorziening is ingesteld conform een vastgesteld inrichtingsdocument (configuratiedossier).
- Alarmering is een functie, die onmiddellijk signalen naar systeembeheerders kan afgeven als grenswaarden van het vastgestelde inrichtingsdocument (configuratiedossier) worden overschreden.
- Rapportering maakt het mogelijk beveiligingsincidenten, zoals hacking (ook van binnenuit) te onderkennen op basis van analyse en correlatie van vastleggingen.

Motivering

Op basis van de signaleringen kunnen beheerders acties ondernemen om verstoringen in de productieverwerking te voorkomen of om beveiligingsrisico's in de werking van een infrastructuur te kunnen beheersen.

C.13.9.1 Controle op beveiligingsinstellingen

Beheersmaatregel

Instellingen van functies die voor de informatiebeveiliging van belang zijn en wijzigingen daarin worden automatisch gecontroleerd.

Implementatierichtlijnen

a) Bij automatische controle op beveiligingsinstellingen wordt het inbrengen van het Soll-bestand voor beveiligingsinstellingen gescheiden van andere systeemfuncties.

b) Instellingen van IB-functies, die betrokken zijn bij filtering kunnen automatisch op wijzigingen worden gecontroleerd en gealarmeerd.

C.13.9.2 Automatische signalering

Beheersmaatregel

Tevoren gespecificeerde, afwijkende gebeurtenissen volgens de loginformatie worden tijdig gesignaleerd en zo nodig gealarmeerd.

Implementatierichtlijnen

a) Er is gespecificeerd welke beveiligingsincidenten kunnen optreden. Deze beveiligingsincidenten zijn geclassificeerd naar ernst en urgentie.

b) Instelbaar is bij welke drempelwaarden (gebaseerd op de ernst en urgentie van een gebeurtenis daarbij rekening houdend met hoe vaak een gebeurtenis voorkomt) een melding wordt gegeven die direct zichtbaar is voor de beheerorganisatie.

c) Instelbaar is bij welke drempelwaarden de beheerorganisatie wordt gealarmeerd, zonodig ook buiten kantooruren.

d) De IB-functies voor Filtering en Logische Toegangsbeveiliging sluiten aan op de generieke beveiligingsvoorziening voor Security Incident en Event Management (SIEM) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven kunnen worden

C.13.9.3 Analyse en rapportage

Beheersmaatregel

Logbestanden worden periodiek geanalyseerd en gecorreleerd ten einde beveiligingsincidenten dan wel de juiste werking van het systeem te detecteren.

Implementatierichtlijnen

a) Periodiek worden er automatisch correlaties en rapportages gemaakt over de verschillende vastgelegde gebeurtenissen.

b) Periodiek worden er trendanalyses vervaardigd en gerapporteerd over relevante gebeurtenissen in de logbestanden van een in te stellen periode.

C.13.10. Systeemintegriteit

Doelstelling

In de technische infrastructuur zijn functies werkzaam, die de systeemintegriteit ondersteunen

Definitie

Het foutloos uitvoeren van de beoogde bewerkingen door de technische infrastructuur.

Toelichting

De factoren die in samenhang het feitelijke uitoefenen van gezaghebbende bevelingen bepalen zijn legio en als geheel niet logisch onder te brengen onder één van de andere IB-functies. Factoren zijn o.a.: bugs in programmatuur, het bestaan van ongewenste applicaties- en infrastructurele functies, de juiste of onterechte configuratie instellingen van programmatuurpakketten en voorzieningen van de technische infrastructuur, tijdelijke deployment (functionele configuratie) van applicaties en/of infrastructuur.

Afbakening

De scope van de hieronder genoemde maatregelen is voor zover niet door andere functies bepaald, beperkt tot controlemechanismen op de actualiteit van de code, de integriteit van programmapakketten en infrastructurele programmatuur en mechanismen tot beheersing van mobiele code en tenslotte overige instellingen voor "hardening" van systemen. In de maatregelen is (nog) geen uitwerking gegeven aan normen voor weborgtevingen.

Motivatie

In de huidige technologie neemt een aantal risico's, die onder de noemer van systeemintegriteit als kapstokbegrip als IB-functie zijn aangemerkt. De maatregelen geschikt zijn aan de praktijk ontleend.

C.13.10.1 Handhaven technische functionaliteit

Beheersmaatregel

De door de leverancier bepaalde technische functionaliteit van programmapakketten en infrastructurele programmatuur blijven gehandhaafd.

Toelichting en afbakening

In dit document worden voor de onderkende IB-functies normen geformuleerd, die doels bepalend zijn voor de instellingen van infrastructurele elementen van IT-voorzieningen. Het is echter niet mogelijk om voor alle beveiligingsrelevante instellingen productonafhankelijke normen te formuleren. Daarom blijft het noodzakelijk om alle overige instellingen op bevelligingsaspecten te beoordelen.

Implementatierichtlijnen

a) De technische integriteit van programmapakketten en infrastructurele programmatuur wordt gecontroleerd d.m.v. een hashingmechanisme en een controlegetal van de leverancier, dat via een vertrouwd kanaal is verkregen.

b) Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructurele programmatuur.

c) De instellingen (parametrisatie) van programmapakketten en infrastructurele programmatuur zijn in overeenstemming met een vastgestelde inrichtingsdocument (configuratiedossier), dat is gebaseerd op aanbevelingen van de leveranciers, operationele productiestandaards van de voorkeur onafhankelijke instellingen, zoals die van NIST, voor zover de instellingen niet door de andere IB-functies van dit document zijn geadresseerd.

d) Instellingen van programmapakketten en infrastructurele programmatuur kunnen geautomatiseerd worden gecontroleerd op configuratiewijkingen van het vastgestelde inrichtingsdocument.

e) Van programmapakketten en infrastructurele programmatuur kan bij voorkeur geautomatiseerd gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd.

f) Het automatisch doorvoeren van een update vindt alleen plaats als hiervoor specifieke afspraken zijn gemaakt met de leverancier.

g) Van programmapakketten en infrastructurele programmatuur kan bij voorkeur geautomatiseerd gecontroleerd worden of er bekende zwakheden in de configuratie voorkomen.

C.13.10.2 Systeemhulpmiddelen

Beheersmaatregel

Het gebruik van hulpprogrammatuur waarmee maatregelen in systeem- en toepassingssoftware zouden kunnen worden gepasseerd, wordt zeveel mogelijk beperkt.

Implementatierichtlijn

a) Identificatie-, authentictie- en autorisatiemechanismen zijn ook voor systeemhulpmiddelen van toepassing.

b) Systeemhulpmiddelen en toepassingsprogrammatuur zijn gescheiden.

c) Onnodige hulpprogramma's en systeemprogrammatuur zijn verwijderd.

C.13.10.3 Hardering

Beheersmaatregel

Infrastructurele programmatuur, die vitale bevelligingsfuncties vervullen, bevatten geen onnodige en ongebruikte functies.

Toelichting

Vitale beveiligingsfuncties hebben hier betrekking op infrastructurele voorzieningen, die de zonering bepalen, deel uitmaken van de beheer en audit zone en van de zone waar de data van de bedrijfstoepassingen worden opgeslagen.

Afbakening

Voor het 'hardenen' van infrastructurele IT-voorzieningen moet tevens worden voldaan aan de andere normen voor deze voorzieningen. Bij applicaties wordt ervan uitgegaan dat de onderliggende beveiligingssystemen reeds geharderd zijn.

Implementatierichtlijn

a) Onnodige en ongebruikte functies van infrastructure e programmatuur zijn uitgeschakeld.

b) Beheermogelijkheden zijn zoveel mogelijk afgesloten.

c) Er is zoveel mogelijk gebruik gemaakt van versleutelde beheermechanismen.

d) Beheer is alleen toegestaan vanaf vooraf gedefinieerde IP-adressen.

e) Voor toegang tot switches wordt gebruik gemaakt van Virtual LAN's (V_LAN) en de toegang tot netwerkpoorten wordt beperkt op basis van MAC-adres (port security)

C.13.10.4 Mobiele code

Beheersmaatregel

Als gebruik van 'mobile code' wordt toegelaten, dan zorgt de configuratie ervoor dat de geautoriseerde 'mobile code' functioneert volgens een vastgesteld inrichtingsdocument (configuratiebladen) en voorkomt de configuratie dat niet-toegelaten "mobile code" wordt uitgevoerd.

Toelichting

'Mobile code' is programmatuur die kan worden overgedragen van de ene naar de andere computer, automatisch wordt uitgevoerd en een specifieke functie vervult zonder of met weinig tussenkomst van de gebruiker. 'Mobile code' werkt samen met besturingsprogrammatuur (zgn. middleware) die de informatie-uitwisseling regelt tussen de clientsoftware en de software die de bedrijfsgegevens beheert. Vaak gaat het om gedistribueerde systemen en meerdere platforms.

Implementatierichtlijnen

a) De volgende handelingen worden overwogen om te verhinderen dat 'mobile code' ongeautoriseerde acties kan uitvoeren:

1. uitvoeren van toegestane 'mobile code' in een logisch geïsoleerde omgeving;
2. blokkeren van elk gebruik van 'mobile code';
3. blokkeren van ontvangen van 'mobile code';
4. activeren van technische maatregelen die beschikbaar zijn op een specifiek systeem om te waarborgen dat toegestane 'mobile code' wordt beheerd;
5. beheersen van de bronnen die beschikbaar zijn voor toegang tot toegestane 'mobile code';
6. cryptografische beveiligingsmaatregelen om toegestane 'mobile code' uniek te authenticeren.

C.13.10.5 Beheersing berichtenverwerking

Beheersmaatregel

De technische infrastructuur voor berichtverwerking is zodanig ontworpen en ingericht, dat foutsituaties worden voorkomen of herkend en dat functioneel beheer over foutbestanden mogelijk is.

Implementatierichtlijnen

a) Infrastructuur bevat logica die het beheer van foutbestanden mogelijk maakt.

b) Berichtverwerkende infrastructuur past foutloze berichtenverwerking toe (Persistence Messaging).

c) Faalhandsters worden niet gebruikt als opslagmechanisme (buffering). Voor tijdelijke opslag van berichten in verwerkingsketens worden aparte tussenbestanden gebruikt.

d) Stapelen van fouten wordt voorkomen door toepassing van 'noodstop' mechanismen. Juist verwerkte resultaten worden hierdoor niet noodgedwongen naar een foutief verwerkingsproces gestuurd.

C.13.10.6 Beheersing batchverwerking

Beheersmaatregel

Bij batchverwerking borgen productieplanning en/of bewakingssystemen dat de risico's van verwerkingsfouten die tot verlies van integriteit leiden geminimaliseerd worden.

Implementatierichtlijn

a) De planning van reguliere batchprogramma's is gebaseerd op de aangegeven tijdstippen en volgorde volgens de systeemdocumentatie en houdt rekening met de afhankelijkheden die er tussen verwerkingen en met andere applicaties kan bestaan, start van de eerste taak en beëindiging van de laatste taak.

b) Onderdelen voor verwerking van batches worden pas opgestart, nadat voorafgaande verwerkingen succesvol zijn beëindigd.

c) Generatievalidatie- en herstelmechanismen voorkomen dubbele of onvolledige verwerkingen en borgen oudere verwerkingsroutines bij het opleveren van productiefouten.

d) Bij uitwisseling van bestanden tussen centrale en decentrale servers of met externe partijen wordt

met een apart file-transformmechanisme zeker gesteld dat uitwisseling niet achterwege blijft of dubbel plaatsvindt, tenzij behandeling geheel kan plaatsvinden volgens punt f hiervoor.

e) Er wordt een logbestand aangemaakt van de activiteiten die tijdens de verwerking plaatsvinden.

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
Ministerie van Financiën
Directoraat-Generaal Belastingdienst
Concerndirectie Informatievoorziening en databeheersing
Ter attentie van:
Mevrouw drs. A.C. van Huffelen
Persoonsgegevens
Korte Voorhout 7
2500 EE Den Haag

3SRRC15346681

3SRRC15346682

Datum
12 november 2021

Ons kenmerk
z2021-16923

Contactpersoon
Persoonsgegevens

Onderwerp
Kopie voornemen handhaving en gelegenheid tot geven zienswijze

Geachte mevrouw Van Huffelen,

De Autoriteit Persoonsgegevens (AP) heeft het verwerken van persoonsgegevens in de Fraude Signalering Voorziening (FSV) en het gebruik van deze applicatie door de Belastingdienst onderzocht.

Hierbij treft u ter informatie een afschrift aan van de brief die de AP in het kader van deze zaak heeft verzonden aan de heer W.B. Hoekstra, minister van Financiën. Het betreft een voornemen tot handhaven en een gelegenheid tot het geven van een zienswijze op zowel de inhoud van het rapport als de mogelijke oplegging van een sanctie. Kortheidshalve verwijs ik u naar de inhoud van deze brief.

Ik vertrouw er op u hiermee naar behoren te hebben geïnformeerd.

Hoogachtend,
de Autoriteit Persoonsgegevens,

Persoonsgegevens

AUTORITEIT
PERSOONSGEGEVENS

De minister van Financien
Ter attentie van:
De heer mr. W.B. Hoekstra, MBA
Persoonsgegevens
Korte Voorhout 7
2500 EE Den Haag

Datum

Ons kenmerk

Contactpersoon

Onderwerp
Voornemen handhaving en gelegenheid tot geven zienswijze

Geachte heer Hoekstra,

De Autoriteit Persoonsgegevens (AP) heeft onderzoek gedaan naar het verwerken van persoonsgegevens in de Fraude Signalering Voorziening (FSV) van de Belastingdienst. De AP heeft op 29 oktober 2021 het definitief rapport met de bevindingen over dit onderzoek aan mevrouw Van Huffelen verstrekt.

Samengevat concludeert de AP in het rapport dat dat de minister van Financiën, als verwerkingsverantwoordelijke voor de verwerkingen van de Belastingdienst, van 4 november 2013 tot en met 27 februari 2020 door het verwerken van persoonsgegevens in FSV in strijd heeft gehandeld met de beginselen van rechtmatigheid, doelspecificatie, juistheid en opslagbeperking.[1]

Naast het overtreden van de vier hiervoor benoemde beginselen concludeert de AP dat de Belastingdienst onvoldoende passende technische en organisatorische maatregelen heeft genomen ten aanzien van de toegangsbeveiliging, logging en controle op de logging om een passend beveiligingsniveau voor de persoonsgegevens in FSV te waarborgen.[2] Tot slot heeft de AP geconcludeerd dat de Belastingdienst de Functionaris gegevensbescherming niet naar behoren en tijdig heeft betrokken bij de uitvoering van de gegevensbeschermingseffectbeoordeling van FSV.[3]

[1] Zie artikel 5, eerste lid, aanhef en onder a, van de AVG en artikel 6 van de Wbp (rechtmatigheid), artikel 5, eerste lid, aanhef en onder b, van de AVG en artikel 7 van de Wbp (doelspecificatie), artikel 5, eerste lid, aanhef en onder d, van de AVG en artikel 11, tweede lid, van de Wbp (juistheid) en artikel 5, eerste lid, aanhef en onder e, van de AVG en artikel 10, eerste lid, van de Wbp (opslagbeperking)
[2] Zie artikel 32, eerst lid, aanhef van de AVG en artikel 13 van de Wbp.
[3] Zie artikel 38, eerste lid, van de AVG jo. artikel 35, tweede lid, van de AVG.

AUTORITEIT
PERSOONSGEGEVENS

Datum [redacted] Ons kenmerk [redacted]

De AP is voornemens om, gelet op de bovenstaande geconstateerde overtredingen, de haar toekomende bevoegdheid tot het opleggen van een sanctie aan te wenden. U dient ermee rekening te houden dat dit kan resulteren in het opleggen van een bestuurlijke boete en/of een corrigerende maatregel.

Ingeval de AP overgaat tot boeteoplegging bepaalt zij de hoogte van de boete aan de hand van de door haar vastgestelde Boetebeleidsregels.[4] Deze kunt u vinden op de website van de AP. De basisboetes kunnen worden verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 7 van de Boetebeleidsregels daartoe aanleiding geven.

Voordat de AP hierover beslist, stel ik u in de gelegenheid om een zienswijze te geven op zowel de inhoud van het rapport als de mogelijke oplegging van een sanctie. Een schriftelijke zienswijze ontvangt de AP graag uiterlijk **13 december 2021**. Als u uw reactie mondeling wenst te geven, verneemt de AP dat graag uiterlijk **22 november 2021**. U kunt hiervoor contact opnemen met bovengenoemd contactpersoon.

Een afschrift van deze brief en de onderliggende op de zaak betrekking hebbende stukken zullen verstuurd worden naar de Belastingdienst.

Ik vertrouw er op u hiermee naar behoren te hebben geïnformeerd.

Indien u vragen heeft over deze brief, dan wel informatie wilt doorgeven of versturen, verzoek ik u contact op te nemen met bovengenoemd contactpersoon.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

Persoonsgegevens

[4] Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes., *Stcrt.* 2019, 14586.

bij lage 33

FSV
Deel 3/5

Ministerie van Financiën

Handboek Beveiliging Belastingdienst

2017

Deel D

Implementatierichtlijnen

BCM

Boekdata

Titel Handboek Beveiliging Belastingdienst 2017
Deel D : Implementatierichtlijnen BCM

Versie December 2016

Versie	Opmerkingen - revisies
December 2014	Eerste jaargang HBB Deel D
Februari 2016	Tweede jaargang HBB Deel D
December 2016	Derde jaargang HBB Deel D – Dit document bevat de vertaling in het Nederlands van de Europese norm EN ISO 22313:2014. – Bron: Rijksoverheid NEN Connect 2016-2020

Nederlandse norm

NEN-EN-ISO 22313

(nl)

Maatschappelijke veiligheid -
Managementsystemen voor bedrijfscontinuïteit
(business continuity management systems) -
Richtlijnen (ISO 22313:2012,IDT)

Societal security -
Business continuity management systems -
Guidance (ISO 22313:2012,IDT)

ICS 03.100.01
november 2014

EUROPESE NORM

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO 22313

november 2014

ICS 03.100.01

Nederlandstalige versie

Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Richtlijnen (ISO 22313:2012)

Sicherheit und Schutz des Gemeinwesens – Aufrechterhaltung der Betriebsfähigkeit – Leitlinie (ISO 22313:2012)	Societal security – Business continuity management systems – Guidance (ISO 22313:2012)	Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices (ISO 22313:2012)

Deze norm is de Nederlandstalige versie van de Europese norm EN ISO 22313:2014. Hij is vertaald door NEN. Hij heeft dezelfde status als de officiële versies.

Deze Europese norm is door CEN aangenomen op 18 oktober 2014.

CEN-leden zijn verplicht zich te houden aan het huishoudelijk reglement van CEN-CENELEC, waarin is vastgelegd onder welke voorwaarden aan deze Europese norm, zonder veranderingen, de status van nationale norm moet worden gegeven. Bijgewerkte lijsten van en bibliografische gegevens betreffende zulke nationale normen kunnen op aanvraag worden verkregen bij het managementcentrum van CEN-CENELEC en bij elk CEN-lid.

Deze Europese norm bestaat in drie officiële versies (Duits, Engels en Frans). Een versie in een andere taal die onder verantwoordelijkheid van een CEN-lid in zijn landstaal is gemaakt en die is aangemeld bij het managementcentrum van CEN-CENELEC, heeft dezelfde status als de officiële versies.

Leden van CEN zijn de nationale normalisatieorganisaties van België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Macedonië, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

CEN

Europees Comité voor Normalisatie

Europäisches Komitee für Normung

European Committee for Standardization

Comité Européen de Normalisation

Managementcentrum CEN-CENELEC: Marnixlaan 17, B-1000 Brussel

Ref. nr. EN ISO 22313:2014 nl

Inhoud

ISO-voorwoord

ISO (International Organization for Standardization) is een wereldwijde federatie van nationale normalisatie-instituten (de ISO-leden). Het voorbereidingswerk voor internationale normen wordt doorgaans uitgevoerd door de technische commissies van ISO. Elk lid dat interesse heeft in een onderwerp waarvoor een technische commissie is samengesteld, heeft recht op vertegenwoordiging in deze commissie. Ook internationale organisaties, zowel overheidsinstanties als niet-gouvernementele organisaties, nemen in samenwerking met ISO deel aan deze werkzaamheden. ISO werkt nauw samen met de International Electrotechnical Commission (IEC) inzake alle elektrotechnische normalisatie.

Internationale normen worden opgesteld overeenkomstig de voorschriften die in de ISO/IEC-richtlijnen deel 2 zijn opgenomen.

De voornaamste taak van de technische commissies is de voorbereiding van internationale normen. Ontwerpversies van internationale normen die zijn aangenomen door de technische commissies, worden ter stemming voorgelegd aan de leden. Publicatie als internationale norm vereist goedkeuring van ten minste 75 % van de stemmen die zijn uitgebracht door deelnemende leden.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp kunnen zijn van patentrechten. ISO is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

ISO 22313 werd opgesteld door Technische Commissie ISO/TC 223, *Societal security*.

Inleiding

Algemeen

Deze internationale norm geeft, indien van toepassing, richtlijnen voor de eisen die zijn beschreven in ISO 22301:2012 en in relatie hiermee aanbevelingen ('behoort te') en goedkeuring ('kunnen/mogen'). Het is niet de bedoeling van deze internationale norm om algemene richtlijnen voor alle aspecten van bedrijfscontinuïteit te geven.

Deze internationale norm heeft dezelfde hoofdstuktitels als ISO 22301 maar herhaalt niet de eisen voor managementsystemen voor bedrijfscontinuïteit en de termen en definities die ermee samenhangen. Organisaties die geïnformeerd willen worden over deze eisen, termen en definities moeten daarom ISO 22301 en ISO 22300 raadplegen.

Om nadere opheldering en uitleg over belangrijke punten te geven, bevat deze internationale norm een aantal figuren. Die figuren dienen alleen voor illustratieve doeleinden en de gerelateerde tekst in deze internationale norm heeft voorrang boven de figuren.

Een BCMS benadrukt het belang van:

— het onderkennen van de behoeften van de organisatie en de noodzaak om beleid en doelstellingen voor bedrijfscontinuïteitsmanagement vast te stellen;

— het implementeren en uitvoeren van beheersmaatregelen die ervoor zorgen dat een organisatie het vermogen heeft om verstorende incidenten te managen;

— monitoren en beoordelen van de prestaties en de doeltreffendheid van het BCMS; en

— continue verbetering gebaseerd op objectieve meting.

Net als elk ander managementsysteem bestaat een BCMS uit de volgende hoofdcomponenten:

a) beleid;

b) mensen met gedefinieerde verantwoordelijkheden;

c) managementprocessen met betrekking tot:

   1) beleid;

   2) planning;

   3) implementatie en uitvoering;

   4) prestatiebeoordeling;

   5) directiebeoordeling; en

   6) verbetering.

d) documentatie waarmee auditeerbaar bewijsmateriaal wordt geleverd; en

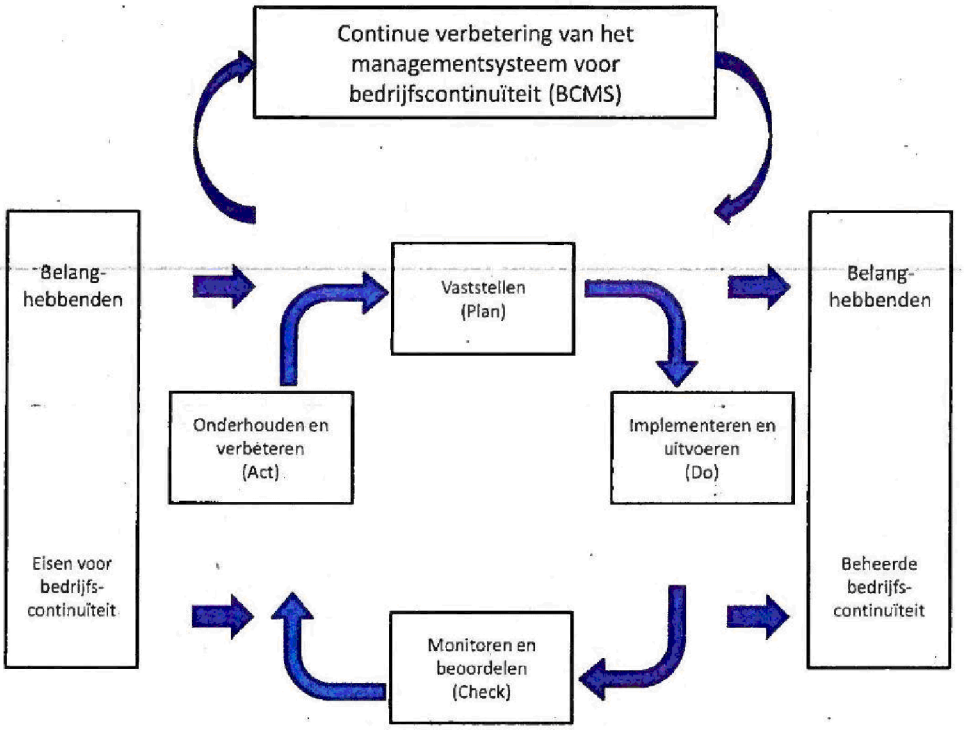
e) de BCMS-processen die relevant zijn voor de organisatie.

Bedrijfscontinuïteit is in het algemeen bedrijfsspecifiek, maar de implementatie ervan kan verstrekkende implicaties hebben voor de maatschappij en andere derden. Een organisatie heeft waarschijnlijk externe organisaties waar zij afhankelijk van is, en andere organisaties zijn afhankelijk van haar. Doeltreffende bedrijfscontinuïteit draagt daarom bij aan een veerkrachtiger maatschappij.

De Plan-Do-Check-Act-cyclus

Deze internationale norm past de Plan-Do-Check-Act (PDCA)-cyclus toe voor het plannen, inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en continu verbeteren van de doeltreffendheid van het BCMS van de organisatie.

Figuur 1 laat zien hoe het BCMS de eisen van de belanghebbenden neemt als input voor bedrijfscontinuïteitsmanagement (BCM) en, door middel van de vereiste handelingen en processen, als uitkomsten continuïteit levert (d.w.z. beheerde bedrijfscontinuïteit) die aan deze eisen voldoet.



Figuur 1 — PDCA-model toegepast op BCMS-processen

Tabel 1 — Verklaring van het PDCA-model

Plan (Vaststellen)	Beleid, doelstellingen, taakstellingen, beheersmaatregelen, processen en procedures voor bedrijfscontinuïteit vaststellen die relevant zijn om de bedrijfscontinuïteit te verbeteren, teneinde resultaten te leveren die overeenstemmen met het algehele beleid en de doelstellingen van de organisatie.
Do (Implementeren en uitvoeren)	Beleid, beheersmaatregelen, processen en procedures voor bedrijfscontinuïteit implementeren en uitvoeren.
Check (Monitoren en beoordelen)	De prestaties ten opzichte van doelstellingen en beleid voor bedrijfscontinuïteit monitoren en beoordelen, de resultaten ter beoordeling aan het management rapporteren, en geaccordeerde maatregelen voor herstel en verbetering vaststellen.
Act (Onderhouden en verbeteren)	Het BCMS onderhouden en verbeteren door corrigerende maatregelen te nemen, op basis van de resultaten van de directiebeoordeling en herbeoordeling van het toepassingsgebied van het BCMS en tevens van het beleid en de doelstellingen voor bedrijfscontinuïteit

Componenten van PDCA in deze internationale norm

Er bestaat een directe relatie tussen de inhoud van figuur 1 en de hoofdstukken van deze internationale norm:

Tabel 2 — Relatie tussen het PDCA-model en de hoofdstukken 4 t/m 10

PDCA-component	Hoofdstuk dat een PDCA-component behandelt
Plan (Vaststellen)	**Hoofdstuk 4 (Context van de organisatie)** beschrijft wat de organisatie moet doen om zeker te stellen dat het BCMS voldoet aan de eisen, rekening houdend met alle relevante externe en interne factoren, met inbegrip van:
	— de behoeften en verwachtingen van belanghebbenden,
	— de verplichtingen voortkomend uit wet- en regelgeving,
	— het vereiste toepassingsgebied van het BCMS.
	Hoofdstuk 5 (Leiderschap) beschrijft de belangrijke rol van management in de zin van betrokkenheid tonen, beleid definiëren en rollen, verantwoordelijkheden en bevoegdheden vaststellen.
	Hoofdstuk 6 (Planning) beschrijft de maatregelen die nodig zijn om strategische doelstellingen en beginselen voor het BCMS als geheel vast te stellen. Deze geven de context voor de bedrijfsimpactanalyse en risicobeoordeling (8.2) en de bedrijfscontinuïteitsstrategie (8.3).
	Hoofdstuk 7 (Ondersteuning) identificeert de belangrijke elementen die aanwezig moeten zijn om het BCMS te ondersteunen, namelijk: middelen, competentie, bewustzijn, communicatie en gedocumenteerde informatie.
Do (Implementeren en uitvoeren)	**Hoofdstuk 8 (Uitvoering)** identificeert de elementen van bedrijfs-continuïteitsmanagement (BCM) die nodig zijn om bedrijfscontinuïteit te bereiken.

Check (Monitoren en beoordelen)	**Hoofdstuk 9 (Evaluatie van de prestaties)** biedt de basis voor het verbeteren van het BCMS door de prestatie te meten en te evalueren.
Act (Onderhouden en verbeteren)	**Hoofdstuk 10 (Verbetering)** behandelt de corrigerende maatregelen die nodig zijn om afwijkingen die door evaluatie van de prestatie zijn geïdentificeerd aan te pakken.

Bedrijfscontinuïteit

Bedrijfscontinuïteit is het vermogen van de organisatie om na een verstorend incident producten of diensten te blijven leveren op acceptabele, vooraf vastgestelde niveaus. Bedrijfscontinuïteitsmanagement (BCM) is het proces waarmee bedrijfscontinuïteit bereikt wordt en gaat over het voorbereiden van een organisatie op het afhandelen van verstorende incidenten die anders zouden kunnen verhinderen haar doelstellingen te bereiken.

Door BCM te plaatsen binnen het kader en de disciplines van een managementsysteem wordt een bedrijfscontinuïteitsmanagementsysteem (BCMS) gecreëerd waardoor het BCM kan worden beheerst, geëvalueerd en continu verbeterd.

In deze internationale norm wordt het woord bedrijf gebruikt als een allesomvattende term voor de activiteiten en diensten die een organisatie verricht bij het nastreven van haar doelstellingen, doelen of missie. Als zodanig is het gelijkelijk van toepassing op grote, middelgrote en kleine organisaties die actief zijn in industriële, commerciële, publieke en non-profitsectoren.

Elk incident, groot of klein, natuurlijk, per ongeluk of opzettelijk, heeft de potentie om een grote verstoring te veroorzaken in de bedrijfsactiviteiten van een organisatie en haar vermogen om producten en diensten te leveren. Door echter bedrijfscontinuïteit te implementeren voordat zich een verstorend incident voordoet, in plaats van te wachten totdat het gebeurt, is de organisatie in staat haar bedrijfsactiviteiten voort te zetten voordat dit leidt tot onacceptabele impactniveaus.

BCM houdt in:

a) duidelijk zijn over de belangrijkste producten en diensten van de organisatie en de activiteiten waar zij uit voortkomen;

b) de prioriteiten kennen voor het voortzetten van activiteiten en de middelen die hiervoor vereist zijn;

c) duidelijk inzicht hebben in de bedreigingen voor deze activiteiten, met inbegrip van hun afhankelijkheden, en weten wat de gevolgen zijn als de activiteiten niet hervat worden;

d) beschikken over beproefde en vertrouwde voorzieningen om deze activiteiten te hervatten na een verstorend incident; en

e) bewerkstelligen dat deze voorzieningen volgens vaste regels worden beoordeeld en geactualiseerd, zodat ze in alle omstandigheden doeltreffend zijn.

Bedrijfscontinuïteit kan doeltreffend zijn bij het behandelen van zowel plotselinge verstorende incidenten (bijv. explosies) als incidenten die zich geleidelijk voltrekken (bijv. grieppandemieën).

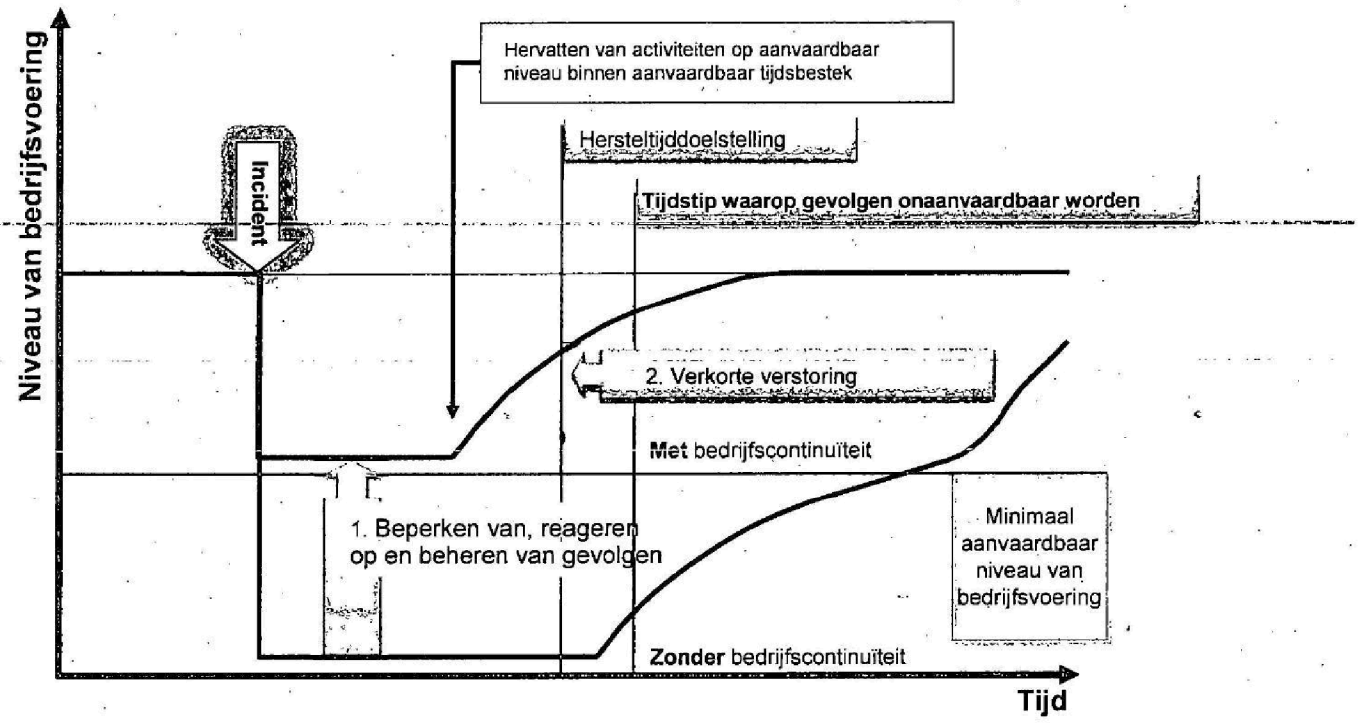
Activiteiten kunnen worden verstoord door veel verschillende incidenten die vaak moeilijk te voorspellen of te analyseren zijn. Door de aandacht te richten op het gevolg van de verstoring in plaats van op de oorzaak identificeert bedrijfscontinuïteit de activiteiten waar de organisatie van afhankelijk is om te overleven, en stelt het de organisatie in staat om vast te stellen wat nodig is om aan haar verplichtingen te blijven voldoen. Door middel van bedrijfscontinuïteit kan een organisatie herkennen wat gedaan moet worden om haar middelen (bijv. personen, gebouwen, technologie en informatie), toeleveringsketen, belanghebbenden en reputatie te beschermen, voordat zich een verstorend incident voordoet. Op basis van die herkenning is de organisatie in

staat de reactie die waarschijnlijk nodig is ingeval zich een verstoring voordoet realistisch te bezien, zodat zij het vertrouwen kan hebben dat ze de gevolgen kan managen en onaanvaardbare gevolgen kan vermijden.

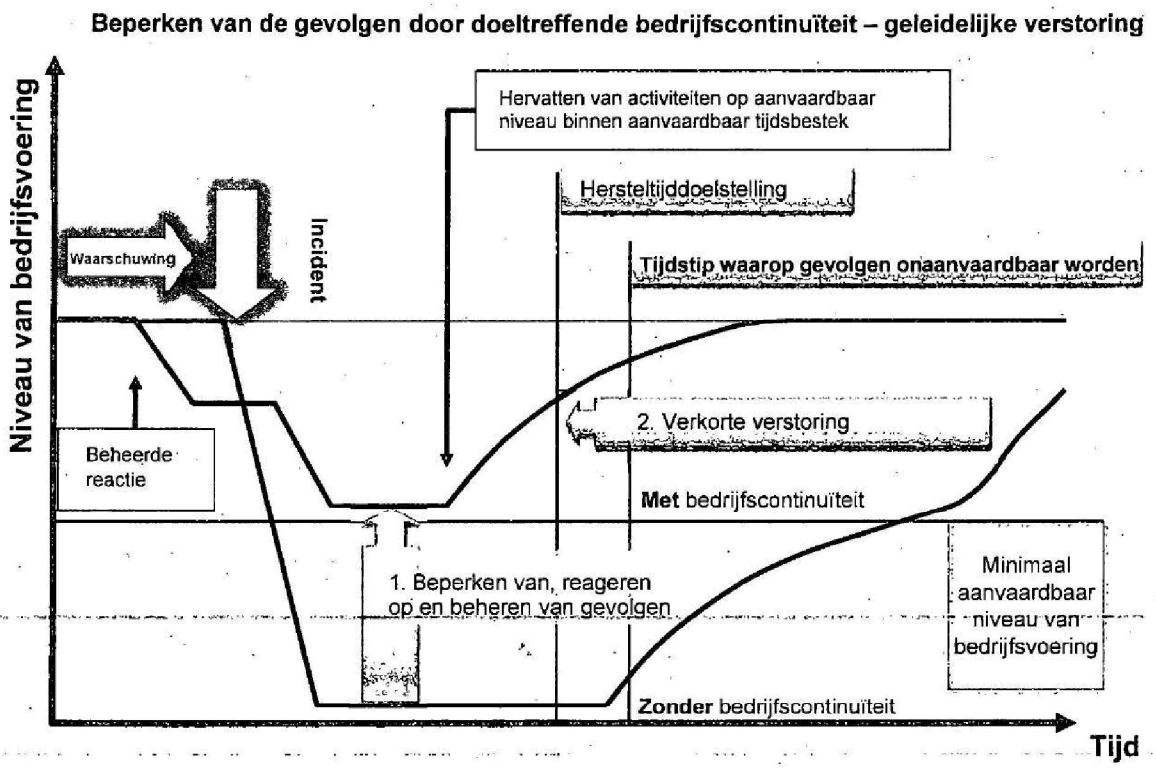
Een organisatie met de juiste bedrijfscontinuïteit kan ook profijt hebben van mogelijkheden die anders als te risicovol worden beoordeeld.

De volgende diagrammen (figuren 2 en 3) zijn bedoeld om conceptueel te illustreren hoe bedrijfscontinuïteit doeltreffend kan zijn om gevolgen in bepaalde situaties te beperken. Er zijn geen bepaalde tijdschalen geïmpliceerd door de relatieve afstand tussen de stadia die in beide diagrammen worden weergegeven.

Beperken van de gevolgen door doeltreffende bedrijfscontinuïteit – plotselinge verstoring



Figuur 2 — Illustratie van bedrijfscontinuïteit die doeltreffend is in geval van plotselinge verstoring



Figuur 3 — Illustratie van bedrijfscontinuïteit die doeltreffend is in geval van geleidelijke verstoring (bijv. een naderende pandemie)

Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Richtlijnen

1 Onderwerp en toepassingsgebied

Deze internationale norm voor BCM geeft richtlijnen die zijn gebaseerd op een goede internationale werkwijze voor het plannen, inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en continu verbeteren van een gedocumenteerd managementsysteem, ter bescherming tegen, verkleining van de kans op, voorbereiding op, reactie op en herstel van verstorende incidenten wanneer deze zich voordoen.

Deze internationale norm heeft niet tot doel een uniforme structuur op te leggen voor een managementsysteem voor bedrijfscontinuïteit (BCMS), maar om een organisatie in staat te stellen een BCMS te ontwerpen dat op haar behoeften is afgestemd en dat voldoet aan de eisen van haar belanghebbenden. Deze behoeften worden gevormd door wettelijke, regelgevende, organisatie- en branchespecifieke eisen, de producten en diensten, de toegepaste processen, de omgeving waarin zij actief is, de omvang en structuur van de organisatie en de eisen van haar belanghebbenden.

Deze internationale norm is generiek en van toepassing op organisaties van elke omvang en van elk type, met inbegrip van grote, middelgrote en kleine organisaties die actief zijn in industriële, commerciële, publieke en non-profitsectoren, die:

a) een BCMS willen inrichten, implementeren, onderhouden en verbeteren;

b) naleving van het vastgestelde beleid voor bedrijfscontinuïteit willen bewerkstelligen; of

c) zelf de naleving van deze internationale norm vast willen stellen en daarvan een eigen verklaring willen opstellen.

Deze internationale norm kan niet worden gebruikt ter beoordeling van het vermogen van een organisatie om te voldoen aan haar eigen bedrijfscontinuïteitseisen, noch aan die van een klant, of aan eisen van wet- of regelgeving. Organisaties die dit willen, kunnen de eisen van ISO 22301 gebruiken om aan andere partijen conformiteit aan te tonen of kunnen een geaccrediteerde certificatie-instelling vragen hun BCMS te certificeren.

2 Normatieve verwijzingen

De volgende documenten waarnaar is verwezen zijn onmisbaar voor de toepassing van dit document. Bij gedateerde verwijzingen is alleen de aangehaalde versie van toepassing. Bij ongedateerde verwijzingen is de laatste versie van het document (met inbegrip van wijzigings- en correctiebladen) waarnaar is verwezen van toepassing.

ISO 22300	*Societal security – Terminology*
ISO 22301	*Societal security – Business continuity management systems – Requirements*

3 Termen en definities

Met betrekking tot dit document gelden de termen en definities zoals beschreven in ISO 22300 en ISO 22301.

4 Context van de organisatie

4.1 Inzicht in de organisatie en haar context

Deze paragraaf gaat over inzicht krijgen in de context van de organisatie in verband met het inrichten en beheren van het BCMS. Het inrichten en beheren van BCM wordt behandeld in 8.1.

De organisatie behoort inzicht te hebben in de interne en externe factoren die relevant zijn voor haar doel en bedrijfsvoering en deze te evalueren. Deze informatie behoort in aanmerking genomen te worden bij het inrichten, implementeren, onderhouden en verbeteren van het BCMS van de organisatie en bij het toekennen van prioriteiten.

Een evaluatie van de externe context van de organisatie behoort, indien relevant, de volgende factoren te omvatten:

— het politieke, wettelijke en regelgevende kader, hetzij internationaal, nationaal, regionaal of lokaal;

— het sociale en culturele, financiële, technologische, economische, natuurlijke en concurrentiekader, hetzij internationaal, nationaal, regionaal of lokaal;

— verplichtingen voortkomend uit toeleveringsketens en relaties;

— overweging van interne studies over de risico's, rekening houdend met andere relevante informatiemanagementsystemen en meer in het algemeen informatie van kennismanagement;

— belangrijke sturende factoren en trends die invloed hebben op de doelstellingen en de bedrijfsvoering van de organisatie; en

— relaties met, en percepties en waarden van belanghebbenden buiten de organisatie.

Een evaluatie van de interne context van de organisatie behoort, indien relevant, de volgende factoren te omvatten:

— producten en diensten, activiteiten, middelen, toeleveringsketens, en relaties met belanghebbenden;

— het vermogen in termen van middelen en kennis (bijv. kapitaal, tijd, mensen, processen, systemen en technologieën);

— informatiesystemen, informatiestromen en besluitvormingsprocessen (zowel formeel als informeel);

— belanghebbenden binnen de organisatie;

— beleid, doelstellingen, en de aanwezige strategieën om deze te halen;

— toekomstige kansen en bedrijfsprioriteiten;

— percepties, waarden en cultuur;

— normen en referentiemodellen die binnen de organisatie worden gehanteerd; en

— structuren (bijv. bestuur, rollen en verantwoordelijkheden).

4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

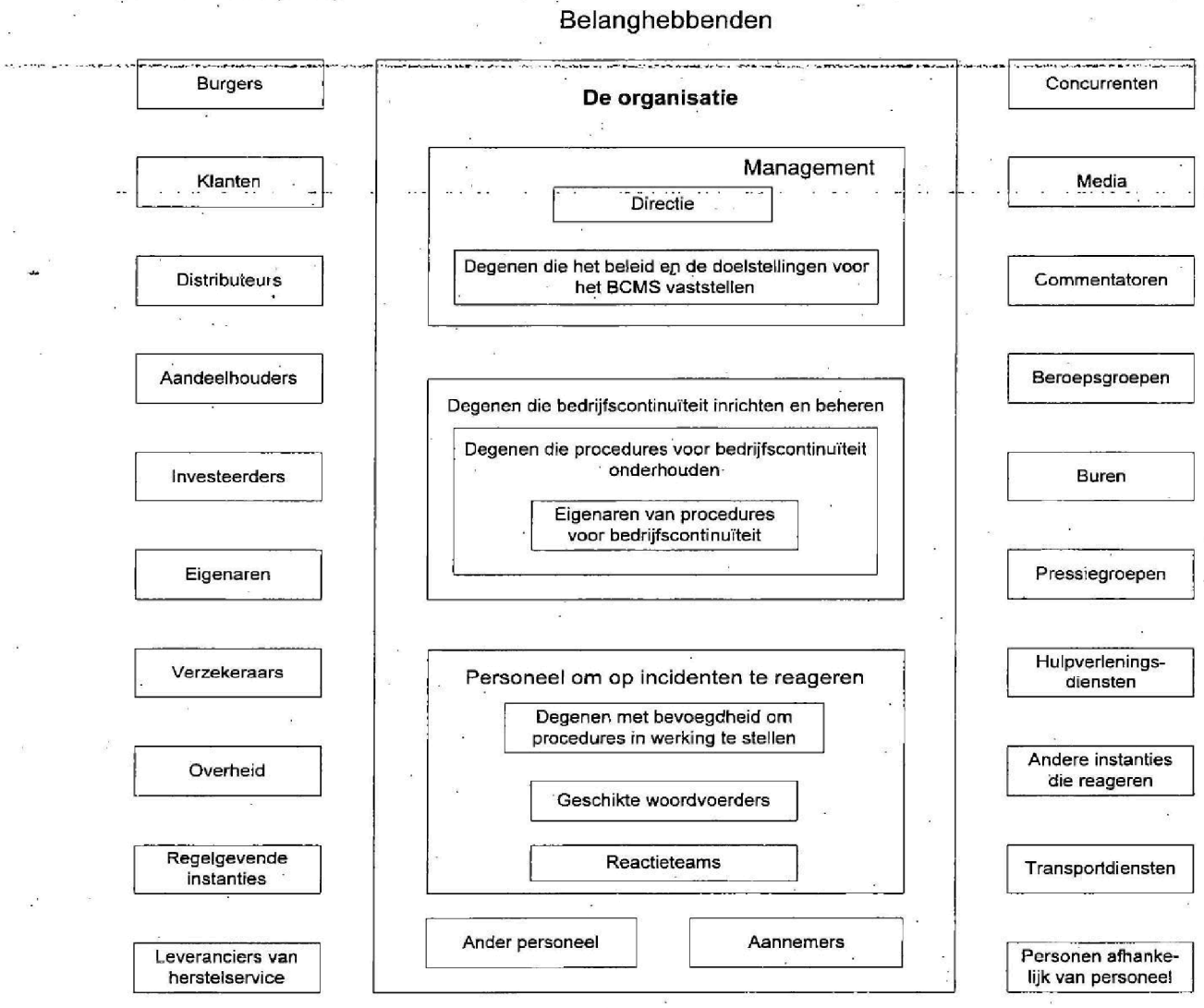
4.2.1 Algemeen

Bij het inrichten van haar BCMS behoort de organisatie te bewerkstelligen dat de behoeften en eisen van belanghebbenden in aanmerking worden genomen.

De organisatie behoort alle belanghebbenden die relevant zijn voor haar BCMS te identificeren, en gebaseerd op hun behoeften en verwachtingen, hun eisen vast te stellen. Het is belangrijk niet alleen verplichte en vastgelegde eisen te identificeren maar ook impliciete eisen.

OPMERKING De organisatie behoort zich bewust te zijn van iedereen die een belang heeft in de organisatie zoals de media, het publiek, concurrenten enz.

Bij het plannen en implementeren van het BCMS is het belangrijk activiteiten te identificeren die passend zijn in verband met belanghebbenden, maar te differentiëren tussen de verschillende categorieën. Het kan bijvoorbeeld passend zijn om na een verstorend incident te communiceren met alle belanghebbenden, maar het is mogelijk niet passend om bij het inrichten en beheren van BCM met alle belanghebbenden te communiceren (8.1.1).



Figuur 4 — Voorbeelden van belanghebbenden met wie in openbare en particuliere sectoren rekening gehouden moet worden