normatieve uitwerking van de hls creatieve

ISO/IEC 27002: 2013 Grafimedia

Praktijkrichtlijn met beheersmaatregelen voor Informatietechnologie, Beveiligingstechnieken en de Code voor Informatiebeveiliging

Onderdeel van de Grafimedia Certificatienorm Informatiebeveiliging

Uitgave van de Stichting Certificatie Grafimedia branche (SCGM)

INHOUDSOPGAVE

1 INLEIDING

Informatiebeveiliging wordt als gevolg van de digitalisering en de koppeling van informatiesystemen (internet) voor organisaties steeds belangrijker. Klanten en ook medewerkers stellen steeds meer eisen op dat vlak. Dit speelt in het bijzonder voor grafische ondernemingen die informatie vertalen naar een grafisch product en daarvoor informatie in de vorm van digitale 'assets' in beheer houden. Daarnaast is het van belang om bedrijfsinformatie te beschermen om de bedrijfscontinuïteit te waarborgen. Het 'kwijtraken' van orderinformatie schaadt bijvoorbeeld direct het functioneren van de onderneming. Ook op het gebied van wet- en regelgeving heeft de onderneming te maken met het zorgvuldig beheren van informatie, bijvoorbeeld de wet- en regelgeving op het gebied van het beheer van personeelsgegevens.
Organisaties en hun informatiesystemen en netwerken worden geconfronteerd met beveiligingsrisico's uit allerlei bronnen, zoals computerfraude, spionage, sabotage, vandalisme, brand en overstromingen. Met de komst van het internet zijn nieuwe oorzaken van schade ontstaan, zoals: computervirussen, computerinbraak en 'denial of service'-aanvallen. Deze vormen van schade komen steeds vaker voor en worden steeds ambitieuzer en vernuftiger.

Informatiebeveiliging is de bescherming van informatie tegen een breed scala bedreigingen om de bedrijfscontinuïteit te waarborgen en bedrijfsrisico's te minimaliseren.
Informatiebeveiliging wordt bereikt door de juiste verzameling beheersmaatregelen te treffen, waaronder beleid, werkwijzen, procedures, organisatiestructuren en programmatuur- en apparaat functies. Deze beheersmaatregelen moeten worden vastgesteld, gecontroleerd, beoordeeld en waar nodig verbeterd, om te waarborgen dat de specifieke beveiligings- en bedrijfsdoelstellingen van de organisatie worden bereikt. Dit behoort te worden gedaan in samenhang met andere bedrijfsbeheerprocessen (bijvoorbeeld kwaliteitszorg).

De ISO/IEC 27002: 2013 Grafimedia is gebaseerd op de internationale norm (praktijkrichtlijn) voor informatiebeveiliging NEN-ISO/IEC: 27002:2013. Deze is opgesteld als de praktische lijst maatregelen die beheerst worden door een zogenaamd ISMS – een managementsysteem voor informatiebeveiliging (Information Security Management System).

Dit ISMS wordt door de SCGM als aparte norm omschreven: ISO/IEC 27001: 2013 Grafimedia. Deze norm is conform de zogenaamde High Level Structure. Deze structuur is opgezet om eenvoudig geïntegreerd te worden met andere ISO systemen, met name het ISO 9001 kwaliteitszorgsystemen.

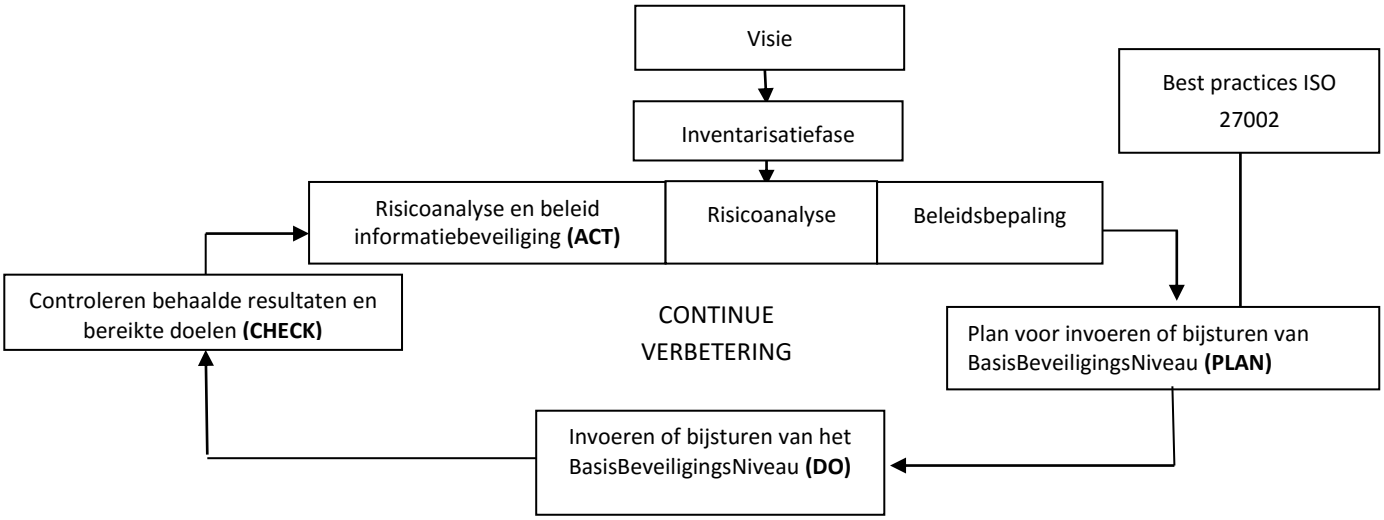
1.1 Grafimedia Certificatienorm Informatiebeveiliging

De totale Grafimedia Certificatienorm Informatiebeveiliging (GCI) is de norm die gesteld wordt door toepassing van zowel de ISO/IEC 27001: 2013 Grafimedia en de ISO/IEC 27002: 2013 Grafimedia norm.

De GCI is gebaseerd op drie pijlers die richting geven aan het effectief en efficiënt inrichten van de informatiebeveiliging. Het gaat immers niet om het treffen van veel maatregelen, maar juist die maatregelen die nodig en effectief zijn. De drie pijlers zijn:

- De context van de organisatie van de onderneming met betrekking tot de gewenste beveiliging en de daarmee gemoeide risico's;
- Het risicoprofiel van de onderneming, door middel van inventarisatie van de specifieke risico's die de onderneming loopt en hoe deze risico's worden beoordeeld;
- De planning van doelstellingen en maatregelen, ondersteund door de 'best practices' die in ISO 27002 worden omschreven en die zijn toegesneden op de grafische sector.

Op basis van de drie pijlers wordt binnen de context van de 27002 norm het BasisBeveiligingsNiveau (BBN) vastgesteld dat voor de onderneming moet (gaan) gelden, dat wordt vastgelegd in de Verklaring van Toepasselijkheid (VvT). Daarnaast kunnen voor bepaalde processen of afdelingen additionele maatregelen worden gedefinieerd die niet voor de gehele organisatie gelden. Vervolgens wordt de planning- en controlecyclus geïmplementeerd waarmee feedback op de naleving wordt gegeven, zodat bijgestuurd en verbeterd kan worden. Dit leidt tot een model voor invoering van informatiebeveiliging zoals onder weergegeven. Dit model is gebaseerd op de Deming cirkel.



Als startpunt voor informatiebeveiliging zijn een aantal beheersmaatregelen van belang, namelijk:

- de beheersmaatregelen die vanuit wet- en regelgeving essentieel zijn, en
- de beheersmaatregelen die als algemene basis gelden voor het realiseren van informatiebeveiliging.

De relevante wet- en regelgeving kunnen o.a. betreffen, maar zijn niet beperkt tot:

- Bescherming van persoonsgegevens (Wet Bescherming Persoonsgegevens)
- Beleidsregels rondom datalekken van de Autoriteit Persoonsgegevens
- Bescherming van specifieke bedrijfsdocumenten (Archiefwet)
- Intellectuele eigendomsrechten en rechten op digitaal materiaal (o.a. Auteurswet)
- Telecommunicatiewet
- Wet computercriminaliteit

- Burgerlijk en Strafrechtelijk wetboek

De certificering van het GCI omvat het toetsen van het BasisBeveiligingsNiveau zoals vastgelegd in de Verklaring van Toepasselijkheid ten opzichte van het risicoprofiel en de beleidsuitgangspunten op basis van de 'best practices.' Verder wordt het proces getoetst waarmee het BBN gerealiseerd en gehandhaafd zal worden. Dat betekent dat niet noodzakelijkerwijs alle doelstellingen al ingevoerd hoeven te zijn. De certificeringsaudit heeft tot doel vast te stellen of het juiste BBN wordt gehanteerd en of het proces van interne controle zodanig is ingericht dat het BBN wordt gehandhaafd. Bij de certificeringsaudit wordt rekening gehouden met de diversiteit van de grafische bedrijven ten aanzien van de bedrijfsgrootte, aard van de productieprocessen en de aard van de producten en diensten die worden aangeboden.

De GCI is opgesteld voor de Grafimedia branche en is daarom van toepassing op elke organisatie die:

- Een vorm van grafimedia dienstverlening kent;
- Een intern systeem van informatiebeveiliging wil invoeren, handhaven en verbeteren;
- Ervan verzekerd wil zijn dat het door haar vastgestelde informatiebeveiligingsbeleid met de daaraan verbonden risico's op alle niveaus wordt nageleefd;
- Een dergelijke naleving van het informatiebeveiligingsbeleid aantoonbaar wil maken voor derden;
- Haar BasisBeveiligingsNiveau BBN en VvT door de externe certificatie-instantie Stichting Certificatie Grafimedia branche wil laten certificeren en registreren.

De certificatienorm voor ISO/IEC 27002: 2013 Grafimedia is omschreven in de hoofdstukken 5 t/m 18 en geeft de eisen aan waaraan het systeem van informatiebeveiliging moet voldoen. De wijze van invulling die door de organisatie aan deze eisen wordt gegeven, wordt bepaald door het beleid van de organisatie, de aard en omvang van de risico's die samenhangen met procesmatige activiteiten, de relevante wet- en regelgeving en de overige omstandigheden waarbinnen de organisatie moet opereren. De organisatie is zelf verantwoordelijk voor de passendheid van haar systeem van informatiebeveiliging, teneinde de relevante wet- en regelgeving op de juiste wijze na te leven en beveiligingsrisico's te voorkomen, danwel zoveel mogelijk te beperken. Tevens heeft de organisatie de plicht om de wijze waarop invulling is gegeven aan deze eisen aantoonbaar en inzichtelijk te maken voor de certificerende instantie.

2 NORMATIEVE VERWIJZINGEN

De ISO/IEC 27002: 2013 Grafimedia is gebaseerd op de internationale norm (praktijkrichtlijn) voor informatiebeveiliging NEN-ISO/IEC: 27002:2013. Deze is opgesteld als de praktische lijst maatregelen die beheerst worden door een zogenaamd ISMS – een managementsysteem voor informatiebeveiliging.

De totale Grafimedia Certificatienorm Informatiebeveiliging (GCI) is de norm die gesteld wordt door toepassing van zowel de ISO/IEC 27001: 2013 Grafimedia en de ISO/IEC 27002: 2013 Grafimedia norm.

3 TERMEN EN DEFINITIES

Voor de toepassing van deze norm gelden onderstaande termen en definities:

Audit trail
Zodanige vastlegging van gegevens dat de verwerkingsresultaten achteraf kunnen worden gecontroleerd.
Bedreiging
Een potentiële oorzaak van een ongewenst incident dat een systeem of organisatie schade kan toebrengen.
Bedrijfsmiddel
Alles dat waarde heeft voor de organisatie.

Beheersmaatregel
Middel om risico te beheersen, waaronder beleid, procedures, richtlijnen, werkwijzen of organisatiestructuren, die administratief, technisch, beheersmatig of juridisch van aard kunnen zijn.
Beleid
De verklaring van de organisatie ten aanzien van haar visie en de daaruit voortvloeiende doelstellingen welke zij voornemens is te realiseren in het kader van informatiebeveiliging.
Certificaatautoriteit
Organisatie die gerechtigd is om digitale certificatie uit te geven.
Deming cirkel: Ook wel de Plan-Do-Check-Act (PDCA cyclus) genoemd. Dit model kan worden gehanteerd bij vrijwel elke verbeteractiviteit en omvat de volgende stappen:
Plan: ontwikkel een plan om de kwaliteit te verbeteren.
Do: voer het plan uit, eerst kleinschalig.
Check: Evalueer de resultaten om door te starten of het Plan aan te passen.
Act: Bevestig de aanpak of bestudeer de gevolgen van aanpassingen.
Derde partij
Persoon of entiteit die wat betreft de zaak in kwestie, als onafhankelijk van de betrokken partijen wordt gezien.
Digital assets
Elke vorm van content en/of media die in digitale vorm is opgeslagen.
Digital rights management (DRM)
Een techniek om digitale rechten van makers of uitgevers (de 'rechthebbenden') van werken (b.v. afbeeldingen, teksten) digitaal te beheren.
IT voorzieningen
Elk(e) systeem, dienst of infrastructuur voor informatieverwerking, of de fysieke locaties waarin ze zijn ondergebracht.
Informatiebeveiliging
Het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie; daarnaast kunnen ook andere eigenschappen zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid hierbij een rol spelen.
Informatiebeveiligingsgebeurtenis
De vastgestelde status van een procedure, register, systeem, dienst of netwerk die duidt op een mogelijke

overtreding van het beleid voor informatiebeveiliging of een falen van beveiligingsvoorzieningen, die relevant kan zijn voor beveiliging. Informatiebeveiligingsgebeurtenissen dienen te worden beoordeeld of deze incident zijn of niet.

Informatiebeveiligingsincident
Een afzonderlijke gebeurtenis, of een serie ongewenste of onverwachte informatiebeveiligingsgebeurtenissen, waarvan het waarschijnlijk is dat ze nadelige gevolgen voor de bedrijfsvoering hebben en een bedreiging vormen voor de informatiebeveiliging.

Kwetsbaarheid
De zwakte van een bedrijfsmiddel of groep bedrijfsmiddelen die door een of meer bedreigingen kan worden benut.

Mobile code
Software die tussen systemen wordt uitgewisseld, zonder expliciete installatie door de gebruiker. Mobile code heeft over het algemeen de vorm van een script of macro.

Richtlijn
Beschrijving die verduidelijkt wat behoort te worden gedaan en hoe, om de doelstellingen te bereiken die in het beleid zijn vastgelegd.

Risico
De combinatie van de waarschijnlijkheid van een gebeurtenis en het gevolg ervan.

Risicoacceptatie
Het accepteren van risico's op basis van een evaluatie van risico's aan de hand van vooraf vastgestelde criteria.

Risicoanalyse
Systematisch gebruik van informatie om bronnen te identificeren en de risico's in te schatten.

Risicobeheer
Gecoördineerde activiteiten om een organisatie sturing te geven en te bewaken met betrekking tot risico's.

Risicobehandeling
Het proces van keuze en implementatie van maatregelen om risico's te verlagen.

Risicobeoordeling
Het algehele proces van risicoanalyse en risico-evaluatie.

Risico-evaluatie
Het proces waarin het ingeschatte risico wordt afgewogen tegen vastgestelde risicocriteria om te bepalen in welke mate het risico significant is.

4 STRUCTUUR VAN DEZE NORM

Ter compleetheid worden hier op hoofdlijnen de categorieën van beheersaspecten en -maatregelen van zowel GCI/ISO 27001 als GCI/ISO 27002 genoemd. Daarbij richt 27001 zich op het managementsysteem en de beheersdoelstellingen, en 27002 zich op de praktijkmaatregelen die de beheersdoelstellingen dienen te realiseren. De volgorde van de hoofdstukken geeft niet aan hoe belangrijk een maatregel is: alle hoofdstukken en paragrafen dienen op afdoende wijze ingericht te zijn.

GCI/ISO 27001 (conform HLS):
4. De organisatie en haar context
5. Leiding en leiding geven
6. Plannen
7. Ondersteuning
8. Uitvoeren
9. Prestaties evalueren
10. Verbeteren

GCI/ISO 27002:
5. Beleidsdocument voor informatiebeveiliging
6. Organisatie van de informatiebeveiliging
7. Beveiliging van personeel
8. Beheer van bedrijfsmiddelen die verband houden met IT voorzieningen
9. Bedrijfseisen toegangsbeheersing
10. Cryptografie (versleuteling)
11. Fysieke beveiliging en omgevingsbeveiliging
12. Beveiliging bedrijf: bedieningsprocessen
13. Beveiliging bedrijf: communicatieprocessen
14. Verwerving, ontwikkeling en onderhoud van informatiesystemen
15. Relaties met leveranciers
16. Informatiebeveiligingsincidenten
17. Informatiebeveiliging en continuïteitsbeheer
18. Naleving

Conform de ISO 27002 norm zijn in de GCI norm de beveiliging beheersmaatregelen ingedeeld naar onderwerp. Per onderwerp wordt omschreven:

- Een beheersdoelstelling die vermeldt wat er moet worden bereikt.
- De beheersmaatregelen : de specifieke maatregelen om aan de beheersdoelstelling te voldoen.
- Implementatierichtlijnen die nadere informatie geven om de implementatie van de Beheersmaatregel te ondersteunen en om de beheersdoelstelling te realiseren. Bij een aantal onderdelen worden praktische voorbeelden gegeven die grafimedia organisaties kunnen overnemen. Sommige richtlijnen zijn niet in alle gevallen van toepassing.
- Overige informatie, hier staat (meestal) nadere informatie waarmee rekening moet worden gehouden, bijvoorbeeld juridische overwegingen, verwijzingen naar andere normen of naar 'best practices'.

Bij de norm zijn een aantal bijlagen met instructies en voorbeelden gemaakt (waaronder risicobeoordeling, systeemarchitectuur, checklist aanschaf voorzieningen) die u kunt inzetten bij implementatie van uw systeem. Deze bijlagen zijn als apart document van de website van SCGM te downloaden.

5 BELEIDSDOCUMENT VOOR INFORMATIEBEVELIGING

5.1 Aansturing door de directie

Doel: Zorgen voor directieaansturing van, en directieondersteuning voor, informatiebeveiliging passend bij de bedrijfseisen en relevante wet- en regelgeving.

5.1.1 Beleidsregels voor informatiebeveiliging

Beheersmaatregel
De directie behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

Implementatierichtlijnen
De directie behoort:

a. te waarborgen dat de informatiebeveiligingsdoelstellingen worden vastgesteld, deze voldoen aan de eisen van de organisatie en zijn geïntegreerd in de relevante processen;
b. het informatiebeveiligingsbeleid te formuleren, te beoordelen en goed te keuren;
c. de doelmatigheid van de implementatie van het informatiebeveiligingsbeleid te beoordelen;

d. te zorgen voor een heldere koers en zichtbare ondersteuning voor beveiligingsinitiatieven;
e. te zorgen voor de middelen die nodig zijn voor informatiebeveiliging;
f. het toekennen van rollen en verantwoordelijkheden voor de informatiebeveiliging en in alle lagen van de organisatie goed te keuren;
g. vast te stellen de behoefte aan opleiding en zorgdragen voor opleidingen;
h. plannen en programma's te initiëren om het informatiebeveiligingsbewustzijn levend te houden;
i. te waarborgen dat de implementatie van de beheersmaatregelen voor informatiebeveiliging in alle lagen van de organisatie wordt gecoördineerd (zie 7.1.2).
j. de directie behoort de behoefte aan interne of externe bronnen van deskundig advies voor informatiebeveiliging vast te stellen en de resultaten van het advies te beoordelen en te coördineren.

Afhankelijk van de grootte van de organisatie kunnen deze verantwoordelijkheden worden uitgevoerd door een daartoe aangewezen en bevoegd beheerorgaan of bevoegd medewerker, of door de directie.

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

Beheersmaatregel
Het beleid voor informatiebeveiliging moet met geplande tussenpozen en wanneer er significante veranderingen zijn worden beoordeeld, zodat het daardoor voortdurend passend, adequaat en doeltreffend is.

Implementatierichtlijn

Beleid dient een eigenaar te hebben. Deze eigenaar is namens directie verantwoordelijk voor het evalueren, beoordeling en ontwikkelen van beleidsregels. In de beoordeling moet ook vallen:
a. Beoordeling van verbetermogelijkheden voor de organisatorische beleidsregels en
b. de wijze van het informatiebeveiligingsbeheer als reactie op veranderingen in de omgeving van de organisatie, de bedrijfsomstandigheden, juridische voorwaarden of technische omgeving.

De specifieke directiebeoordeling is een van de zaken waar specifiek rekening mee moet worden gehouden bij deze beoordeling.

Als er nieuw beleid uit deze beoordeling volgt, dient hiervoor directiegoedkeuring te zijn alvorens het van kracht kan worden.

6 ORGANISEREN VAN INFORMATIEBEVEILIGING

6.1 Interne organisatie

Doel: organisatorische beheersing van de informatiebeveiliging binnen de organisatie. De organisatie heeft taken, verantwoordelijkheden en bevoegdheden omschreven en toegewezen, aangevuld met een omschrijving van de coördinatie en de inrichting en uitvoering van communicatie.

6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

Beheersmaatregel
Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

Implementatierichtlijnen
Het toewijzen van verantwoordelijkheden voor de informatiebeveiliging behoort te worden uitgevoerd in overeenstemming met het informatiebeveiligingsbeleid. De verantwoordelijkheid voor de bescherming van

individuele bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsmaatregelen behoort duidelijk te worden gedefinieerd. Deze verantwoordelijkheid behoort indien nodig te worden aangevuld met meer gedetailleerde richtlijnen voor bepaalde locaties, afdelingen of IT voorzieningen.
Personen aan wie beveiligingsverantwoordelijkheden zijn opgedragen, mogen beveiligingstaken aan anderen delegeren. Zij blijven echter verantwoordelijk en behoren zelf vast te stellen dat een gedelegeerde taak op de juiste wijze is uitgevoerd.
De terreinen waarvoor personen verantwoordelijk zijn behoren duidelijk te worden aangegeven; in het bijzonder behoort het onderstaande te worden uitgevoerd:

a. de bedrijfsmiddelen en beveiligingsmaatregelen van elk afzonderlijk systeem behoren te worden vastgesteld en duidelijk te worden gedefinieerd;
b. er behoort voor elk bedrijfsmiddel of maatregel een 'eigenaar' te worden aangewezen en de details van deze verantwoordelijkheid behoren te worden gedocumenteerd;
c. bevoegdheden behoren duidelijk te worden gedefinieerd en gedocumenteerd.

Overige informatie
Het verdient aanbeveling om een directielid de eindverantwoordelijkheid toe te wijzen, die de volledige verantwoordelijkheid krijgt voor de ontwikkeling en implementatie van de beveiliging en die ondersteuning verleent bij het vaststellen van de beheersmaatregelen.
De verantwoordelijkheid voor het beschikbaar stellen van middelen en het implementeren van de beheersmaatregelen ligt bij individuele managers. Het is goed gebruik voor elk bedrijfsmiddel een 'eigenaar' aan te wijzen, die vervolgens verantwoordelijk is voor de dagelijkse bescherming ervan.

6.1.2 Scheiding van taken

Beheersmaatregel
Taken en verantwoordelijkheden die (kunnen) conflicteren moeten zoveel mogelijk worden gescheiden zodat de kans op onbevoegd of onbedoeld wijzigen, of misbruik van de bedrijfsmiddelen van de organisatie, verminderd wordt.

Implementatierichtlijn
Het scheiden van taken en verantwoordelijkheden heeft als doelstelling het risico tot ongewenst wijzigen kleiner te maken. Dit wordt bereikt door minder toegang van personen tot gegevens, en het beperken van autonome toegang tot gegevens of middelen op die plekken of momenten waar dit beter gedaan kan worden door meerdere personen.

Er moet dus op worden gelet dat niemand ongemerkt of zonder autorisatie toegang kan krijgen tot bedrijfsmiddelen en ze daardoor kan wijzigen of gebruiken. Het kunnen uitvoeren van een (risicovolle) taak behoort te worden gescheiden van de autorisatie ervan. Daarbij moet rekening worden gehouden met de mogelijkheid van samenzwering.

Voor kleine organisaties kan het moeilijk zijn om taken te scheiden. Toch moet het principe zoveel mogelijk (naar haalbaarheid) worden toegepast. Wanneer het scheiden niet of onvoldoende lukt, moeten andere beheersmaatregelen zoals monitoring, auditing en supervisie worden overwogen.

6.1.3 Contact met overheidsinstanties

Beheersmaatregel
Indien er ten behoeve van informatiebeveiliging contacten met relevante overheidsinstanties nodig zijn, moeten deze contacten worden onderhouden en afspraken/werkwijzen worden gedocumenteerd.

Implementatierichtlijnen
Organisaties behoren procedures te hebben geïmplementeerd die beschrijven wanneer en door wie er met autoriteiten contact behoort te worden opgenomen (bijvoorbeeld politie, brandweer, toezichthouders) en hoe de vastgestelde informatiebeveiligingsincidenten tijdig behoren te worden gerapporteerd, indien het vermoeden bestaat dat er wetgeving is overtreden.

6.1.4 Contact met speciale belangengroepen

Beheersmaatregel
Indien relevant behoren er geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.
Implementatierichtlijnen
Het lidmaatschap van bepaalde belangengroeperingen of forums behoort te worden beschouwd als een middel om:

a. kennis te vergroten van beproefde werkwijzen ('best practices') en op de hoogte te blijven van de laatste stand van zaken op het gebied van informatiebeveiliging;
b. te waarborgen dat kennis en begrip van het vakgebied informatiebeveiliging volledig actueel en compleet zijn;
c. vroegtijdig signalen te krijgen van waarschuwingen, adviezen en 'patches' die verband houden met aanvallen en kwetsbaarheden;
d. toegang te verkrijgen tot deskundig informatiebeveiligingsadvies;
e. informatie over nieuwe technologieën, producten, bedreigingen of kwetsbaarheden te delen en uit te wisselen;
f. geschikte aanspreekpunten te leveren wanneer men te maken heeft met informatiebeveiligingsincidenten.

Overige informatie
Binnen een aantal sectoren van de grafische industrie zijn speciale sectorgroepen aanwezig. Een voorbeeld is de sector security printers. Ondernemingen kunnen t.a.v. informatiebeveiliging contacten onderhouden, respectievelijk het initiatief nemen voor kennisontwikkeling of het aanpakken van bepaalde vraagstukken. Ook op het gebied van regelgeving m.b.t. Direct Marketing, zijn diverse organisaties die informatie en kennis bieden over het gebruik van consumenten en Business to Business data.

6.1.5 Informatiebeveiliging in projectbeheer

Beheersmaatregel
Informatiebeveiliging moet altijd een onderwerp zijn bij projectbeheer.

Implementatierichtlijn
De organisatie moet informatiebeveiliging meenemen als een te beheersen onderwerp in projecten en daarvoor de juiste (project)beheermethode(s) voor hanteren. Deze methodes moeten de relevante risico's identificeren en waar nodig tegenmaatregelen nemen.

Dit geldt voor alle type projecten (van operationele, ondersteunende of verbeterende aard), of hierbij een IT component is of niet.

De gebruikte projectbeheermethoden moeten ervoor zorgen dat:

a. informatiebeveiligingsdoelstellingen worden opgenomen in projectdoelstellingen;
b. een risicobeoordeling van de impact van het project op informatiebeveiliging tijdig wordt uitgevoerd
c. zodat eventueel nodige beheersmaatregelen tijdig geïdentificeerd (en eventueel toegepast) kunnen worden.

d. informatiebeveiliging een onderdeel is van alle onderdelen (stappen of fasen) van de toegepaste projectmethodologie.

In alle projecten moeten de overwegingen voor informatiebeveiliging regelmatig worden behandeld en beoordeeld. De organisatie moet verantwoordelijkheden voor informatiebeveiliging definiëren en toewijzen aan specifieke rollen (die passen bij de organisatie en/of de projectbeheermethode).

6.2 Mobiele apparatuur en telewerken

Doel: Zorgen voor informatiebeveiliging bij het gebruik van draagbare computers (mobiele apparatuur) en faciliteiten voor telewerken op passend niveau van deze manier van werken.

6.2.1 Beleid voor mobiele apparatuur

Beheersmaatregel
Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

Implementatierichtlijnen
Bij het gebruik van draagbare computers en communicatievoorzieningen, zoals smartphones, tablets, behoren bijzondere voorzorgen te worden genomen om te waarborgen dat bedrijfsinformatie niet wordt gecompromitteerd. In het beleid voor mobiel computergebruik behoort rekening te worden gehouden met de risico's van het werken met draagbare computervoorzieningen in onbeschermde omgevingen.
Het beleid voor mobiel computergebruik behoort onder meer eisen te bevatten ten aanzien van fysieke bescherming, toegangsbeleid, cryptografische technieken, back-ups en virusbescherming. Zorgvuldigheid behoort in acht te worden genomen bij het gebruik van draagbare computerapparatuur in openbare gelegenheden, vergaderzalen en andere onbeschermde ruimten buiten het terrein van de organisatie. Van de gebruiker wordt een zorgvuldig beheer verwacht.

6.2.2 Telewerken/thuiswerken

Beheersmaatregel
Er behoren beleid, operationele plannen en procedures voor telewerken/thuiswerken te worden ontwikkeld en geïmplementeerd.

Implementatierichtlijnen
Organisaties behoren telewerken/thuiswerken alleen toe te laten indien bevredigende afspraken zijn gemaakt en beveiligingsmaatregelen zijn getroffen die in overeenstemming zijn met het beveiligingsbeleid van de organisatie.
De telewerklocatie behoort te zijn voorzien van geschikte bescherming, bijvoorbeeld tegen diefstal van apparatuur en informatie, onbevoegde openbaarmaking van informatie, onbevoegde toegang op afstand tot interne systemen van de organisatie of misbruik van voorzieningen. Het telewerken behoort zowel geautoriseerd als beheerst te worden door de directie en er behoren geschikte maatregelen te worden getroffen voor deze manier van werken.

De volgende punten behoren te worden overwogen:

a. de eisen op het gebied van communicatiebeveiliging, waarbij rekening behoort te worden gehouden met de behoefte aan toegang op afstand tot de interne systemen van de organisatie, de gevoeligheid van de informatie die wordt opgevraagd en die via de communicatieverbinding wordt verzonden, en de gevoeligheid van het interne systeem;
b. het risico van onbevoegde toegang tot informatie of middelen door andere gebruikers van de accommodatie, bijvoorbeeld familie en vrienden;
c. het gebruik van een VPN verbinding voor toegang op het bedrijfsnetwerk;
d. eisen aan antivirusbescherming en firewalls. Richtlijnen en afspraken die behoren te worden overwogen zijn onder meer:
   - definitie van het toegelaten werk, de werktijden, de classificatie van informatie waarover men mag beschikken en de interne systemen en diensten waartoe de telewerker toegang heeft;
   - regels en richtlijnen voor toegang door familie en bezoekers tot de apparatuur en de informatie;
   - het beschikbaar stellen van ondersteuning en onderhoud voor apparatuur en programmatuur;
e. procedures voor het maken van back-ups en voor de bedrijfscontinuïteit;
f. controleren van de beveiliging;
g. intrekken van bevoegdheden en toegangsrechten en inleveren van apparatuur na beëindiging van de telewerkactiviteiten.

7 VEILIG PERSONEEL

7.1 Voorafgaand aan het dienstverband

Doel: Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

De verantwoordelijkheden ten aanzien van beveiliging behoren vóór het dienstverband te worden vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden. Indien er producten worden verwerkt of geproduceerd waar veiligheidseisen m.b.t. informatie aan zijn verbonden dienen alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers op geschikte wijze te worden gescreend, in het bijzonder voor vertrouwensfuncties.

Werknemers, ingehuurd personeel en externe gebruikers die IT voorzieningen gebruiken behoren een overeenkomst te tekenen over hun beveiligingsrollen en –verantwoordelijkheden.

7.1.1 Screening

Beheersmaatregel
Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

Implementatierichtlijnen
De screening behoort rekening te houden met alle relevante wetgeving op het gebied van privacy, bescherming van persoonsgegevens en/of arbeidswetgeving, en behoort, mits toegelaten, het volgende mee te nemen:

a. controle van (de volledigheid en nauwkeurigheid van) het curriculum vitae van de sollicitant;
b. bevestiging van vermelde professionele kwalificaties;

c. onafhankelijke identiteitscontrole (paspoort of vergelijkbaar document).

Waar bij een eerste aanstelling of promotie sprake is van een functie waarbij de betrokkene toegang heeft tot IT voorzieningen met in het bijzonder waar gevoelige informatie wordt verwerkt, bijvoorbeeld financiële informatie of zeer vertrouwelijke informatie, behoort de organisatie eveneens verdere, meer gedetailleerde controles te overwegen, bijvoorbeeld op het hebben van een strafblad.

De criteria en beperkingen van de screening behoren in procedures te zijn gedefinieerd, bijvoorbeeld wie is gerechtigd om personen te screenen en hoe, wanneer en waarom screening wordt uitgevoerd.
Bij het werken met gevoelige informatie of waarde dragende materialen behoort een screeningproces ook te worden uitgevoerd voor ingehuurd personeel. Indien ingehuurd personeel via een uitzendbureau worden ingehuurd, behoren in het contract met dit bureau duidelijk de verantwoordelijkheden van het bureau te worden gespecificeerd ten aanzien van de screening en de meldingsprocedures die het bureau moet volgen indien de screening nog niet is voltooid of indien de resultaten aanleiding geven tot twijfel of zorg. Op overeenkomstige wijze behoren in de overeenkomst met de derde partij duidelijk de verantwoordelijkheden en de meldingsprocedures voor de screening te worden gespecificeerd.
Informatie over alle kandidaten die worden overwogen voor functies in de organisatie behoort te worden verzameld en verwerkt in overeenstemming met de geldende wet- en regelgeving in het relevante rechtsgebied. Afhankelijk van de toepasselijke wetgeving behoren de kandidaten van tevoren te worden geïnformeerd over de screeningactiviteiten.

7.1.2 Arbeidsvoorwaarden

Beheersmaatregel
Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.

Implementatierichtlijnen
De arbeidsvoorwaarden behoren naast overeenstemming met het beveiligingsbeleid van de organisatie duidelijk te maken en te vermelden:

a. dat alle werknemers, ingehuurd personeel en externe gebruikers die toegang krijgen tot gevoelige informatie een vertrouwelijkheids- of geheimhoudingsovereenkomst behoren te tekenen, voordat men toegang krijgt tot de IT voorzieningen;
b. de wettelijke verantwoordelijkheden en rechten van de werknemer, ingehuurde medewerker en elke andere gebruiker, bijvoorbeeld wat betreft auteursrecht- of wetgeving voor gegevensverwerking;
c. verantwoordelijkheden voor de classificatie van informatie en het beheer van bedrijfsmiddelen van de organisatie, die te maken hebben met informatiesystemen en -diensten die worden gehanteerd door de werknemer, ingehuurde medewerker of externe gebruiker;
d. verantwoordelijkheden van de werknemer, ingehuurde medewerker of externe gebruiker voor het verwerken van informatie die is ontvangen van andere bedrijven of externe partijen;
e. verantwoordelijkheden van de organisatie voor het verwerken van persoonlijke informatie, waaronder persoonlijke informatie gecreëerd als resultaat van of gedurende het dienstverband met de organisatie;
f. verantwoordelijkheden die zich uitstrekken buiten het terrein van de organisatie en buiten de normale kantooruren, bijvoorbeeld bij thuiswerken;
g. welke handelingen moeten worden uitgevoerd indien de werknemer, ingehuurde medewerker of een externe gebruiker de beveiligingseisen van de organisatie veronachtzaamt.

De organisatie behoort te waarborgen dat werknemers, ingehuurd personeel en externe gebruikers instemmen met de voorwaarden voor informatiebeveiliging die passend zijn voor de aard en de mate van

toegang die zij zullen hebben tot de bedrijfsmiddelen van de organisatie die verband houden met informatiesystemen en -diensten.

Overige informatie
Er mag een gedragscode worden gebruikt om de verantwoordelijkheden van werknemer, ingehuurde medewerker of externe gebruiker te dekken ten aanzien van vertrouwelijkheid, gegevensbescherming, ethiek, passend gebruik van de apparatuur en voorzieningen van de organisatie, evenals voor het eerzame handelen verwacht door de organisatie.

7.2 Tijdens het dienstverband

Doel: Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

Alle werknemers, al het ingehuurd personeel en alle externe gebruikers behoren over een passend niveau van bewustwording, opleiding en training in beveiligingsprocedures en het juiste gebruik van IT voorzieningen te beschikken om mogelijke beveiligingsrisico's te minimaliseren.

7.2.1 Directieverantwoordelijkheid

Beheersmaatregel
De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures en werkinstructies van de organisatie.

Implementatierichtlijnen
Tot de verantwoordelijkheden van de directie moeten behoren dat werknemers, ingehuurd personeel en externe gebruikers:

a. goed zijn ingelicht over hun informatiebeveiligingsrollen en -verantwoordelijkheden voordat de toegang wordt verleend tot gevoelige informatie of informatiesystemen;
b. zijn voorzien van richtlijnen die de beveiligingsverwachtingen van hun rol in de organisatie aangeven;
c. een zodanig niveau van competenties verwerven en bijhouden, als nodig voor hun rollen en verantwoordelijkheden binnen de organisatie;
d. handelen in overeenstemming met de arbeidsvoorwaarden, waarin het informatiebeveiligingsbeleid en gepaste werkmethoden van de organisatie zijn opgenomen.

7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beheersmaatregel
Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte instructie en waar nodig training en bijscholing te krijgen met betrekking tot beleid, procedures en werkzaamheden van de organisatie, voor zover relevant voor hun functie.

Implementatierichtlijnen
Bij de introductie van nieuwe IT voorzieningen behoort opleiding betreffende beveiligingseisen en bedrijfsbeheersmaatregelen, evenals training in het correcte gebruik van de IT voorzieningen.

Overige informatie
De activiteiten voor het aankweken van beveiligingsbewustzijn, opleiding en training behoren geschikt en van toepassing te zijn op de rol, verantwoordelijkheden en vaardigheden van de desbetreffende persoon. Binnen de organisatie kunnen medewerkers die deskundig en vaardig zijn ook de benodigde opleiding en training uitvoeren.

7.2.3 Disciplinaire maatregelen

Beheersmaatregel
Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

Implementatierichtlijnen
Het disciplinaire proces behoort niet te worden gestart zonder voorafgaande verificatie dat zich een inbreuk op de beveiliging heeft voorgedaan (zie ook 14.3.3 voor het verzamelen van bewijsmateriaal).
Het formele disciplinaire proces behoort te waarborgen dat werknemers die worden verdacht van inbreuk op de beveiliging een correcte en eerlijke behandeling krijgen. Het formele disciplinaire proces behoort te voorzien in een getrapte aanpak die rekening houdt met factoren als aard en ernst van de inbreuk en de gevolgen ervan voor de organisatie.

7.3 Beëindiging of wijziging van dienstverband

Doel: de belangen van de organisatie beschermen bij wijziging of beëindiging van het dienstverband.

7.3.1 Beëindiging van verantwoordelijkheden

Beheersmaatregel
De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.

Implementatierichtlijnen
Wijziging van verantwoordelijkheid of dienstverband behoort te worden behandeld als de beëindiging van de desbetreffende verantwoordelijkheid of het desbetreffende dienstverband en de nieuwe verantwoordelijkheid of het nieuwe dienstverband behoort te worden behandeld als beschreven in 3.1.1. Het is gewenst om klanten, personeel of externe gebruikers op de hoogte te stellen van de personeels- en functiewijzigingen indien dit relevant is.

8 BEHEER VAN BEDRIJFSMIDDELEN

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doel: Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie, die verband houden met IT voorzieningen. Alle bedrijfsmiddelen behoren te zijn verantwoord en aan een 'eigenaar' te zijn toegewezen. Voor alle bedrijfsmiddelen behoort een eigenaar bekend te zijn en er behoort te worden vastgelegd wie verantwoordelijk is voor het handhaven van geschikte beheersmaatregelen. De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.

8.1.1 Inventarisatie van bedrijfsmiddelen

Beheersmaatregel
Alle bedrijfsmiddelen die verband houden met IT voorzieningen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden. Er behoort een overzicht te zijn van de systeemarchitectuur waarin de IT voorzieningen zijn omschreven en de wijze waarop deze middels netwerkvoorzieningen gekoppeld zijn.

Implementatierichtlijnen
Een organisatie behoort alle bedrijfsmiddelen die verband houden met IT voorzieningen te identificeren. De inventarislijst van bedrijfsmiddelen behoort alle informatie te bevatten die nodig is voor herstel na een calamiteit, waaronder type bedrijfsmiddel, locatie, informatie over back-up en licenties en bedrijfswaarde. De inventarislijst behoeft geen onnodige duplicatie te zijn van andere inventarislijsten, maar er behoort op te worden gelet dat de inhoud daarmee is afgestemd.
Daarnaast behoort te worden overeengekomen en vastgelegd wie de eigenaar en wat de informatieclassificatie van elk van de bedrijfsmiddelen is. Op basis van het belang van het bedrijfsmiddel, de bedrijfswaarde en de beveiligingsclassificatie behoren er beschermingsniveaus te worden vastgesteld die passen bij het belang van de bedrijfsmiddelen.

Overige informatie
Voor grafische bedrijven zijn vooral onderstaande bedrijfsmiddelen in dit verband van belang:

a. informatie: databases en gegevensbestanden (Digital Asset Management systemen), contracten en overeenkomsten, systeemdocumentatie, logbestanden en andere registers, bedieningsprocedures en ondersteunende procedures, continuïteitsplannen, uitwijkregelingen, 'audit trails' en gearchiveerde informatie;
b. programmatuur: toepassingsprogrammatuur (waaronder integratie/workflows), systeemprogrammatuur, scripts (bijvoorbeeld Adobe Indesign scripting). ontwikkelingsprogrammatuur en hulpprogrammatuur;
c. fysieke bedrijfsmiddelen: computerapparatuur, netwerkapparatuur, communicatieapparatuur, back-up systemen en uitwisselbare media (waaronder dus ook de computerfaciliteiten in productiemachines)
d. diensten: computer- en communicatiediensten, algemene (nuts)voorzieningen.

Inventarislijsten zijn ook van toepassing voor kwaliteitszorg, milieu- en arbozorg.

8.1.2 Eigendom van bedrijfsmiddelen

Beheersmaatregel
Alle informatie en bedrijfsmiddelen die verband houden met IT voorzieningen behoren een 'eigenaar', d.w.z. een persoon die verantwoordelijk is voor het gebruik of beheer van een voorziening, te hebben in de vorm van een aangewezen deel van de organisatie.

Implementatierichtlijnen
De eigenaar van het bedrijfsmiddel behoort verantwoordelijk te zijn voor:
a. het waarborgen dat informatie en bedrijfsmiddelen die verband houden met IT voorzieningen op de juiste wijze worden geclassificeerd;
b. het definiëren en periodiek beoordelen van de toegangsbeperkingen en classificaties, daarbij rekening houdend met het van toepassing zijnde beleid voor toegangscontrole;
c. het zorgdragen voor het basisbeveiligingsniveau van de voorziening.

Het toewijzen van de 'eigenaar' kan zijn voor een bedrijfsproces, deel van activiteiten, een specifiek bedrijfsmiddel of IT voorziening.

8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Beheersmaatregel
Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT voorzieningen.

Implementatierichtlijnen
Alle werknemers, ingehuurd personeel en externe gebruikers behoren zich te houden aan de regels voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die te maken hebben met IT voorzieningen, waaronder:
a. regels voor elektronische post (e-mail) en gebruik van internet;
b. regels voor het gebruik van bedrijfsapplicaties, zoals web to print systemen en Management Informatie Systemen, onderhoudsmonitoring en procesmanagement systemen;
c. richtlijnen voor het gebruik van mobiele apparatuur, zoals laptops, mobiele telefoons en tablets, in het bijzonder voor gebruik buiten het terrein van de organisatie.

Er behoren specifieke regels of richtlijnen te worden verstrekt door het management. Werknemers, ingehuurd personeel en externe gebruikers die gebruikmaken van of toegang hebben tot de bedrijfsmiddelen van de organisatie behoren zich bewust te zijn van de grenzen die bestaan voor hun gebruik van de informatie en bedrijfsmiddelen die te maken hebben met IT voorzieningen en hulpmiddelen. Zij behoren verantwoordelijk te zijn voor hun gebruik van informatievoorzieningen en voor elk gebruik uitgevoerd onder hun verantwoordelijkheid.

8.1.4 Retournering van bedrijfsmiddelen

Beheersmaatregel
Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

Implementatierichtlijnen
In het beëindigingproces behoort formeel te worden vastgelegd dat alle eerder verstrekte programmatuur, bedrijfsdocumenten en apparatuur wordt teruggegeven. Andere bedrijfsmiddelen zoals draagbare computerapparatuur, mobiele telefoon, creditcards, toegangskaarten, programmatuur, handboeken en informatie opgeslagen op elektronische media moeten ook worden teruggegeven.
Wanneer een werknemer, ingehuurde medewerker of externe gebruiker apparatuur van de organisatie koopt of zijn eigen persoonlijke apparatuur gebruikt, behoren er procedures te worden gevolgd om te waarborgen dat alle relevante informatie wordt overgedragen aan de organisatie en nauwkeurig wordt gewist van de apparatuur.

Wanneer een werknemer, ingehuurde medewerker of externe gebruiker beschikt over kennis die belangrijk is voor de lopende bedrijfsvoering, behoort die informatie te worden gedocumenteerd en overgedragen aan de organisatie.

8.2 Informatieclassificatie

Doel: Ervoor zorgen dat informatie een geschikt niveau van bescherming krijgt. Op basis van een goede classificatie is het mogelijk om bij informatieverwerking de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven. Informatie kan in meerdere of mindere mate gevoelig of kritisch zijn. Voor een deel van de informatie binnen een organisatie kan extra bescherming of een speciale verwerking nodig zijn. Er moet een informatieclassificatieschema worden opgesteld en toegepast om de juiste niveaus van bescherming te definiëren en de momenten wanneer aparte verwerkingsmaatregelen dienen te worden toegepast te communiceren.

8.2.1 Classificatie van informatie

Beheersmaatregel
Informatie behoort te worden geïnventariseerd en vervolgens worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie en/of voor de klant. De informatiestromen worden beschreven in een informatiestroom diagram.

Implementatierichtlijnen
Het inventariseren van de informatie wordt gedaan door het opstellen van een informatiestroom diagram. Een informatiestroom diagram is een grafische voorstelling van de informatiestromen in een organisatie en tussen organisaties.
Classificaties en de bijbehorende beschermende beheersmaatregelen voor informatie behoren rekening te houden met de zakelijke behoefte aan het delen van informatie of het beperken ervan en de invloed van deze behoeften op het bedrijf. Het classificatieschema behoort eenvoudig te zijn, door gebruik te maken van een beperkt aantal classificatiecategorieën.

Overige informatie
Het beschermingsniveau kan worden beoordeeld door het analyseren van de vertrouwelijkheid, integriteit en beschikbaarheid en eventuele andere eisen voor de informatie die wordt beschouwd.
Na verloop van tijd is informatie vaak niet langer gevoelig of kritiek, bijvoorbeeld wanneer de informatie is openbaar gemaakt. Ook daarmee behoort rekening te worden gehouden, omdat te zware classificatie (overclassificatie) kan leiden tot de implementatie van overbodige beheersmaatregelen die leiden tot onnodige extra uitgaven.

8.2.2 Labeling en verwerking van informatie

Beheersmaatregel
Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

Implementatierichtlijnen
De procedures voor het labelen van informatiebedrijfsmiddelen moeten zowel fysieke als elektronische hulpmiddelen omvatten. Uitvoer van systemen die informatie bevatten die als gevoelig of kritiek wordt geclassificeerd, behoort van het benodigde classificatielabel (in de uitvoer) te zijn voorzien. Het label behoort de classificatie te weer te geven volgens de regels van 2.2.1. Items die hiervoor in aanmerking komen zijn afgedrukte rapporten, weergaven op het beeldscherm, beschreven media (bijvoorbeeld tapes, schijven, cd's), Opslagsystemen/Back-up systemen (Raid systemen, NAS, etc.) elektronische berichten en bestandsoverdrachten (inclusief FTP infrastructuur).
Voor elk classificatieniveau behoren verwerkingsprocedures te worden opgesteld, waaronder beveiligd verwerken, opslag, transmissie, declassificatie en vernietiging. Hierbij horen ook de procedures voor de beheersketen en voor het registreren van gebeurtenissen die relevant zijn voor de beveiliging.
Overeenkomsten met externe partijen waarin het delen van informatie aan de orde is behoren procedures te omvatten voor de identificatie van de classificatie van die informatie en voor het interpreteren van de classificatielabels van andere organisaties.

Overige informatie
Het labelen van digitale informatie verloopt via een beschrijving van een procedure of via metadata.

8.2.3 Behandelen van bedrijfsmiddelen

Beheersmaatregel

Bedrijfsmiddelen moeten worden behandeld op een bij de informatieclassificatie passende wijze; hiervoor moeten procedures voor worden ontwikkeld en geïmplementeerd.

Implementatierichtlijnen
De procedures moeten rekening houden met het hanteren, verwerken, opslaan en communiceren van informatie. Daarbij moet er rekening worden gehouden met het volgende:

a. Toegangsbeperkingen, passend bij de beschermingseisen van de verschillende classificatieniveau ‘s;
b. een actuele registratie van de bevoegde ontvangers van bedrijfsmiddelen;
c. bescherming van tijdelijke of permanente kopieën van informatie, consistent met het niveau van de originele informatie;
d. opslag van IT-middelen op een wijze die consistent is met de fabrikantsvoorschriften;
e. duidelijke identificatie en markering van kopieën van media ter attentie van de bevoegde ontvanger(s);

Overige informatie
Het is zeer waarschijnlijk dat classificatieniveau ‘s en de beschermingseisen per classificatieniveau verschillen tussen organisaties. Door organisatie A als vertrouwelijk gelabelde informatie kan bij organisatie B zeer vertrouwelijk geacht worden. De aansluiting van de classificatieschema’s en bijbehorende labeling is dus van belang bij het vaststellen van overeenkomsten tussen organisaties.

Voor de grafische industrie is met name punt c van belang. Het fysieke eindproduct, afval, platen, modellen, en gegevens in productiemachines / software: het zijn allemaal kopieën die beschermd moeten worden.

8.3 Bescherming van media

Doel: Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van media die van belang zijn voor de bedrijfsactiviteiten.

Media behoren te worden beschermd. Er behoren passende procedures te worden vastgesteld om documenten, opslagmedia (bij voorbeeld banden, schijven), in- en uitvoergegevens en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging

8.3.1 Beheer van transporteerbare media

Beheersmaatregel
Er behoren procedures te zijn vastgesteld voor het beheer van transporteerbare media.

Implementatierichtlijnen
De volgende richtlijnen voor het beheer van transporteerbare media behoren te worden overwogen:

a. Van alle transporteerbare media die de organisatie verkrijgt (t.b.v. productiewerkzaamheden) behoort een registratie te zijn, met daarin beschrijving van het eigendom, aard van de data, vereisten aan beheer en teruglevering of verwijdering;
b. van herbruikbare media die de organisatie verlaten behoort de inhoud, als die niet meer nodig is, te worden gewist;
c. waar nodig en toepasbaar, behoort goedkeuring te worden verkregen voor alle media die de organisatie verlaten en al dergelijke verwijderingen behoren te worden geregistreerd om een ‘audit trail’ te creëren;
d. alle media behoren te worden bewaard in een veilige en in een juist geconditioneerde omgeving, overeenkomstig de instructies van de fabrikant;
e. informatie die langer beschikbaar moet zijn dan de levensduur van de media waarop hij is opgeslagen (overeenkomstig de specificaties van de fabrikant) behoort ook elders te worden opgeslagen om verlies van informatie door veroudering van de media te voorkomen;
f. Alle procedures en autorisatieniveaus behoren duidelijk te worden gedocumenteerd.

Tot de transporteerbare media worden o.a. gerekend: banden (tapes), schijven, flashgeheugenkaarten, USB sticks, transporteerbare harde schijven, cd's, dvd's en gedrukte media.

8.3.2 Verwijdering van media

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

Implementatierichtlijnen
Formele procedures voor het beveiligd verwijderen van media behoren het risico dat gevoelige informatie bij een onbevoegd persoon komt, zo klein mogelijk te maken. De procedures voor beveiligd verwijderen van media met gevoelige informatie behoren in verhouding te staan tot de gevoeligheid van die informatie. De volgende punten behoren te worden overwogen:

a. er behoren procedures te zijn voor het identificeren van de media met gevoelige informatie;
b. media die gevoelige informatie bevatten behoren op een beveiligde en veilige manier te worden opgeslagen en verwijderd, bijvoorbeeld door verbranding of versnippering, of de gegevens behoren te worden gewist voordat de media worden gebruikt in een andere toepassing binnen de organisatie;
c. het kan handiger zijn om alle media die moeten worden afgevoerd te verzamelen en veilig te verwijderen, in plaats van te proberen alle gevoelige media te scheiden;

d. wanneer verzamel- en verwijderdiensten voor papier, apparatuur en media, van externe bedrijven wordt ingehuurd behoort een geschikt bedrijf te worden geselecteerd met adequate beheersmaatregelen en ervaring;
e. het verwijderen van gevoelige gegevens behoort zoveel mogelijk te worden geregistreerd teneinde een 'audit trail' te handhaven.

8.3.3 Fysieke media die worden getransporteerd

Beheersmaatregel
Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport buiten de fysieke begrenzing van de organisatie.

Implementatierichtlijnen
De volgende richtlijnen behoren te worden overwogen voor het beschermen van informatie die tussen locaties wordt getransporteerd:
a. er behoren betrouwbare transport- of koeriersdiensten te worden gebruikt;
b. de directie behoort een lijst van bevoegde koeriers goed te keuren;
c. er behoren procedures voor het controleren van de identificatie van koeriers te worden ontwikkeld;
d. de verpakking behoort afdoende bescherming te bieden tegen fysieke schade die tijdens transport kan optreden, en behoort in overeenstemming te zijn met de specificaties van de fabrikant (bijvoorbeeld voor programmatuur), bijvoorbeeld bescherming tegen omgevingsomstandigheden die het herstelvermogen van de media verminderen, zoals blootstelling aan warmte, vocht of elektromagnetische velden;
e. ondernemingen die direct mail of andere vormen van geadresseerd drukwerk in opdracht versturen behoren te waarborgen dat de aanlevering aan de verzender correct is. Indien door de klant gewenst behoort de dienstverlener daarvoor een 'audit trail' bij te houden;
f. waar nodig, bijvoorbeeld het aanleveren van informatie voor het produceren van vermogensrapportages of jaarverslagen, behoren bijzondere beheersmaatregelen te worden genomen om gevoelige informatie te beschermen tegen onbevoegde openbaarmaking of wijziging; bijvoorbeeld:
   - gebruik van afgesloten ruimte of opslagkasten;
   - persoonlijke aflevering;
   - gebruik van verpakkingsmateriaal waaraan direct te zien is of iemand heeft geprobeerd het pakket te openen;
   - in uitzonderlijke gevallen, opsplitsing van de zending in meer delen en verzending via verschillende routes.

Overige informatie
Informatie kan gevoelig zijn voor toegang door onbevoegden, misbruik of datacorruptie tijdens fysiek transport, bijvoorbeeld wanneer media per post of koerier worden verzonden.

9 TOEGANGSBEVEILIGING

9.1 Bedrijfseisen ten aanzien van toegangsbeheersing

Doel: Beheersen van de toegang tot informatie.

De toegang tot informatie, IT voorzieningen en bedrijfsprocessen behoort te worden beheerst op grond van bedrijfsbehoeften en beveiligingseisen. In de regels voor toegangsbeveiliging behoort rekening te worden gehouden met beleid ten aanzien van informatieverspreiding en autorisatie.

9.1.1 Toegangsbeleid

Beheersmaatregel
Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

Implementatierichtlijnen
In een beleidsverklaring voor toegangsbeveiliging behoren voor elke gebruiker of gebruikersgroep duidelijke regels en rechten te zijn vastgelegd voor het toegangsbeleid. De toegangsbeleidsmaatregelen zijn zowel logisch als fysiek en behoren als een geheel te worden beschouwd. Gebruikers en dienstverlenende bedrijven behoren een duidelijke verklaring te krijgen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiliging moet voldoen.

In het beleid behoort rekening te worden gehouden met de volgende aspecten:
a. beveiligingseisen voor afzonderlijke bedrijfstoepassingen;
b. identificatie van alle informatie die verband houdt met de bedrijfstoepassingen en de risico's waaraan de informatie kan worden blootgesteld;
c. beleid ten aanzien van informatieverspreiding en -autorisatie, bijvoorbeeld op basis van behoefte ('need-to- know'-principe), beveiligingsniveaus en classificatie van informatie;
d. afstemming van beleid voor toegangsbeveiliging en classificatie van informatie voor verschillende systemen en netwerken;
e. relevante wetgeving en eventuele contractuele verplichtingen ten aanzien van bescherming van toegang tot gegevens of diensten (conform de afspraken met klanten);
f. standaard gebruikersprofielen met toegangsrechten voor veelvoorkomende rollen in de organisatie;
g. beheer van toegangsrechten in een (gedistribueerde) netwerkomgeving, waarbij rekening wordt gehouden met alle beschikbare typen verbindingen;
h. scheiding van toegangsbeveiligingsrollen bijvoorbeeld toegangsverzoek, toegangsautorisatie, toegangsadministratie;
i. eisen voor formele autorisatie van toegangsverzoeken;
j. eisen voor periodieke beoordeling van toegangsbeveiliging;
k. intrekken van toegangsrechten.

9.1.2 Toegang tot netwerken en netwerkdiensten

Beheersmaatregel
Gebruikers moeten alleen toegang krijgen tot de netwerken en netwerkdiensten waar ze specifiek bevoegd voor zijn.

Implementatierichtlijnen
Er moet een beleid geformuleerd worden voor het gebruik van netwerken en netwerkdiensten. In dat beleid behoort aanwezig te zijn:

a. de betreffende netwerken en –diensten waar toegang tot wordt verleend;
b. de autorisatieprocedures zodat vastgesteld kan worden wie toegang krijgt tot welke netwerken en netwerkdiensten;
c. de beheersmaatregelen en beheersprocedures die deze toegang beschermen;
d. de middelen / methodes die worden gebruikt om toegang te krijgen tot netwerken of netwerkdiensten;
e. de eisen voor authenticatie van gebruikers voor de toegang tot verschillende netwerken en netwerkdiensten;
f. hoe het gebruik van de netwerken en netwerkdiensten gemonitord wordt.

Dit beleid moet aansluiten bij het toegangsbeleid (zie 9.1.1).

Overige informatie
Onveilige toegang tot netwerkdiensten en met name netwerken kunnen zeer schadelijk zijn. Speciale aandacht is vooral noodzakelijk bij bedrijfskritische toepassingen of informatie, of bij toegang vanuit (openbare) plekken met hoog risico. Om deze reden is het verstandig aparte, of aanvullende, toegangsregels of maatregelen te treffen voor deze situaties.

9.2 Beheer van toegangsrechten van gebruikers

Doel: Het voorkomen van onbevoegde toegang tot netwerkdiensten.

De gebruikerstoegang tot netwerken en netwerkdiensten behoort de veiligheid hiervan niet in gevaar brengen. Dit kan worden gerealiseerd door te zorgen voor:
a. geschikte interfaces tussen het netwerk van de organisatie en netwerken van andere organisaties, en openbare netwerken;
b. geschikte authenticatiemiddelen voor gebruikers en apparatuur;
c. strikte beheersing van toegang tot informatiediensten.

9.2.1 Registratie en afmelden van gebruikers

Beheersmaatregel
Om toewijzing van toegangsrechten mogelijk te maken dient er een formele procedure te zijn geïmplementeerd voor registratie en afmelding.

Implementatierichtlijn

In de procedure moet aanwezig zijn:
a. het gebruik van unieke gebruikersidentificaties waardoor gebruikers kunnen worden gekoppeld aan hun acties (en verantwoordelijk kunnen worden gehouden). (Groepsidentificaties horen alleen te worden toegelaten als deze noodzakelijk zijn en moeten worden goedgekeurd en gedocumenteerd);
b. het direct ongeldig maken en/of verwijderen van de gebruikersidentificatie van gebruikers die de
c. organisatie hebben verlaten (zie 9.2.6);
d. op gezette momenten overbodige gebruikersidentificaties identificeren en verwijderen;
e. de manier waarop er voor gezorgd wordt dat (overtollige) gebruikersidentificaties niet aan andere gebruikers worden uitgegeven.

Overige informatie
Bij het maken of verwijderen van gebruikersidentificaties zijn er meestal twee stappen die doorlopen worden.
a. een gebruikersidentificatie maken of toewijzen en activeren, of intrekken; hierdoor ontstaat een unieke entiteit (welke toegang kan krijgen tot systemen onder deze eigen identiteit)
b. toegangsrechten aan deze gebruikersidentificatie verlenen of intrekken (zie 9.2.2).

Het deactiveren van een identificatie is algemeen genomen een snellere handeling dan het individueel verwijderen van rechten: door het deactiveren van een identificatie worden in de praktijk vaak niet alle toegangsmogelijkheden tot systemen in de organisatie direct opgeheven.

9.2.2 Gebruikers toegang verlenen

Beheersmaatregel
Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.

Implementatierichtlijnen
De procedure voor toegangsbeveiliging voor registratie en afmelden van gebruikers behoort te omvatten:
a. gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen; het gebruik van groepsidentificatie behoort alleen te worden toegelaten als dat noodzakelijk is om bedrijfs- of operationele redenen en behoort te worden goedgekeurd en gedocumenteerd;
b. controleren dat de gebruiker door de systeemeigenaar is geautoriseerd voor het gebruik van het informatiesysteem of de informatiedienst; afzonderlijke goedkeuring van de directie met betrekking tot toegangsrechten kan ook terecht zijn;
c. controleren dat het toegewezen toegangsniveau geschikt is voor de bedrijfstoepassing en consistent is met het beveiligingsbeleid van de organisatie;
d. gebruikers te informeren en verplichten een verklaring te ondertekenen waarin ze aangeven de voorwaarden voor de toegang te begrijpen en zullen naleven;
e. waarborgen dat dienstverlenende bedrijven geen toegang verlenen totdat de autorisatieprocedures zijn voltooid;
f. een formele registratie bijhouden van alle personen die geregistreerd zijn als gebruikers van de dienst;
g. onmiddellijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd of de organisatie hebben verlaten;
h. periodieke controle op en verwijderen of blokkeren van overtollige gebruikersaccounts en waarborgen dat overtollige gebruikers-ID's niet aan andere gebruikers worden uitgegeven.

9.2.3 Beheer van speciale bevoegdheden

Beheersmaatregel
De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.

Implementatierichtlijnen
Voor informatiesystemen met meer gebruikers die bescherming tegen toegang door onbevoegden vereisen (bijvoorbeeld voor de productie van gevoelige producties, zoals vermogensrapportages), behoort een formeel autorisatieproces te worden vastgesteld voor de toewijzing van speciale bevoegdheden. Hierbij behoren de volgende stappen te worden overwogen:
a. de speciale bevoegdheden behorend bij elke systeemcomponent, bijvoorbeeld een Digital Asset Management systeem en elke toepassing die voor een betreffende productie wordt gebruikt, en de gebruikers aan wie deze bevoegdheden moeten worden toegewezen behoren te worden vastgesteld;
b. gebruikers behoren alleen die speciale bevoegdheden toegewezen te krijgen die voor hun functie echt nodig zijn (‘need-to-use’) en in overeenstemming met het beleid ten aanzien van het toegangsbeleid, d.w.z. wat ze minimaal nodig hebben om hun functie uit te oefenen op een moment dat het nodig is;
c. er behoort een autorisatieproces te worden gehanteerd en een registratie te worden bijgehouden van alle toegewezen speciale bevoegdheden; er behoren geen bevoegdheden te worden verleend voordat dit autorisatieproces is voltooid;
d. het ontwikkelen en gebruiken van systeemroutines behoort te worden aangemoedigd om het verlenen van speciale bevoegdheden aan gebruikers te vermijden;

9.2.4 Beheer van gebruikerswachtwoorden

Beheersmaatregel
De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.

Implementatierichtlijnen
Het proces behoort de volgende eisen te omvatten:
a. gebruikers behoren te worden verplicht een verklaring te ondertekenen dat zij hun persoonlijke wachtwoorden geheimhouden en groepswachtwoorden uitsluitend aan leden van de groep kenbaar maken; deze ondertekende verklaring kan worden opgenomen in het arbeidscontract;
b. wanneer gebruikers hun eigen wachtwoorden moeten bijhouden, behoren ze aanvankelijk een beveiligd tijdelijk wachtwoord toegewezen te krijgen dat ze onmiddellijk moeten wijzigen;
c. procedures vaststellen om de identiteit van een gebruiker te controleren voordat hem een nieuw, vervangend of tijdelijk wachtwoord wordt verstrekt;
d. tijdelijke wachtwoorden behoren op een veilige manier te worden uitgegeven aan gebruikers; gebruik via derden of gebruik van onbeschermde e-mailberichten (ongecodeerde tekst) behoort te worden vermeden;
e. tijdelijke wachtwoorden behoren uniek te zijn voor een persoon en mogen niet te raden zijn;
f. gebruikers behoren de ontvangst van wachtwoorden te bevestigen;
g. wachtwoorden behoren nooit in onbeschermde vorm te worden opgeslagen op computersystemen;
h. standaardwachtwoorden van leveranciers behoren te worden veranderd na installatie van systemen of programmatuur.

9.2.5 Beoordeling van toegangsrechten van gebruikers

Beheersmaatregel
De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

Implementatierichtlijnen
Bij de beoordeling van toegangsrechten behoren de volgende richtlijnen te worden overwogen:
a. toegangsrechten van gebruikers behoren met regelmatige tussenpozen te worden beoordeeld, bijvoorbeeld elk jaar en na wijzigingen, zoals functiewijziging of beëindiging van het dienstverband;
b. wijzigingen van speciale accounts behoren te worden geregistreerd voor periodieke beoordeling.

9.2.6 Blokkering van toegangsrechten

Beheersmaatregel
De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

Implementatierichtlijnen
Bij beëindiging van dienstverband behoren de toegangsrechten van een persoon tot de bedrijfsmiddelen die verband houden met informatiesystemen en diensten te worden beoordeeld. Hieruit zal blijken of het nodig is om de toegangsrechten in te trekken. Verandering van dienstverband behoort te worden weerspiegeld in het intrekken van toegangsrechten die niet zijn goedgekeurd voor het nieuwe dienstverband. Tot de toegangsrechten die behoren te worden ingetrokken of aangepast behoren fysieke en logische toegang, sleutels, legitimatiebewijzen, IT voorzieningen, abonnementen en het verwijderen van alle documentatie die hen identificeert als een huidig lid van de organisatie. Indien een vertrekkende werknemer, ingehuurde medewerker of externe gebruiker bekende wachtwoorden heeft voor toegang tot IT voorzieningen die actief

blijven, behoren deze te worden gewijzigd bij beëindiging of wijziging van dienstverband, contract of overeenkomst.

9.3 Verantwoordelijkheden van gebruikers

Doel: Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT voorzieningen.

Doeltreffende beveiliging vereist de medewerking van geautoriseerde gebruikers. Gebruikers behoren op de hoogte te worden gebracht van hun verantwoordelijkheid voor het handhaven van doeltreffende toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur.

9.3.1 Gebruik van wachtwoorden

Beheersmaatregel
Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

Implementatierichtlijnen
Alle gebruikers behoren het advies te krijgen om:

a. wachtwoorden geheim te houden;
b. wachtwoorden niet vast te leggen (bijvoorbeeld op papier, in bestand of in handcomputer), tenzij deze registratie veilig kan worden opgeslagen en de methode van opslag is goedgekeurd;
c. wachtwoorden te wijzigen zodra er aanwijzingen zijn dat het systeem of het wachtwoord mogelijk gecompromitteerd is;
d. een wachtwoord van voldoende minimumlengte te kiezen, dat:
   - gemakkelijk te onthouden is;
   - niet is gebaseerd op iets dat iemand anders gemakkelijk zou kunnen raden of verkrijgen door gebruik te maken van persoonsgerelateerde informatie, zoals namen, telefoonnummers en geboortedata enz.;
   - de sterkte van het wachtwoord aan de gebruiker kenbaar te maken;
   - niet kwetsbaar is voor woordenboekaanvallen (d.w.z. niet bestaat uit woorden die in een woordenboek voorkomen);
   - geen opeenvolgende gelijke tekens bevat en niet uitsluitend uit numerieke of alfabetische tekens bestaat;
e. wachtwoorden met regelmatige tussenpozen of op basis van het aantal malen dat men toegang tot het systeem heeft gehad te wijzigen (wachtwoorden voor accounts met speciale bevoegdheden moeten vaker worden gewijzigd dan normale wachtwoorden) en hergebruik of rouleren van oude wachtwoorden te voorkomen;
f. tijdelijke wachtwoorden bij eerste inlog te wijzigen;
g. geen wachtwoorden te gebruiken in automatische inlogprocessen bijvoorbeeld opgeslagen in een macro of onder een functietoets;
h. geen individuele wachtwoorden met anderen te delen;

Indien gebruikers toegang nodig hebben tot meer diensten of platforms en meer afzonderlijke wachtwoorden moeten onderhouden, behoren zij het advies te krijgen om één goed gekozen wachtwoord te gebruiken voor alle diensten, mits de gebruiker ervan verzekerd is dat een redelijk niveau van bescherming wordt geboden voor de opslag van het wachtwoord binnen elk(e) dienst, systeem of platform.

9.4 Toegangsbeheersing voor informatiesystemen en informatie

Doel: Voorkomen van onbevoegde toegang tot informatie in informatiesystemen.

Er behoren beveiligingsvoorzieningen te worden getroffen om toegang tot en binnen informatiesystemen te beperken.

9.4.1 Beperken van toegang tot informatie

Beheersmaatregel
Toegang tot informatie en functies van informatiesystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.

Implementatierichtlijnen
De toegangsbeperkingen behoren te zijn gebaseerd op de beveiligingseisen voor afzonderlijke informatiesystemen. Het toegangsbeleid behoort ook in overeenstemming te zijn met het toegangsbeleid van de organisatie.
Het toepassen van de volgende richtlijnen behoort te worden overwogen om toegangsbeperkende maatregelen te ondersteunen:

a. het gebruik van menu's om toegang tot functies van het informatiesysteem te beheersen;
b. beheersen van toegangsrechten van gebruikers, bijvoorbeeld lezen, schrijven, verwijderen, uitvoeren;
c. beheersen van de toegangsrechten tot andere toepassingen;
d. waarborgen dat de uitvoer van informatiesystemen waarmee gevoelige informatie wordt verwerkt, alleen gegevens bevat die relevant zijn voor het gebruiksdoel van de uitvoer en dat deze alleen wordt verzonden naar computerterminals en locaties met een autorisatie; tevens moet deze uitvoer regelmatig worden beoordeeld om te waarborgen dat overtollige informatie wordt verwijderd.

9.4.2 Beveiligde inlogprocedures

Beheersmaatregel
Toegang tot systemen en toepassingen moet worden beheerst door een beveiligde wijze van inloggen (indien het beleid voor toegangsbeveiliging dit vereist)

Implementatierichtlijn
Een gebruiker van een systeem identificeert zichzelf door middel van een identificatiekenmerk (gebruikersnaam). Om de authenticiteit van de gebruiker te bewijzen dient een authenticatietechniek te worden toegepast die de risico's van toegang tot dat systeem afdoende beheerst.

Op basis van dat risico kan het nodig zijn sterkere methoden te gebruiken dan alleen wachtwoorden, zoals cryptografische middelen (uitdelen van tijdelijke cryptkeys), chipkaarten, tokens (druppels) of biometrische middelen (vingerafdruk, retina scan).

De methode om in te loggen moet zo ontworpen zijn dat de kans op onbevoegde toegang zo klein mogelijk is – de methode moet zelf dus ook geen informatie prijsgeven waardoor deze kwetsbaarder zou worden.

Een goede inlogmethode moet daarom:

a. geen feedback met inhoudelijk informatie over het inlogsysteem of inlogmethode(/software) te tonen voordat het inlogproces met succes is afgerond;
b. alle gebruikers waarschuwen dat de computer of het systeem alleen toegankelijk is voor bevoegde gebruikers;

c. tijdens de inlogprocedure geen (overbodige) hulpboodschappen weer geven waarmee onbevoegde gebruikers (mede) gemakkelijker toegang krijgen;
d. de inloginformatie pas na invoer van alle gegevens valideren en bij niet-geslaagde validatie moet het systeem niet aangeven welk deel van de gegevens (on)juist is.
e. gehard zijn tegen inlogpogingen die met grove middelen worden uitgevoerd (brute force attacks, dictionary attacks);
f. zowel niet-succesvolle als succesvolle pogingen registreren;
g. automatisch melding maken van een informatiebeveiligingsgebeurtenis (of incident) wanneer een gepoogde aanval of geslaagde schending van de beveiligingsmaatregelen in de inlogmethode wordt gedetecteerd;
h. een wachtwoord dat wordt ingevoerd niet weergeven (waaronder eventuele korte weergave van het laatst ingevoerde teken);
i. geen ongecodeerde wachtwoorden via een netwerk versturen;
j. inactieve sessies na een bepaalde tijd van inactiviteit beëindigen, vooral op locaties met een hoog
k. risico, zoals openbare of externe locaties die buiten het beveiligingsbeheer van de organisatie vallen, of op mobiele apparaten;
l. de verbindingstijd beperken om extra beveiliging te bieden voor toepassingen met een hoog risico en de mogelijkheden voor onbevoegde toegang te verkleinen.
m. informatie tonen nadat het inloggen met succes is voltooid (zodat de gebruiker eigen validatie toe kan passen):
    - datum en tijdstip van de voorliggende succesvolle inlog;
    - details van niet-succesvolle pogingen om in te loggen sinds de vorige succesvolle inlog;

Overige informatie
De meest gangbare vorm van identificatie en authenticatie is op basis van wachtwoorden (die alleen unieke gebruikers kennen. Voor wachtwoorden (zowel beheer als gebruikersgedrag) gelden best practices.

9.4.3 Systeem voor wachtwoordbeheer

Beheersmaatregel
Systemen voor wachtwoordbeheer moeten passend bij het risiconiveau worden toegepast, interactief zijn en sterke wachtwoorden afdwingen.

Implementatierichtlijn
Een systeem voor wachtwoordbeheer ondersteunt zowel beheerders als gebruikers bij het uitvoeren van hun taken in overeenstemming met het beveiligingsbeleid. Zo'n systeem versterkt het wachtwoordbeheer door:
a. individuele gebruikersidentificaties en wachtwoorden af te dwingen;
b. gebruikers hun eigen wachtwoord te kunnen laten kiezen en wijzigen, met een bevestigingsprocedure ter bescherming tegen foutieve invoer;
c. sterke wachtwoorden af te dwingen;
d. gebruikers te dwingen hun wachtwoord bij het eerste inloggen op te geven of te wijzigen;
e. wijzigen van het wachtwoord periodiek en wanneer nodig af te dwingen;
f. eerder gebruikte wachtwoorden bij te houden om 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;
i. wachtwoorden in beschermde vorm op te slaan en te versturen.

Overige informatie
Het kan zijn dat wachtwoorden geheel opgelegd worden door een externe instantie. In dat geval vervallen een aantal punten. Dit, en ook het periodiek afdwingen van nieuwe wachtwoorden kan leiden tot het opschrijven van wachtwoorden door de gebruiker – dit kan een nieuwe beveiligingsrisico introduceren.

9.4.4 Speciale systeemhulpmiddelen gebruiken

Beheersmaatregel
(Systeem)hulpmiddelen die beveiligings-/beheersmaatregelen voor systemen en toepassingen kunnen omzeilen, moeten worden beperkt en nauwkeurig gecontroleerd.

Implementatierichtlijn
Hulpmiddelen die beheersmaatregelen kunnen omzeilen zijn soms niet uit te sluiten. Voor het gebruik hiervan moeten de volgende richtlijnen worden overwogen:

a. aparte identificatie-, authenticatie- en autorisatiemethoden voor (ad-hoc) systeemhulpmiddelen;
b. scheiding van systeemhulpmiddelen en toepassingssoftware;
c. het onmogelijk maken van installatie van systeemhulpmiddelen;
d. beperking van het gebruik van systeemhulpmiddelen;
e. beperking van de beschikbaarheid van systeemhulpmiddelen, bijv. voor de duur van een (geautoriseerde) wijziging;
f. registreren van het gebruik van systeemhulpmiddelen;
g. de relevante autorisatieniveaus voor systeemhulpmiddelen definiëren en vastleggen in registers;
h. alle onnodige systeemhulpmiddelen verwijderen, deactiveren of onbruikbaar maken;
i. niet beschikbaar stellen van systeemhulpmiddelen aan gebruikers die toegang hebben tot toepassingen op systemen waarbij scheiding van taken vereist is.

Overige informatie
De meeste computersystemen hebben een of meer systeemhulpmiddelen die in staat zijn beheersmaatregelen voor systemen en toepassingen te omzeilen. Denk hierbij ook aan database-beheer systemen waardoor een databasebeheerder de normale beveiligingsmaatregelen van een applicatie kan omzeilen.

9.4.5 Toegangsbeheersing voor broncode van programmatuur

Beheersmaatregel
De toegang tot broncode van programmatuur behoort te worden beperkt.

Implementatierichtlijnen
Toegang tot programmabroncode en daarmee verbonden zaken (zoals ontwerpen, specificaties, verificatie- en validatieplannen) behoort nauwgezet te worden beheerst om het invoeren van onbevoegde functionaliteit te voorkomen en onbedoelde wijzigingen te vermijden. Dit kan voor programmabroncode worden bereikt met behulp van een beheerste centrale opslag van de code, bij voorkeur in broncodebibliotheken. De volgende richtlijnen behoren dan te worden overwogen om de toegang tot deze broncodebibliotheken te beheersen en zo de kans op corruptie van computerprogramma's te verminderen:

a. waar mogelijk behoren broncodebibliotheken niet in productiesystemen te worden opgeslagen;
b. de programmabroncode en de broncodebibliotheken behoren te worden beheerd volgens vastgestelde procedures;
c. onderhoudspersoneel behoort niet onbeperkt toegang worden te verleend tot broncodebibliotheken;
d. het updaten van broncodebibliotheken en daarmee verbonden zaken, en het afgeven van broncodes aan programmeurs behoort alleen te worden uitgevoerd nadat daarvoor de juiste autorisatie is ontvangen;
e. programma-uitdraaien behoren te worden bewaard in een beveiligde omgeving
f. er behoort een auditlogbestand te worden bijgehouden waarin elke toegang tot broncodebibliotheken wordt geregistreerd;
g. het bijhouden en kopiëren van broncodebibliotheken behoort aan strikte procedures voor wijzigingsbeheer te worden onderworpen.

10 CRYPTOGRAFIE

10.1 Cryptografische beheersmaatregelen

Doel: cryptografie juist en doeltreffend en conform wet- en regelgeving toepassen om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel
Om ervoor zorg te dragen dat de bescherming van informatie gebruik maakt van relevante technieken én voldoet aan wet- en regelgeving behoort een beleid voor (het gebruik van) cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

Implementatierichtlijn
Cryptografie kent voor- en nadelen voor gebruikers en organisaties. Om deze op de juiste wijze te beheersen dienen de volgende aspecten in beleid over cryptografie overwogen te worden:

a. de algemene manier waarop omgegaan wordt met cryptografische beheersmaatregelen en –methoden, conform het algemene beleid van bedrijfsinformatie
b. het vereiste beschermingsniveau dat cryptografie mede helpt bereiken moet zijn geïdentificeerd op basis van een risicobeoordeling. Dit betekent keuze van het juiste versleutelingstype en –sterkte (keylength).
c. versleuteling ter bescherming van informatie die wordt gecommuniceerd (overgedragen) per draagbare of verwijderbare media-apparatuur of via communicatiekanalen (versleuteling van informatie of informatiekanaal);
d. sleutelbeheer op een wijze die cryptografische sleutels beschermt en het herstel van versleutelde informatie mogelijk maakt in geval van verloren, gecompromitteerde of beschadigde sleutels;
e. rollen en verantwoordelijkheden, waaronder de verantwoordelijke voor:
   - het implementeren van het beleid;
   - het sleutelbeheer (zie 10.1.2);
f. de verschillende normen/beveiligingsniveaus voor een doeltreffende implementatie in de gehele organisatie (passende oplossing bij elk bedrijfsproces);
g. de impact van het gebruik van versleutelde informatie op beheersmaatregelen die zijn gebaseerd op controle van de inhoud (bijv. detectie van malware en automatische classificatie van informatie op basis van content).

Bij het implementeren van het cryptografiebeleid moet rekening 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 18.1.5). Cloudoplossingen, informatie-overdrachtssystemen, globally distributed systemen en offshoring maken internationale overdracht van informatie eenvoudig.

Cryptografie kan worden toegepast ten behoeve van:

a. vertrouwelijkheid: gevoelige of essentiële informatie kan door cryptografie worden beschermd tijdens opslag of verzending;
b. integriteit/authenticiteit: digitale handtekeningen (hiervan bestaan diverse vormen met verschillende niveaus van bescherming) of authenticatiecodes voor berichten kunnen tevens worden gebruikt om de authenticiteit of integriteit van gevoelige of essentiële informatie tijdens opslag of verzending te verifiëren;
c. onweerlegbaarheid: het gebruik van cryptografische technieken als bewijs van het (niet) plaatsvinden van een gebeurtenis of actie;

d. authenticatie: het gebruik van cryptografische technieken ter authenticatie van gebruikers en andere systeementiteiten.

Overige informatie
De passendheid van een cryptografische oplossing bij de organisatie en de genomen beslissingen horen bij risicobeoordeling en kiezen van maatregelen. Beleid hierbij is nodig om de risico's te beheersen bij de uitvoering in de praktijk, met name ter voorkomen van onjuist gebruik. Cryptografie is een 'vak apart' waarbij het goed is deskundig advies in te winnen.

10.1.2 Sleutelbeheer

Beheersmaatregel
Er moet beleid zijn ontwikkeld en geïmplementeerd voor sleutelbeheer van cryptografische sleutels (gebruik én bescherming van).

Implementatierichtlijn
Voor cryptografische sleutels gelden dezelfde fasen of handelingen als voor andere informatie: ze worden aangemaakt, ergens opgeslagen en teruggetrokken, gearchiveerd of vernietigd, ze moeten terug te vinden zijn (distributie en vindbaarheid). De kracht van een cryptografische sleutel ontstaat uit het toegepaste algoritme, de sleutellengte en de praktische omgang met de sleutels. Het specialisme 'cryptografie' verandert snel door steeds toegenomen rekenkracht van computers, en door blootgelegde kwetsbaarheden, waardoor algoritmen als geheel gecompromitteerd kunnen raken. Hierdoor is selectie van het juiste algoritme van belang. Wanneer krachtige sleutels toegepast worden is daarmee ook het beheren van die sleutels met zorgvuldig nageleefde procedures van belang. Ook (toegang tot) apparatuur voor sleutelbeheer dient te worden beschermd.

Het systeem voor beheer moet een geaccepteerde set voorzieningen bevatten, die mogelijk maakt:
a) Aanmaken van sleutels voor verschillende cryptografische systemen of technieken voor verschillende toepassingen
b) Het verkrijgen en verstrekken van openbare sleutelcertificaten
c) Het verspreiden van de sleutel naar de juiste ontvangers met instructie hoe om te gaan met de sleutel na ontvangst
d) Hoe sleutels opgeslagen moeten worden en onder welke omstandigheden gebruikers toegang krijgen tot sleutels
e) Wijziging van sleutels, inclusief regels wanneer en hoe dit moet gebeuren
f) Hoe om te gaan met gecompromitteerde sleutels;
g) Het deactiveren of intrekken van sleutels (zowel bij inbreuk als bij vertrekkende medewerkers(typen))
h) Recovery van verloren of corrupte sleutels;
i) Backup en archivering;
j) Vernietiging;
k) Het loggen van gebruik van sleutelbeheer om hiervan audit mogelijk te maken

Het toepassen van sleutels wordt veiliger door met activeringmoment en deactiveringsmoment van de sleutel(s) te werken – dit kan variëren van seconden tot jaren.

Er zijn niet alleen geheime sleutels (waarvoor voorgaande eisen gelden), maar ook openbare sleutels. Dit soort sleutel is meestal uitgegeven door een certificerende instantie. Die instantie moet erkend zijn en zelf ook passende maatregelen hebben getroffen om de betrouwbaarheid van door hen uitgegeven openbare sleutels te garanderen. Goed omgaan met openbare sleutels wordt bepaald door juiste authenticatie van die openbare sleutels.

Voor alle leveranciers gelden vanuit de norm eisen aan hun gedrag (zie 15.2). Voor dienstverleners die cryptografische diensten verstrekken is ten minste hun aansprakelijkheid, betrouwbaarheid van dienstverlening en responstijd van belang.

Vanuit de wet is het mogelijk dat er toegang geëist wordt tot versleutelde informatie. Het kan noodzakelijk zijn hiervoor een procedure op te stellen.

11 FYSIEKE BEVEILIGING EN BEVEILIGING VAN DE OMGEVING

11.1 Beveiligde ruimten

Doel: Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie. IT voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermt door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. De geboden bescherming behoort in overeenstemming te zijn met de vastgestelde risico's.

11.1.1 Fysieke beveiliging van de omgeving

Beheersmaatregel
Er behoren toegangsbeveiligingen (toegangsdeuren of -poorten met kaartsloten) te worden aangebracht om ruimten te beschermen waar zich informatie en IT voorzieningen bevinden.

Implementatierichtlijnen
De volgende richtlijnen en beheersmaatregelen behoren te worden overwogen en desgewenst geïmplementeerd voor fysiek beveiligde zones:

a. De grenzen van de beveiligde zone behoren duidelijk te worden gedefinieerd en de situering en sterkte van elk van de zones behoren afhankelijk te zijn van de beveiligingseisen die worden gesteld aan de bedrijfsmiddelen in de zone en de resultaten van de risicobeoordeling.
b. De omtrek van een gebouw of locatie waarin zich IT voorzieningen bevinden, behoort fysiek deugdelijk te zijn, de buitenmuren van de locatie behoren solide te zijn en alle buitendeuren behoren op passende wijze te zijn beschermd tegen toegang door onbevoegden, bijvoorbeeld met (elektronische) vergrendeling, tralies, alarmsystemen, sloten enz.; deuren en ramen behoren te zijn afgesloten als er niemand aanwezig is en er behoort externe bescherming voor ramen te worden overwogen, vooral op de begane grond.
c. Waar van toepassing behoren fysieke barrières te worden gebouwd om ongeautoriseerde toegang te voorkomen.
d. Alle branddeuren in een beveiligde zone behoren te zijn voorzien van een alarm, te worden gecontroleerd en getest in combinatie met de muren, om overeenkomstig nationale en regionale normen het vereiste brandwerendheidniveau vast te stellen; ze behoren volgens de plaatselijke brandvoorschriften faalveilig te functioneren.
e. Er behoren geschikte anti-inbraaksystemen te worden geïnstalleerd conform nationale en regionale normen; deze systemen behoren regelmatig te worden getest en behoren alle buitendeuren en toegankelijke ramen te bestrijken; onbemande ruimten behoren te allen tijde van een alarmsysteem te zijn voorzien; ook andere ruimten, bijvoorbeeld computerruimten of
f. IT voorzieningen die door de organisatie zelf worden beheerd, behoren fysiek te zijn gescheiden van systemen die door derden worden beheerd.

Overige informatie
Fysieke bescherming kan worden bereikt door het opwerpen van een of meer fysieke barrières rond de IT voorzieningen. Wanneer het beheer van systemen, bijvoorbeeld persmonitoring of monitoring van productieprinters, door derden wordt uitgevoerd, heeft het de voorkeur om dit op een fysiek gescheiden systeem uit te voeren of op een separaat opgezet netwerk. Wanneer een degelijke scheiding van systemen niet mogelijk is moeten er in een overeenkomst afspraken worden gemaakt over toegang tot het computersysteem en het gebruik van netwerkpoorten voor uitvoering van de specifieke taak van de derde partij.

11.1.2 Fysieke toegangsbeveiliging

Beheersmaatregel
Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

Implementatierichtlijnen
De volgende richtlijnen behoren te worden overwogen, afhankelijk van de gewenste beveiliging:

a. Datum en tijdstip van aankomst en vertrek van bezoekers behoren te worden geregistreerd en bezoekers van beveiligde gebieden behoren altijd te worden begeleid of toestemming te hebben om het gebied te betreden. Aan hen mag alleen toegang worden verleend voor bepaalde, geautoriseerde doeleinden en ze behoren te worden geïnstrueerd over de beveiligingseisen van het gebied en over noodprocedures.
b. Toegang tot ruimten waar gevoelige informatie wordt verwerkt of opgeslagen behoort te worden beheerst en behoort te worden beperkt tot bevoegd personeel; er behoren authenticatievoorzieningen te worden toegepast, zoals toegangspasjes met pincode, om alle toegang te autoriseren en te valideren. Er behoort een ‘audit trail’ (naspeurbare registratie) van alle vormen van toegang te worden bijgehouden.
c. Alle werknemers, ingehuurd personeel en externe gebruikers en alle bezoekers behoren zich te kunnen identificeren of een zichtbare vorm van identificatie te dragen.
d. Aan personeel van externe ondersteunende diensten behoort alleen wanneer dit noodzakelijk is beperkte toegang te worden verleend tot beveiligde ruimten of gevoelige IT voorzieningen; deze toegang behoort te worden geautoriseerd en gecontroleerd.
e. Toegangsrechten tot beveiligde gebieden behoren regelmatig te worden beoordeeld en geüpdatet en wanneer nodig te worden ingetrokken.

11.1.3 Beveiliging van kantoren, ruimten en faciliteiten

Beheersmaatregel
Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast indien dat voor informatiebeveiliging relevant is.

Implementatierichtlijnen
Om kantoren, ruimten en voorzieningen te beveiligen kunnen de volgende richtlijnen worden gevolgd:

a. De belangrijkste voorzieningen behoren te worden geplaatst in gebieden die niet toegankelijk zijn voor bezoekers.
b. Waar van toepassing behoren gebouwen onopvallend te zijn en zo min mogelijk aanwijzingen te geven over het gebruiksdoel ervan; er behoren geen duidelijke tekenen binnen of buiten het gebouw te zijn aangebracht die op de aanwezigheid van informatieverwerkingsactiviteiten duiden.
c. Adresboeken en interne telefoongidsen van de organisatie waarin locaties worden aangeduid met gevoelige IT voorzieningen, behoren niet vrij toegankelijk te zijn voor bezoekers.

11.1.4 Beschermen tegen bedreigingen van buitenaf

Beheersmaatregel
Er moet bescherming zijn (ontworpen en in gebruik) tegen bedreigen van buitenaf, zoals natuurrampen, ongelukken of (kwaadwillige) aanvallen.

Implementatierichtlijn
Bij de beveiliging van elk pand dienen er voorzieningen te zijn tegen 'standaard' verstoringen (zoals brand, of het gedrag van groepen mensen rondom de locatie). Voor een aantal van deze verstoringen geldt dat bijvoorbeeld de brandweer hier eisen aan kan stellen en ook advies kan geven.

Dan zijn er bedreigingen welke door de locatie (of het eigen pand) in meerdere of mindere mate aannemelijk zijn. Bijvoorbeeld de kans op overstroming, explosie (van buurpand of eigen stoffenopslag), aardbeving. Voor deze risico's dien afdoende deskundig advies ingewonnen te worden.

11.1.5 Werken in beveiligde gebieden

Beheersmaatregel
Er moeten procedures zijn opgesteld en in werking zijn voor het werken in beveiligde gebieden.

Implementatierichtlijn
Voor deze procedures gelden de volgende richtlijnen:
a. De aard van werkzaamheden in beveiligde gebieden dient alleen bekend te zijn bij personeel waarvoor deze kennis noodzakelijk is
b. Werken in deze gebieden moet zoveel mogelijk me toezicht geschieden: dit om het risico van kwaadaardige handelingen te verminderen én voor de veiligheid van de aanwezigen
c. (Leegstaande) ruimten moeten worden afgesloten en geïnspecteerd.
d. Het gebruik van opnameapparatuur (geluid en beeld) is in principe niet toegestaan

Zoals veel van deze richtlijnen gelden gemaakte afspraken voor zowel de eigen medewerkers als voor derden.

11.1.6 Laad- en loslocatie

Beheersmaatregel
Laad- en loslocaties en andere punten waar onbevoegden het terrein of pand kunnen betreden, moeten worden beheerst en waar mogelijk worden afgeschermd van locaties waar informatieverwerkende faciliteiten en/of gevoelige informatie aanwezig zijn.

Implementatierichtlijn
Laad- en loslocaties zijn in de praktijk zeer kwetsbaar. Er is vaak sprake van veelvuldig verkeer door meerdere en steeds wisselende personen. Hierdoor is het houden van toezicht minder eenvoudig. In veel gevallen is een laad- en loslocatie niet gescheiden van een eventueel magazijn of een productieruimte. De volgende richtlijnen gelden:
a. Toegang tot de laad- en loslocatie (van buitenaf) moet zoveel mogelijk worden beperkt tot geïdentificeerd en bevoegd personeel, en/of de toegang van personen geschiedt zoveel mogelijk onder begeleiding.
b. De locatie wordt zoveel mogelijk ingericht zodat aanwezigen geen toegang hebben tot andere afdelingen in het gebouw.
c. De buitendeuren van de locatie behoren beveiligd te zijn, zeker wanneer binnendeuren open of niet aanwezig zijn.

Overige informatie
Alternatieve maatregelen welke overwogen kunnen worden zijn bijvoorbeeld cameraregistratie, (automatische) deurbellen, informerende borden bij toegang van de locatie, en het beveiligd (laten) verpakken van te leveren of ontvangen goederen.

11.2 Beveiliging van apparatuur

Doel: het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten. Apparatuur behoort te zijn beschermd tegen fysieke bedreigingen en gevaren van buitenaf.

Bescherming van apparatuur (waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen) is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade. Ook bij het verplaatsen of verwijderen van apparatuur behoort hiermee rekening te worden gehouden. Er kunnen bijzondere beheersmaatregelen nodig zijn om de apparatuur te bescherming tegen fysieke bedreigingen en ter bescherming van de ondersteunende voorzieningen zoals stroomvoorziening en bekabelinginfrastructuur.

11.2.1 Plaatsing en bescherming van apparatuur

Beheersmaatregel
Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

Implementatierichtlijnen
De volgende beheersmaatregelen behoren te worden overwogen om apparatuur te beschermen.

a. IT voorzieningen met gevoelige gegevens behoren te worden geplaatst met een beperkte inkijkhoek zodat de kans vermindert dat informatie door onbevoegden tijdens gebruik wordt gezien; de opslagvoorzieningen behoren te worden beveiligd tegen onbevoegde toegang.
b. Er behoren beheersmaatregelen te worden aanvaard om het risico van mogelijke gevaren te minimaliseren, bijvoorbeeld diefstal, brand, explosie, rook, wateroverlast (of onderbreking van de watertoevoer), stof, trillingen, chemische reacties, verstoring van de elektriciteitsvoorziening en van de communicatie, elektromagnetische straling en vandalisme.
c. De organisatie behoort richtlijnen vast te stellen ten aanzien van eten, drinken en roken in de nabijheid van IT voorzieningen.
d. Omgevingsomstandigheden zoals temperatuur en luchtvochtigheid, behoren te worden gecontroleerd op omstandigheden die de werking van IT voorzieningen negatief beïnvloeden.

11.2.2 Nutsvoorzieningen

Beheersmaatregel
Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die kunnen ontstaan door uitval van nutsvoorzieningen.

Implementatierichtlijn
Nutsvoorzieningen (waaronder watervoorziening, gas, riolering, elektriciteit, telecommunicatie, ventilatie en airconditioning) behoren:

a. te voldoen aan de wettelijke eisen en de technische beschrijving van de fabrikant;
b. regelmatig te worden onderzocht en beoordeeld, onder andere op capaciteit;
c. regelmatig te worden geïnspecteerd en getest om correcte werking te waarborgen;

d. waar nodig worden uitgerust met een alarmsysteem om verstoringen te detecteren;
e. voor zover nodig, te beschikken over meervoudige voeding/aansluiting met verschillende fysieke routes.

(Ook voor noodsituaties) dienen verlichting en communicatiemiddelen aanwezig te zijn. Stroom, water, gas of andere voorzieningen moeten met een schakelaar (in de buurt van een nooduitgang of waar apparatuur aanwezig is) kunnen worden uitgeschakeld.

11.2.3 Beveiliging van kabels

Beheersmaatregel
Voeding- en telecommunicatiekabels die voor data verkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen aftappen of beschadiging te worden beschermd.

Implementatierichtlijnen
De volgende richtlijnen behoren te worden overwogen voor de beveiliging van bekabeling.
a. Elektriciteit- en telecommunicatiekabels voor IT voorzieningen behoren bij voorkeur ondergronds te worden aangelegd of op andere wijze afdoende te worden beschermd.
b. Netwerkkabels behoren te worden beschermd tegen ongeautoriseerd aftappen of beschadiging, bijvoorbeeld door ze in mantelbuizen of kabelgoten te leggen.
c. Netsnoeren behoren gescheiden te worden gehouden van communicatiekabels, om interferentie te voorkomen.
d. Er behoren duidelijk identificeerbare markeringen op kabels en apparatuur te worden gebruikt om fouten bij bewerking te voorkomen, zoals het per ongeluk patchen van de verkeerde netwerkkabels.
e. Er dient een duidelijke lijst aanwezig te zijn van het patchen van de netwerkkabels.

11.2.4 Onderhoud van apparatuur

Beheersmaatregel
Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.

Implementatierichtlijnen
De volgende richtlijnen behoren te worden overwogen voor het onderhouden van apparatuur.
a. Apparatuur behoort te worden onderhouden volgens de door de leverancier aanbevolen voorschriften en service-tijdstippen.
b. Reparatie en/of onderhoud van apparatuur behoren alleen te worden uitgevoerd door bevoegd onderhoudspersoneel of medewerkers die deze taak hebben toegewezen gekregen en daarvoor zijn opgeleid.
c. Wanneer reparatie en/of onderhoud is uitbesteed, behoort in een overeenkomst te zijn vastgelegd de kwalificaties voor het uitvoeren van deze werkzaamheden en behoort de uitvoering daarvan periodiek met de toeleverancier te worden geëvalueerd.
d. Er behoren registraties te worden bijgehouden van alle vermeende of daadwerkelijke storingen en van alle preventieve en corrigerende onderhoudswerkzaamheden.
e. Er behoren passende beheersmaatregelen te worden ingevoerd wanneer apparatuur volgens schema onderhoud zal ondergaan, daarbij in aanmerking nemend of het onderhoud wordt verricht door personeel op locatie of door extern personeel.

11.2.5 Verwijdering van bedrijfseigendommen

Beheersmaatregel
Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

Implementatierichtlijnen
De volgende richtlijnen behoren te worden overwogen.

a. Apparatuur, informatie en programmatuur behoren niet zonder toestemming buiten de locatie te worden meegenomen.
b. Er behoren tijdslimieten te worden gesteld aan het uithuizig zijn van apparatuur en bij inlevering behoort te worden gecontroleerd op naleving daarvan. In het geval van thuiswerken, worden duidelijke afspraken gemaakt over het gebruik van apparatuur.
c. Waar nodig en passend behoort te worden geregistreerd dat apparatuur de locatie verlaat en wanneer deze weer wordt teruggebracht.

11.2.6 Beveiliging van apparatuur buiten het terrein

Beheersmaatregel
Informatieverwerkende apparatuur in gebruik buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de risico's van werken buiten het terrein van de organisatie.

Implementatierichtlijnen
Voor het gebruik van informatieverwerkende apparatuur buiten het terrein van de organisatie behoort te allen tijde toestemming van de directie te worden gevraagd, ongeacht wie de eigenaar is.
De volgende richtlijnen behoren te worden overwogen voor de bescherming van apparatuur buiten de locatie.

a. Apparatuur en media mogen buiten het terrein niet onbeheerd worden achtergelaten in openbare ruimten. Draagbare computers behoren tijdens het reizen als handbagage te worden vervoerd en behoren zo min mogelijk herkenbaar te zijn.
b. De instructies van de fabrikant ter bescherming van de apparatuur behoren te allen tijde te worden opgevolgd.
c. beheersmaatregelen voor thuiswerken behoren te worden vastgesteld aan de hand van een risicobeoordeling. Voorbeelden van beheersmaatregelen zijn een beveiligde toegang tot informatiesystemen van de organisatie en de het opbergen van apparatuur in een afsluitbare kast.

11.2.7 Veilig verwijderen of hergebruiken van apparatuur

Beheersmaatregel
Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

Implementatierichtlijnen
Opslagmedia met gevoelige informatie behoren, in plaats van volgens standaardmethoden te worden gewist of geformatteerd, fysiek te worden vernietigd of de informatie behoort te worden vernietigd, verwijderd of overschreven met technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen.
Wanneer opslagmedia wisselend worden toegepast voor het aanleveren van (grafische) data moet ervoor gezorgd worden dat er controle is op de media die wordt uitgeleverd, of daar geen informatie of programmatuur op aanwezig is.

11.2.8Onbeheerde gebruikersapparatuur

Beheersmaatregel
Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

Implementatierichtlijnen
Alle gebruikers behoren op de hoogte te worden gebracht van de beveiligingseisen en procedures voor het beschermen van onbeheerde apparatuur, evenals van hun verantwoordelijkheden in het uitvoeren van deze bescherming. Gebruikers behoren te worden geadviseerd:

a. actieve sessies te beëindigen als ze klaar zijn, tenzij deze sessies kunnen worden beveiligd met een geschikte vergrendeling, bijvoorbeeld een screensaver beschermd met een wachtwoord;
b. pc's of computerterminal die niet in gebruik zijn tegen onbevoegd gebruik te beveiligen met behulp van een toetsvergrendeling of wachtwoord.

11.2.9 'Clear desk'- en 'clear screen'-beleid

Beheersmaatregel
Er behoort een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor IT voorzieningen te worden ingesteld wanneer gewerkt wordt met gevoelige informatie.

Implementatierichtlijnen
Het 'clear desk'- en 'clear screen'-beleid behoort rekening te houden met de informatieclassificatie, wettelijke en contractuele eisen en de bijbehorende risico's en bedrijfscultuur van de organisatie. De volgende richtlijnen behoren te worden overwogen:

a. gevoelige of kritische bedrijfsinformatie, bijvoorbeeld op papier of op elektronische opslagmedia, behoort afgesloten te worden bewaard (bij voorkeur in een kluis of brandkast of andere vormen van beveiligd meubilair) wanneer de informatie niet wordt gebruikt, vooral als het kantoor verlaten is;
b. computers en computerterminals behoren uitgelogd of beschermd te zijn door een scherm- en toetsenbordvergrendeling met wachtwoord, token of soortgelijke authenticatie van de gebruiker wanneer ze onbeheerd achterblijven en behoren te worden beschermd door middel van toetsvergrendeling, wachtwoorden of andere beheersmaatregelen wanneer ze niet worden gebruikt;
c. ruimten waar post binnenkomt en uitgaat en onbeheerde faxmachines behoren te worden beschermd;
d. onbevoegd gebruik van fotokopieerapparaten en andere reproductieapparatuur (bijvoorbeeld scanners, digitale camera's) behoort te worden voorkomen;
e. documenten met gevoelige of geheime informatie behoren na het afdrukken onmiddellijk van printers te worden verwijderd door het paginageheugen leeg te maken.

Overige informatie
Met een 'clear desk'- en 'clear screen'-beleid worden de risico's van onbevoegde toegang, verlies van en schade aan informatie tijdens en buiten kantooruren verminderd. Ook kluizen of andere soorten beveiligde opslagvoorzieningen zouden de informatie die erin is opgeslagen kunnen beschermen tegen calamiteiten zoals brand, aardbeving, overstroming of ontploffing.

12 BEVEILIGDE BEDRIJFSVOERING

12.1 Bedieningsprocedures en verantwoordelijkheden

Doel: Waarborgen van een correcte en veilige bediening van IT voorzieningen. Er behoren verantwoordelijkheden en procedures te worden vastgesteld voor beheer en bediening van alle IT voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies. Er behoort waar van

toepassing en mogelijk, functiescheiding te worden toegepast om het risico van nalatigheid of opzettelijk misbruik van het systeem te verminderen.

12.1.1 Gedocumenteerde bedieningsprocedures

Beheersmaatregel
Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

Implementatierichtlijnen
Er behoren gedocumenteerde procedures te worden opgesteld voor systeemactiviteiten met betrekking tot informatieverwerking- en communicatievoorzieningen, zoals opstart- en afsluitprocedures voor computers, back-ups, onderhoud van apparatuur, behandeling van media, gebruik van programmatuur, beheer van computerruimten en postverwerking, verzending en veiligheid.
De bedieningsprocedures behoren de instructies te geven voor een gedetailleerde uitvoering van elke taak, waaronder:

a. verwerking en behandeling van informatie.
b. maken van back-ups (zie 11.5).
c. instructies voor de afhandeling van fouten en andere uitzonderlijke situaties die zich tijdens de uitvoering van de taak kunnen voordoen, waaronder beperkingen in het gebruik van systeemhulpmiddelen.
d. contactpersonen voor onverwachte bedieningsmoeilijkheden of technische storingen;
e. instructies voor de behandeling van media en geproduceerde informatieproducten, zoals het beheer van vertrouwelijke uitvoer, van mislukte productie-eenheden en procedures voor een veilige verwijdering van mislukte productie-eenheden of taken.
f. procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
g. beheer van ‘audit trail’ en systeem logbestanden.

Bedieningsprocedures en de gedocumenteerde procedures voor systeemactiviteiten behoren als formele documenten te worden behandeld en wijzigingen behoren te worden geautoriseerd door de directie. Waar technisch mogelijk behoren informatiesystemen consistent te worden beheerd, met gebruik van dezelfde procedures, gereedschappen en hulpmiddelen.
Wanneer in Service Level Agreements met klanten vereisten zijn opgenomen met betrekking tot de productie van informatieproducten met vertrouwelijke informatie, dienen deze vereisten te zijn verwerkt naar instructies voor het productiepersoneel.

Overige informatie
Bij het produceren van variabele data documenten in print (o.a. Direct mail) is het van belang dat de productie zorgvuldig is georganiseerd, zodat de variabele data alleen terecht komt bij de beoogde eindgebruiker. De eisen t.a.v. een zorgvuldige productie worden vastgelegd in een Service Level Agreement. Ten aanzien van variabele data documenten in print toepassingen behoort in de SLA te worden aangegeven de productiewijze en borging gericht op een zorgvuldige productie van elk individueel exemplaar van het variabel geprint document. De beschrijving behoort te zijn vertaald naar werkinstructies en procedures voor de productiemedewerkers en behoort te zijn gedocumenteerd. In de SLA is opgenomen een adequate rapportage over de geproduceerde hoeveelheden, de afgeleverde hoeveelheden aan de verzender, de voorgekomen productieverstoringen en de zorgvuldige verwijdering van de bij de productieverstoring voorgekomen foute producties.

12.1.2 Wijzigingsbeheer

Beheersmaatregel
Wijzigingen in IT voorzieningen en informatiesystemen behoren te worden beheerst.

Implementatierichtlijnen
Wijzigingen in productiesystemen en toepassingsprogrammatuur behoren te worden beheerst met strikt wijzigingsbeheer. In het bijzonder behoort rekening te worden gehouden met de volgende punten:
a. identificatie en registratie van significante wijzigingen;
b. planning en testen van wijzigingen;
c. beoordeling van de mogelijke gevolgen, waaronder de beveiligingsgevolgen, van dergelijke wijzigingen;
d. een formele goedkeuringsprocedure (van de leverancier) voor voorgestelde wijzigingen;
e. communicatie van details van de wijzigingen aan alle betrokken personen;
f. uitwijkprocedures, waaronder de procedures en verantwoordelijkheden ten aanzien van het afbreken en herstellen van niet-geslaagde wijzigingen en onvoorziene gebeurtenissen.

12.1.3 Capaciteitsbeheer

Beheersmaatregel
De hoeveelheid van gebruik van middelen moet worden gemonitord zodat het gebruik kan voldoend aan (verwachte) capaciteitseisen.

Implementatierichtlijn
Op basis van het belang van het systeem dienen er gedefinieerde capaciteitseisen te zijn voor het systeem. Door monitoring moet blijken dat de beschikbaarheid en doelmatigheid van systemen voldoende zijn en niet worden gehinderd door onvoldoende capaciteit. De monitoring dient ook preventief te zijn (detectie wanneer limieten bereikt worden). De verwachting van toekomstig gebruik dient niet alleen gebaseerd te zijn op ‘natuurlijke groei’, maar ook op basis van verwachtingen over veranderingen voor de organisatie.

Naast het perspectief van belangrijke systemen moet er ook specifiek aandacht zijn voor middelen met een lange levertijd of hoge (implementatie)kosten. Beheerders moeten deze middelen én belangrijke systemen monitoren en relevante trends in het gebruik signaleren. Dit dienen ze zo te doen dat knelpunten of afhankelijkheden, van systemen, middelen en belangrijk persoon geen bedreiging gaan vormen voor de systembeveiliging en beschikbaarheid. Hiertoe moeten ze relevante acties definiëren, plannen en uitvoeren.

De juiste afstemming van capaciteit kan worden bereikt door de capaciteit te verhogen of door de vraag te verlagen. De vraag kan worden beheerst en/of gereduceerd door:
a. verwijderen van verouderde gegevens (schijfruimte, omvang van back-ups);
b. het buiten gebruik stellen van toepassingen, systemen, databases of omgevingen;
c. geautomatiseerde workflow- en batchprocessen en -schema’s te optimaliseren;
d. specialistische (effectievere) hardware toe te passen voor bepaalde bewerkingen (bijvoorbeeld grafische processoren)
e. toepassingslogica of databasevragen te optimaliseren (meestal door herprogrammeren);
f. de bandbreedte voor diensten die veel energie of (processor)capaciteit verbruiken te weigeren of te beperken als deze niet van groot bedrijfsbelang zijn (bijv. videostreaming).

Voor belangrijke systemen behoort voor de capaciteit een gedocumenteerd beheersplan te worden overwogen.

Overige informatie
Let op dat deze beheersmaatregel niet alleen geldt voor ‘typische IT’ zaken, zoals beschikbare servers (met load balancing), processorcapaciteit, geheugengebruik en bandbreedte, maar ook voor personele middelen, kantoren en andere faciliteiten. Ook specialistische beveiligingsmiddelen dienen in voldoende mate aanwezig te zijn.

Een gedocumenteerd beheersplan voor capaciteit is vergelijkbaar met een beheersplan voor de capaciteit van productiemachines.

12.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

Beheersmaatregel
In het geval dat een organisatie zelf programmatuur of scripts ontwikkelt, behoren de faciliteiten voor ontwikkeling en testen van de productie te zijn gescheiden om het risico van verstoring van de productie of onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

Implementatierichtlijnen
Er behoort te worden bepaald welk niveau van scheiding nodig is tussen productie omgeving en de ontwikkelings- en testomgeving, om problemen in de productie omgeving te voorkomen.
De volgende punten behoren te worden overwogen:

a. Er behoren regels voor het overdragen van programmatuur van ontwikkelings- naar operationele status te worden gedefinieerd en gedocumenteerd.
b. Gevoelige gegevens behoren niet naar een ontwikkel- en testomgeving te worden gekopieerd.

12.2 Bescherming tegen virussen, ‘mobile code’ en scripts.

Doel: Beschermen van de integriteit van programmatuur en informatie. Er behoren voorzorgen te worden getroffen om de introductie van virussen en ongeautoriseerde ‘mobile code’ te voorkomen en te ontdekken. Programmatuur en IT voorzieningen zijn kwetsbaar voor invoer van virussen, zoals computervirussen, netwerkwormen, Trojans en logische bommen. Gebruikers
behoren bewust te worden gemaakt van de gevaren van virussen. Managers behoren zo nodig bijzondere beheersmaatregelen te treffen om virussen te voorkomen, te ontdekken en te verwijderen.

12.2.1 Maatregelen tegen virussen en mobile code

12.2.1.1 Virussen

Beheersmaatregel
Er behoren maatregelen te worden getroffen voor detectie van virussen, preventie tegen virussen en herstellen van apparatuur geïnfecteerd door virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

Implementatierichtlijnen
Bescherming tegen virussen behoort te zijn gebaseerd op het ontdekken van virussen en op herstelprogrammatuur, op een goed beveiligingsbewustzijn, toegangsbeveiliging van systemen en controle van wijzigingsbeheer. De volgende richtlijnen behoren te worden overwogen:

a. vastleggen van een formeel beleid dat het gebruik van ongeautoriseerde programmatuur verbiedt;
b. vastleggen van een formeel beleid ter bescherming tegen de risico's verbonden aan het verkrijgen van bestanden en programmatuur vanuit of via externe netwerken of via enig ander medium, dat aangeeft welke beschermende maatregelen behoren te worden getroffen;
c. regelmatige beoordeling van de programmatuur en de inhoud van de gegevens van systemen waarmee kritieke bedrijfsprocessen worden ondersteund; de aanwezigheid van niet-goedgekeurde bestanden of ongeautoriseerde wijzigingen behoort formeel te worden onderzocht;

d. installatie en regelmatige actualisering van programmatuur voor het ontdekken van virussen en herstelprogrammatuur om computers en media te scannen, hetzij als voorzorgsmaatregel, hetzij op basis van routine; de volgende controles behoren o.a. te worden uitgevoerd:
   - controleren van bestanden op digitale media en bestanden die via netwerken zijn ontvangen, op virussen voordat ze worden gebruikt;
   - controleren van e-mail, e-mailbijlagen en gedownloade bestanden op virussen voordat ze worden gebruikt; deze controle behoort te worden uitgevoerd op verschillende plaatsen, bijvoorbeeld op e-mailservers, FTP servers in de DMZ, desktopcomputers en bij de toegang tot het netwerk van de organisatie;
   - controleren van de gebruikte webapplicaties en webpagina's op virussen;

e. het regelmatig updaten van programmatuur voor het ontdekken en uitschakelen van virussen.
f. opstellen van geschikte continuïteitsplannen voor herstel na aanvallen met virussen, waaronder alle nodige voorzieningen voor back-ups van gegevens en programmatuur, evenals herstelmaatregelen;

Overige informatie

Er kan antivirusprogrammatuur worden geïnstalleerd die automatische updates levert van de definitiebestanden en 'scanning engines' om te waarborgen dat de bescherming actueel is. Deze programmatuur kan bovendien op elke desktopcomputer worden geïnstalleerd voor het uitvoeren van automatische controles.
Er behoort voor te worden gezorgd dat er ook bescherming is tegen virussen tijdens onderhouds- en noodprocedures die de normale beschermingsmaatregelen tegen virussen zouden kunnen omzeilen.

12.2.1.2 'mobile code'

Beheersmaatregel

Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

Implementatierichtlijnen

Onder 'mobile code' verstaan we het uitwisselen en automatisch uitvoeren van software installatie zonder expliciete opdracht of handelingen van de gebruiker (voorbeelden: VBscript, Javascript), Applets of ActiveX controls). De volgende handelingen behoren te worden overwogen om te verhinderen dat 'mobile code' ongeautoriseerde acties kan uitvoeren:

a. blokkeren van elk gebruik van 'mobile code';
b. blokkeren van ontvangen van 'mobile code';
c. activeren van technische maatregelen die beschikbaar zijn op een specifiek systeem om te waarborgen dat 'mobile code' wordt beheerd;
d. beheersen van de bronnen die beschikbaar zijn voor toegang tot 'mobile code';

12.3 Maken van een Back-up

Doel: Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen.
Er behoren routineprocedures te worden vastgesteld voor uitvoeren van de overeengekomen back-upbeleid en -strategie, ten aanzien van het maken van back-ups van gegevens en het oefenen van een tijdig herstel ervan.

12.3.1 Maken van back-ups

Beheersmaatregel
Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.

Implementatierichtlijnen
Er behoren geschikte back-upvoorzieningen beschikbaar te zijn, zodat alle essentiële bedrijfsgegevens en programmatuur kunnen worden hersteld na een computercalamiteit of een defect medium.
De volgende aspecten behoren te worden meegenomen:

a. een omschrijving van een procedure van welke data een back-up gemaakt moet worden, met een omschrijving van de periode dat de data bewaard moet blijven en de frequentie van het maken van een back-up.
b. er behoren nauwkeurige en volledige registers van back-up kopieën en gedocumenteerde herstelprocedures te worden gemaakt;
c. de back-ups behoren te worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als zich een calamiteit voordoet op de productielocatie of locatie waar de data wordt gebruikt;
d. back-ups en de ruimte waarin deze zijn opgeslagen, behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie;
e. back-ups en backup procedures behoren regelmatig te worden getest, om te waarborgen dat ze betrouwbaar zijn en in geval van nood kunnen worden gebruikt;
f. herstelprocedures behoren regelmatig te worden gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn en dat ze kunnen worden uitgevoerd binnen de daarvoor volgens operationele herstelprocedures gestelde tijd;
g. in gevallen waar vertrouwelijkheid van belang is, behoren back-ups te worden beschermd door middel van encryptie.

Voor kritische systemen en productiesystemen behoren de procedures voor het maken van back-ups alle systeeminformatie, -toepassingen en gegevens te omvatten die nodig zijn om het gehele systeem te herstellen na een calamiteit.
Er behoort een bewaartermijn voor essentiële bedrijfsinformatie te worden vastgesteld, evenals eventuele eisen voor archiefexemplaren die permanent moeten worden bewaard.

Overige informatie
Back-up procedures kunnen worden geautomatiseerd om het back-up- en herstelproces te vereenvoudigen. Dergelijke geautomatiseerde oplossingen behoren voldoende te worden getest.

12.4 Verslaglegging en monitoren

Doel: Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

Systemen behoren te worden gecontroleerd en informatiebeveiligingsgebeurtenissen behoren te worden geregistreerd. Er behoort gebruik te worden gemaakt van logbestanden van operators en storingsregistraties om te waarborgen dat de informatiesysteemproblemen worden vastgesteld

12.4.1 Aanmaken audit-logbestanden

Beheersmaatregel
Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

Implementatierichtlijnen
In de auditlogbestanden behoren waar relevant onder meer de volgende gegevens te worden vastgelegd:
a. Gebruikersidentiteit;
b. data, tijdstippen en details van belangrijke gebeurtenissen, bijvoorbeeld van in- en uitloggen;
c. waar mogelijk de identiteit van de computerterminal of de locatie (MAC adres);
d. registraties van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem;
e. registraties van geslaagde en geweigerde gegevens en andere pogingen om toegang te krijgen;
f. wijzigingen van de systeemconfiguratie;
g. gebruik van speciale bevoegdheden;
h. gebruik van systeemhulpprogramma's en -toepassingen;
i. bestanden waartoe toegang is verkregen en het soort toegang;
j. netwerkadressen en protocollen;
k. alarmering geactiveerd door het toegangscontrolesysteem;
l. activering en de-activering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen.

12.4.2 Bescherming van informatie in logbestanden

Beheersmaatregel
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

Implementatierichtlijnen
beheersmaatregelen behoren te zijn gericht op bescherming tegen onbevoegde wijzingen en operationele problemen met de logvoorzieningen, waaronder:
a. wijzigingen in het soort berichten dat wordt geregistreerd;
b. bewerken of wissen van logbestanden;
c. vollopen van media met logbestanden, waardoor gebeurtenissen niet meer kunnen worden geregistreerd of het bestand zichzelf overschrijft.

Het is een vereiste zijn om bepaalde auditlogbestanden te archiveren als onderdeel van het documentbeheerbeleid of vanwege eisen om bewijsmateriaal te verzamelen en te bewaren.

Overige informatie
Systeemlogbestanden 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, behoort te worden overwogen het juiste type berichten automatisch naar een tweede logbestand te kopiëren, en/of bepaalde systeemhulpprogramma's of audit-hulpmiddelen voor bestandsonderzoek en -rationalisatie te gebruiken.
Systeemlogbestanden behoren te worden beschermd, omdat indien de gegevens kunnen worden gewijzigd of gewist, hun bestaan een vals gevoel van veiligheid zou kunnen wekken.

12.4.3 Logbestanden van administrators en operators

Beheersmaatregel
Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

Implementatierichtlijnen
In de logbestanden behoren onder meer te worden vastgelegd:
a. het tijdstip waarop een gebeurtenis (succesvol of storing) is opgetreden;
b. informatie over de gebeurtenis (bijvoorbeeld de bestanden die zijn behandeld) of storing (bijvoorbeeld fout opgetreden en corrigerende handeling uitgevoerd);
c. welke account en welke beheerder of operator erbij was betrokken;
d. welke processen erbij waren betrokken.

De logbestanden van systeembeheerder en -operator moeten regelmatig worden beoordeeld.

12.4.4 Synchronisatie van systeemklokken

Beheersmaatregel
De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

Implementatierichtlijnen
Waar een computer of communicatieapparatuur over een 'real-time'-klok beschikt, behoort deze te worden ingesteld volgens een overeengekomen norm, bijvoorbeeld Universal Coordinated Time (UCT) of de plaatselijke standaardtijd. Omdat van sommige klokken bekend is dat ze na verloop van tijd voor- of achterlopen, behoort er een procedure te zijn om ze regelmatig te controleren op significante afwijkingen en ze gelijk te zetten.
De juiste interpretatie van het datum/tijdformaat is belangrijk om te kunnen waarborgen dat de tijdsaanduiding overeenkomt met de werkelijke datum/tijd. Er behoort rekening te worden gehouden met plaatselijke zomertijd.

12.5 Beveiliging van operationele software

Doel: Beveiliging van systeembestanden bewerkstelligen.

De toegang tot systeembestanden en programmabroncode behoort te worden beheerst en IT-projecten en ondersteuningsactiviteiten behoren veilig te worden uitgevoerd. Blootstelling van gevoelige gegevens in testomgevingen behoort te worden voorkomen.

12.5.1 Beheersing van operationele programmatuur

Beheersmaatregel
Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.

Implementatierichtlijnen
Om het risico van corrumperen van productiesystemen tot een minimum te beperken behoort rekening te worden gehouden met de volgende richtlijnen om wijzigingen te beheersen:

a. het updaten van productieprogrammatuur, -toepassingen en -programmabibliotheken behoort uitsluitend te worden uitgevoerd door ervaren beheerders na goedkeuring door de directie.
b. op productiesystemen behoort alleen goedgekeurde uitvoerbare programmatuur aanwezig te zijn;
c. toepassingen en besturingssysteemprogrammatuur behoren pas te worden geïmplementeerd na tests; er behoort o.a. te worden getest op bruikbaarheid, beveiliging, effecten op andere systemen en gebruikersvriendelijkheid en de tests behoren op gescheiden systemen te worden uitgevoerd;
d. er behoort te worden gewaarborgd dat alle bijbehorende broncodebibliotheken zijn geüpdatet.
e. er behoort een configuratiebeheerssysteem te worden gebruikt om alle geïnstalleerde programmatuur en de systeemdocumentatie te kunnen beheersen;
f. er behoort een terugdraaistrategie te zijn vastgesteld voordat wijzigingen worden doorgevoerd;
g. er behoort een auditlogbestand te worden bijgehouden van elke update van besturingsprogrammabibliotheken.
h. eerdere versies van de toepassingsprogrammatuur behoren te worden bewaard voor noodgevallen;
i. oude versies van programmatuur behoren te worden gearchiveerd, samen met alle vereiste informatie en parameters, procedures, configuratiedetails en ondersteunende programmatuur zolang er gegevens dienen te worden gearchiveerd of zolang het nodig kan zijn dat gegevens worden geraadpleegd.

Programmatuur van leveranciers die in productiesystemen wordt gebruikt, behoort op een niveau te worden onderhouden dat door de leverancier wordt ondersteund. De organisatie behoort de risico's te onderkennen van het vertrouwen op niet-ondersteunde programmatuur en open source programmatuur.
Bij ieder besluit over upgraden naar een nieuwe programmatuurversie behoort rekening te worden gehouden met de bedrijfseisen voor de wijziging en de veiligheid van deze versie, d.w.z. de eventuele invoering van nieuwe beveiligingsfunctionaliteit of het aantal en de ernst van de beveiligingsproblemen die met deze versie samenhangen. Eventueel behoren herstelprogramma's (patches) in de programmatuur te worden geïmplementeerd om zwakke plekken in de beveiliging te verhelpen of te verminderen.
Leveranciers behoren alleen fysieke of logische toegang te krijgen wanneer dit noodzakelijk is voor ondersteunende diensten en met toestemming van de directie. De activiteiten van de leverancier behoren te worden gecontroleerd.

12.6 Beheer van technische kwetsbaarheden

Doel: Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

Het beheer van technische kwetsbaarheid behoort op een doeltreffende, systematische en herhaalbare wijze te worden geïmplementeerd, met metingen om de doeltreffendheid ervan te bevestigen.

12.6.1 Beheersing van technische kwetsbaarheden

Beheersmaatregel
Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

Implementatierichtlijnen
Een actueel en volledig overzicht van bedrijfsmiddelen die verband houden met IT voorzieningen is een voorwaarde voor een doeltreffend beheer van technische kwetsbaarheid. Tot de specifieke informatie die

nodig is voor de ondersteuning van beheer van technische kwetsbaarheid behoren informatie over de leverancier van programmatuur, versienummers, huidige gebruiksstatus (bijvoorbeeld welke programmatuur op welk systeem is geïnstalleerd) en de perso(o)n(en) in de organisatie verantwoordelijk voor de programmatuur.
Er behoren passende en tijdige handelingen te worden genomen als reactie op de identificatie van mogelijke technische kwetsbaarheden. De volgende richtlijnen behoren te worden gevolgd voor het opzetten van een doeltreffend beheerproces voor technische kwetsbaarheden:

a. de organisatie behoort de rollen en verantwoordelijkheden te definiëren en vast te leggen met betrekking tot het beheer van technische kwetsbaarheid, waaronder controle van de risico's, risicobeoordeling van de kwetsbaarheid, installeren van herstelprogrammatuur, nalopen van bedrijfsmiddelen en alle vereiste coördinatieverantwoordelijkheden;
b. er behoren voor programmatuur en andere IT voorzieningen informatiebronnen te worden vastgesteld om de relevante technische kwetsbaarheden te bepalen en het veiligheidsbewustzijn levend te houden;
c. er behoort een tijdpad te worden gedefinieerd waarbinnen moet worden gereageerd op aankondigingen van mogelijk relevante technische kwetsbaarheden;
d. de organisatie behoort, wanneer een mogelijk relevante technische kwetsbaarheid is vastgesteld, de bijbehorende risico's vast te stellen en de handelingen die daarop moeten worden genomen; deze handelingen zouden kunnen bestaan uit het installeren van herstelprogramma's in kwetsbare systemen en/of nemen van andere beheersmaatregelen;
e. afhankelijk van de urgentie waarmee een technische kwetsbaarheid moet worden aangepakt, behoort de genomen handeling te worden uitgevoerd in het kader van de beheersmaatregelen voor het beheer van wijzigingen of door het volgen van reactieprocedures voor informatiebeveiligingsincidenten;
f. indien een herstelprogramma beschikbaar is, behoren de risico's die gepaard gaan met het installeren van het herstelprogramma te worden beoordeeld;
g. herstelprogramma's behoren te worden getest en beoordeeld voordat ze worden geïnstalleerd om te waarborgen dat ze doeltreffend zijn en geen ontoelaatbare neveneffecten met zich meebrengen; indien geen herstelprogramma beschikbaar is behoren andere beheersmaatregelen te worden overwogen, zoals:
   - uitschakelen van diensten of mogelijkheden die betrekking hebben op de kwetsbaarheid;
   - aanpassen of toevoegen van toegangsbeveiligingsmaatregelen, bijvoorbeeld firewalls, rond de netwerkgrenzen;
   - verhoogde controle om werkelijke aanvallen te ontdekken of te voorkomen.

12.6.2 Beperkingen voor het installeren van software

Beheersmaatregel
Er moeten vastgestelde en opgevolgde regels zijn voor het installeren van software door gebruikers.

Implementatierichtlijn
Voor de (soorten) software die gebruikers mogen installeren moet er een duidelijk en zo strikt mogelijk beleid zijn. Daarbij geldt: geen rechten tenzij uitzondering nodig is. De organisatie dient die uitzonderingen vast te leggen. Updates en patches, met name van beveiligingssoftware, zijn daarbij een veel voorkomend voorbeeld. Software voor persoonlijk gebruik of software met onbetrouwbare herkomst dient zoveel mogelijk te worden uitgesloten.

Overige informatie
Onbeheerste installaties van software kunnen leiden tot diverse beveiligingsproblemen. Om deze reden is het beter om mogelijkheden voor remote beheer te onderzoeken en slechts bij uitzondering installatierechten te gunnen aan gebruikers. Een meldplicht van (beoogde/) geïnstalleerde software kan aanvullende zekerheid bieden.

12.7 Overwegingen bij audits van informatiesystemen

Doel: Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

Er behoren beheersmaatregelen te worden genomen om productiesystemen te beveiligen tijdens informatiesysteemaudits.
Bescherming is ook vereist om de integriteit van hulpmiddelen voor audits te waarborgen en misbruik van deze hulpmiddelen te voorkomen.

12.7.1 beheersmaatregelen voor audits van informatiesystemen

Beheersmaatregel
Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

Implementatierichtlijnen
De volgende richtlijnen behoren in acht te worden genomen:

a. de auditeisen behoren met de juiste managers te zijn overeengekomen;
b. de reikwijdte van de controles behoort te worden overeengekomen en beheerst;
c. de controles behoren te worden beperkt tot alleen-lezen-toegang (‘read-only’) tot programmatuur en gegevens;
d. andere toegang dan ‘alleen lezen’ behoort uitsluitend te worden toegelaten voor geïsoleerde kopieën van systeembestanden, die na beëindiging van de audit weer behoren te worden gewist of op een juiste wijze behoren te worden beschermd indien de auditdocumenatie dit vereist;
e. hulpmiddelen voor de uitvoering van de controles behoren expliciet te worden vastgesteld en beschikbaar te worden gesteld;
f. eisen voor bijzondere of aanvullende verwerking behoren te worden vastgesteld en overeengekomen;
g. alle toegang behoort te worden gecontroleerd en vastgelegd in een logbestand om een ‘audit trail’ te produceren; voor kritische gegevens of systemen behoort een ‘reference trail’ met tijdregistratie te worden overwogen;
h. alle procedures, eisen en verantwoordelijkheden behoren te worden gedocumenteerd;
i. de persoon/personen die de audit uitvoert/uitvoeren behoort/behoren geen belangen te hebben bij de activiteiten die worden geaudit.

13 COMMUNICATIEBEVEILIGING

13.1 Beheer van netwerkbeveiliging

Doel: Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

13.1.1 Maatregelen voor netwerken

Beheersmaatregel
Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk.

Implementatierichtlijnen
Systeembeheerders behoren beheersmaatregelen in te voeren voor het waarborgen van de beveiliging van informatie in netwerken en van aangesloten diensten tegen ongeoorloofde toegang. Hierbij behoort in het bijzonder rekening te worden gehouden met de volgende aspecten:

a. verantwoordelijkheden en procedures voor het beheer van apparatuur op afstand, waaronder apparatuur in gebruikersruimten, behoren te worden vastgesteld;
b. er behoren beheersmaatregelen te worden getroffen om de vertrouwelijkheid en integriteit te waarborgen van gegevens die via openbare netwerken (internet) en over draadloze netwerken worden verzonden en om de aangesloten systemen en toepassingen te beschermen (bijvoorbeeld door het gebruik van encryptie);
c. er behoort een passende registratie en controle te worden toegepast om handelingen die van belang zijn voor de beveiliging te kunnen vastleggen;
d. beheeractiviteiten behoren nauwkeurig te worden gecoördineerd, om de dienstverlening aan de organisatie te optimaliseren en om te waarborgen dat beveiligingsmaatregelen consistent worden toegepast over de informatieverwerkende infrastructuur als geheel.

13.1.2 Beleid ten aanzien van het gebruik van netwerkdiensten

Beheersmaatregel
Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.
Implementatierichtlijnen
Er behoort beleid te worden geformuleerd ten aanzien van het gebruik van netwerken en netwerkdiensten. Dit beleid zou de volgende punten moeten omvatten:

a. de netwerken en netwerkdiensten waartoe toegang wordt verleend;
b. autorisatieprocedures om te bepalen wie toegang heeft tot welke netwerken en netwerkdiensten;
c. beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en netwerkdiensten te beschermen;
d. de middelen gebruikt om toegang te krijgen tot netwerken en netwerkdiensten (bijvoorbeeld de voorwaarden waaronder toegang tot een leverancier van internetdiensten of een systeem op afstand wordt toelaten).

13.1.3 Scheiding van netwerken

Beheersmaatregel
Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

Implementatierichtlijnen
Een methode voor het beveiligen van grote netwerken is het opsplitsen van de netwerken in afzonderlijke logische domeinen, bijvoorbeeld het productienetwerkdomeinen, administratienetwerkdomein van een organisatie en externe netwerkdomeinen, die elk wordt beschermd door een afgegrensd beveiligd gebied. Er kan een getrapte verzameling beheersmaatregelen worden toegepast in verschillende logische netwerkdomeinen om de beveiligingsomgevingen van het netwerk verder te scheiden, bijvoorbeeld openbaar toegankelijke systemen, interne netwerken en kritische bedrijfsmiddelen. De domeinen behoren te worden gedefinieerd aan de hand van een risicobeoordeling en de verschillende beveiligingseisen binnen elk van de domeinen.
Een dergelijke beveiligingsomgeving kan worden geïmplementeerd door een ‘firewall’ te installeren tussen twee onderling te verbinden netwerken, om toegang en informatiestromen tussen de twee netwerkdomeinen te beheersen.

13.2 Uitwisseling van informatie

Doel: Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe partij (klant, toeleverancier, etc.).

De uitwisseling van informatie en programmatuur tussen organisaties behoort te zijn gebaseerd op een formeel uitwisselingsbeleid, dat in lijn is met de uitwisselingsovereenkomsten en behoort te worden uitgevoerd in overeenstemming met relevante wetgeving.
Er behoren procedures en normen te worden vastgesteld ter bescherming van informatie en fysieke media die informatie bevatten die wordt getransporteerd.

13.2.1 Beleid en procedures voor informatie-uitwisseling

Beheersmaatregel
Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

Implementatierichtlijnen
Voor de procedures die moeten worden gevolgd en beheersmaatregelen die moeten worden uitgevoerd bij het gebruik van elektronische communicatievoorzieningen voor informatie-uitwisseling behoren de volgende aspecten te worden overwogen:

a. procedures opgesteld om uitgewisselde informatie te beschermen tegen onderscheppen, aftappen, kopiëren, wijzigen, verkeerd verzenden en vernietigen;
b. procedures voor het ontdekken van en de bescherming tegen virussen die via het gebruik van elektronische communicatiemiddelen kan worden overgebracht;
c. procedures voor het beschermen van gevoelige elektronische informatie die wordt gecommuniceerd in de vorm van een bijlage;
d. procedures voor het beschermen van gevoelige informatie die via online applicaties wordt ontvangen, beheerd of verzonden;
e. beleid of richtlijnen waarin aanvaardbaar gebruik van elektronische communicatievoorzieningen wordt uitgelegd;
f. procedures voor het gebruik van draadloze communicatie, zoals het toepassen van encryptie;
g. de verantwoordelijkheid van werknemer, ingehuurde medewerker en elke andere gebruiker om de organisatie niet te compromitteren, bijvoorbeeld door laster, pesterij, aannemen van een valse hoedanigheid, doorsturen van kettingbrieven, aanstootgevende informatie, verrichten van ongeautoriseerde aankopen enz.;
h. gebruik van encryptie technieken, om bijvoorbeeld de geheimhouding, integriteit en authenticiteit van de informatie te beschermen;
i. richtlijnen voor bewaren en vernietigen van alle bedrijfscorrespondentie, waaronder berichten, die in overeenstemming zijn met de relevante nationale en plaatselijke wet- en regelgeving;
j. personeel erop te attenderen om geen gevoelige of kritische informatie achter te laten op multifunctionals of andere afdrukvoorzieningen, omdat deze kan worden gezien door daartoe onbevoegd personeel;
k. beheersmaatregelen en beperkingen voor doorzenden via communicatievoorzieningen, bijvoorbeeld het automatisch doorzenden van elektronische post naar externe e-mailadressen, ontsluiting via FTP server of online applicaties;
l. personeel eraan herinneren dat zij passende voorzorgen behoren te nemen, bijvoorbeeld om geen gevoelige informatie te onthullen via het opvangen of afluisteren van telefoongesprekken door:
    - mensen in de nabije omgeving, vooral bij gebruik van mobiele telefoons;
    - aftappen van telefoons met behulp van scanningontvangers;
    - mensen in de nabijheid van de ontvanger van het gesprek;

m. personeel erop attenderen om geen demografische gegevens, zoals e-mailadressen of andere persoonlijke informatie te registeren in externe programmatuur om het verzamelen voor ongeoorloofd gebruik te vermijden;
n. personeel erop attenderen dat printers en multifunctionals zijn voorzien van pagina-opslaggeheugen waarin pagina's worden opgeslagen in het geval van een papier- of transmissiestoring, die zullen worden afgedrukt zodra de storing is verholpen. In het geval van gevoelige informatie behoort personeel de daarvoor aangegeven instructie uit te voeren of contact op te nemen met de beheerder van deze bedrijfsmiddelen voor een zorgvuldige verwijdering van de opgeslagen informatie.

13.2.2 Uitwisselingsovereenkomsten

Beheersmaatregel
Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen (klanten/toeleveranciers).

Implementatierichtlijnen
De uitwisselingsovereenkomsten behoren de volgende beveiligingsaspecten te overwegen:
a. managementverantwoordelijkheden met betrekking tot beheersing en melding van doorgifte, verzending en ontvangst;
b. procedures voor kennisgeving aan de afzender van doorgifte, verzending en ontvangst. Zowel voor fysieke uitwisseling als online uitwisseling;
c. procedures voor het waarborgen van traceerbaarheid en onweerlegbaarheid;
d. technische minimumeisen voor verpakking en verzending;
e. technische eisen voor versleuteling en ontsleuteling van online verzending en ontvangst;
f. borgovereenkomsten;
g. identificatie van de verzender en ontvanger;
h. verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten, zoals bij verlies of verminking van gegevens;
i. gebruik van een overeengekomen labelsysteem voor gevoelige of kritische informatie, om te waarborgen dat de betekenis van de labels meteen wordt begrepen en dat de informatie op de juiste manier wordt beschermd;
j. het bepalen van de eigenaar van gegevens en programmatuur en het vastleggen van de verantwoordelijkheden voor gegevensbescherming, auteursrechten, licenties van programmatuur en vergelijkbare aspecten;
k. eventueel vereiste bijzondere beheersmaatregelen om gevoelige gegevens te beschermen, zoals het toepassen van cryptografische sleutels.

Er behoren procedures, normen en beleid te worden vastgesteld en onderhouden om informatie en fysieke media die worden getransporteerd te beschermen, en hier moet naar verwezen worden in de uitwisselingsovereenkomst.
De beveiligingsinhoud van elke overeenkomst behoort in overeenstemming te zijn met de gevoeligheid van de desbetreffende bedrijfsinformatie.

Overige informatie
Overeenkomsten kunnen elektronisch of in de vorm van een papieren document bestaan en kunnen in de vorm van formele contracten zijn opgesteld of als onderdeel van de dienstverlening. Voor gevoelige informatie behoren de specifieke mechanismen voor de uitwisseling van die informatie consistent te zijn voor alle organisaties en alle soorten overeenkomsten.

13.2.3 Elektronisch berichtenuitwisseling

Beheersmaatregel
Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.

Implementatierichtlijnen
De overwegingen voor het elektronische berichtenverkeer behoren onder meer te zijn:
a. beschermen van berichten tegen toegang door onbevoegden, wijziging of weigeren van dienst;
b. waarborgen van correcte adressering en transport van het bericht;
c. Toevoegen van een disclaimer aan het bericht;
d. volledige betrouwbaarheid en beschikbaarheid van de dienst;
e. wettelijke overwegingen, bijvoorbeeld eisen te stellen aan elektronische handtekeningen;
f. verkrijgen van voorafgaande toestemming voor het gebruiken van externe openbare diensten, zoals 'instant messaging' of 'file sharing';

13.2.4 Beveiliging regelen in overeenkomsten met een derde partij

Beheersmaatregel
In overeenkomsten met derden waarbij toegang tot, of het verwerken en beheer van informatie of IT voorzieningen of daaraan gekoppelde bedrijfsmiddelen van de organisatie sprake is, behoren alle relevante beveiligingseisen te zijn opgenomen.

Implementatierichtlijnen
De volgende punten behoren te worden overwogen voor opname in de overeenkomst om te waarborgen dat er geen misverstanden bestaan tussen de organisatie en een derde partij. Organisaties behoren zich ervan te vergewissen dat de aansprakelijkheid van een derde partij voldoende is afgedekt.
In een dergelijke overeenkomst behoren de volgende punten te worden opgenomen om invulling te geven aan de vastgestelde beveiligingseisen (zie 7.2.1):
a. het informatiebeveiligingsbeleid;
b. beheersmaatregelen voor het waarborgen van de bescherming van bedrijfsmiddelen, waaronder:
   - procedures voor de bescherming van bedrijfsmiddelen, waaronder informatie, programmatuur, hardware of gebruik van online services;
   - alle benodigde fysieke beschermingsmaatregelen en -mechanismen;
   - beheersmaatregelen ter bescherming tegen virussen, phishing of aanvallen van toegang;
   - procedures om vast te stellen of bedrijfsmiddelen gecompromitteerd zijn, bijvoorbeeld of zich verlies of wijziging van informatie, programmatuur en hardware heeft voorgedaan;
   - beheersmaatregelen om de teruggave of vernietiging van informatie en andere bedrijfsmiddelen aan het einde van of op een overeengekomen tijdstip tijdens de looptijd van de overeenkomst te waarborgen. Er behoren procedures te zijn voor het beheer en terugleveren van data van klanten waarvoor gebruik wordt gemaakt van online services van derden;
   - beperkingen ten aanzien van het beschikbaar stellen voor verwerking in productie, kopiëren en openbaar maken van informatie en het gebruik van geheimhoudingsovereenkomsten;
c. opleiding voor gebruikers en (externe) beheerders op het gebied van het gebruik en de beveiliging van systemen;
d. waarborgen dat gebruikers zich bewust zijn van verantwoordelijkheden en aspecten van informatiebeveiliging;
e. een voorziening voor het overplaatsen van personeel, waar van toepassing;
f. verantwoordelijkheden ten aanzien van installatie en onderhoud van hardware en programmatuur;
g. een duidelijke rapportagestructuur en afspraken over de vorm van de rapportage;
h. een duidelijk en gespecificeerd proces voor het beheer van wijzigingen;
i. afspraken over toegangsbeleid, waaronder:

- de verschillende redenen, eisen en voordelen die de toegang voor de derde partij noodzakelijk maken;
- goedgekeurde toegangsmethoden, evenals beheersing en gebruik van unieke identificatiemethoden zoals gebruikersidentificaties en wachtwoorden;
- een autorisatieproces voor toegang en speciale bevoegdheden van gebruikers;
- een verplichting tot het bijhouden van een lijst van personen die bevoegd zijn de ter beschikking gestelde dienst te gebruiken, en wat hun rechten en speciale bevoegdheden zijn ten aanzien van een dergelijk gebruik;
- een proces voor het intrekken van toegangsrechten of voor het onderbreken van de verbinding tussen de systemen;

j. afspraken over rapportage, kennisgeving en onderzoek naar informatiebeveiligingsincidenten en lekken in de beveiliging; evenals schendingen van de eisen opgesomd in de overeenkomst;
k. een beschrijving van het product dat of de dienst die beschikbaar wordt gesteld, en een beschrijving van de informatie die moet worden verstrekt samen met de beveiligingsclassificatie;
l. het beoogde serviceniveau en wanneer het serviceniveaus onvoldoende is;
m. de definitie van verifieerbare prestatiecriteria en het controleren daarvan en rapportage daarover;
n. het recht om elke activiteit verband houdend met de bedrijfsmiddelen van de organisatie te controleren of in te trekken;
o. het recht de in de overeenkomst vastgelegde verantwoordelijkheden te auditen, deze audit door een derde partij te laten uitvoeren;
p. het vaststellen van een escalatieproces voor het oplossen van problemen;
q. eisen voor servicecontinuïteit, waaronder maatregelen voor beschikbaarheid en betrouwbaarheid, in overeenstemming met de bedrijfsprioriteiten van de organisatie;
r. de respectievelijke aansprakelijkheden van de partijen die bij de overeenkomst betrokken zijn;
s. verantwoordelijkheden met betrekking tot juridische aangelegenheden en hoe wordt gewaarborgd dat wordt voldaan aan de wettelijke eisen, bijvoorbeeld de wetgeving voor gegevensbescherming, waarbij in het bijzonder rekening wordt gehouden met de verschillende nationale rechtssystemen als de overeenkomst betrekking heeft op samenwerking met organisaties in andere landen;
t. het beheer van intellectuele eigendomsrechten en bescherming van gezamenlijk werk;
u. betrokkenheid van een derde partij met onderaannemers, en de beveiligingsmaatregelen die deze onderaannemers moeten implementeren;
v. voorwaarden voor heronderhandeling/beëindigen van overeenkomsten.

Overige informatie
Bijzondere aandacht is vereist wanneer met derden partijen wordt gewerkt voor de productie van informatiegevoelige producten (bijv. jaarverslagen) en wanneer digitaal materiaal wordt verwerkt waar rechten op berusten. Daarnaast zijn specifieke maatregelen nodig wanneer wordt gewerkt met waardedragende producten of deze producten worden geproduceerd.

14 VERWERVING, ONTWIKKELING EN ONDERHOUD VAN INFORMATIESYSTEMEN

14.1 Beveiligingseisen voor informatiesystemen

Doel: Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

Informatiesystemen omvatten besturingssystemen, infrastructuur, bedrijfstoepassingen, kant-en-klare producten, diensten en toepassingen die door de gebruiker zijn ontwikkeld. Ontwerp en implementatie van het informatiesysteem dat het bedrijfsproces ondersteunt kunnen van doorslaggevend belang zijn voor de

beveiliging. Beveiligingseisen behoren voorafgaand aan de ontwikkeling en/of implementatie van informatiesystemen te worden vastgesteld en overeengekomen.
Alle beveiligingseisen behoren te worden vastgesteld tijdens de specificatie van de eisen voor het project en behoren te worden verantwoord, overeengekomen en gedocumenteerd als onderdeel van de verwerving van een informatiesysteem.

14.1.1 Analyse en specificatie van beveiligingseisen bij de verwerving van informatiesystemen

Beheersmaatregel
Bij het opstellen van de eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.
In het proces van aanschaf van informatiesystemen behoren deze eisen in het inkoopproces te worden meegenomen. In de contracten met de leverancier behoren de vastgestelde beveiligingseisen te zijn opgenomen. Waar de beveiligingsfunctionaliteit in een voorgesteld product niet voldoet aan de gestelde eis, behoren het geïntroduceerde risico en de daarmee verbonden beheersmaatregelen te worden heroverwogen alvorens het product aan te schaffen. Waar extra functionaliteit wordt geleverd die een beveiligingsrisico met zich meebrengt, behoort dit risico te worden uitgeschakeld of behoort de voorgestelde beheersstructuur opnieuw te worden beoordeeld om te bepalen of er voordeel te behalen is uit de extra functionaliteit die beschikbaar is.

Implementatierichtlijnen
In de eisen voor beveiligingsmaatregelen behoort te worden aangegeven welke geautomatiseerde beheersmaatregelen in het systeem moeten worden ingebouwd, evenals de behoefte aan ondersteunende handmatige beheersmaatregelen. Vergelijkbare afwegingen behoren te worden gemaakt bij het beoordelen van programmatuur die wordt ontwikkeld of aangeschaft voor bedrijfstoepassingen.

Overige informatie
In het bijlagedocument is een checklist opgenomen.

14.1.2 Toepassingen op openbare netwerken beveiligen

Beheersmaatregel
Uitvoeringsdiensten (toepassingen) die via openbare netwerken gevoed worden met informatie moeten beschermd worden tegen o.a. fraude, contractgeschillen, onbevoegde openbaarmaking en vandalisme.

Implementatierichtlijn
Wanneer het beleid en de beveiliging worden opgesteld voor toepassingen die gebruik maken van openbare netwerken (bijvoorbeeld bestelsystemen via de eigen website, informatie-uitwisseling via de eigen website, en informatie-transacties over (draadloze) telecomsystemen) dan dient met het volgende rekening gehouden te worden:

a. Het garanderen van de identiteit van beide partijen, bijvoorbeeld door authenticatie
b. Een procedure die duidelijk maakt wie geautoriseerd is voor het goedkeuren van (belangrijke) transactiedocumenten, het ondertekenen ervan en ze in circulatie mag brengen (lees: mag communiceren)
c. Het volledig informeren van de communicerende partijen met betrekking tot hun bevoegdheden om de dienst/toepassing te gebruiken
d. Vaststellen welke (samen afdoende) eisen er zijn zodat vertrouwelijkheid, integriteit, bewijsbaarheid (van verzending en ontvangst) en (juridische) onweerlegbaarheid van totstand gekomen afspraken en/of contracten gegarandeerd kunnen worden.
e. Vaststelling van de integriteit van belangrijke documenten (bijvoorbeeld via hash checks)
f. In hoeverre vertrouwelijke informatie beschermd is;

g. Specifiek de vertrouwelijkheid en integriteit van ordertransacties, betalingsinformatie, gegevens betreffende adressen en (ontvangst)bevestigingen;
h. Verificatie en controle van betalingsinformatie
i. De juiste betalingsvorm om te beschermen tegen fraude
j. Het noodzakelijke beschermingsniveau om de vertrouwelijkheid en integriteit van orderinformatie te handhaven
k. Beschermingsmaatregelen tegen het verlies, verminking of duplicatie van transactie-informatie
l. Aansprakelijkheid in verband met frauduleuze of anderszins onwettige transacties
m. Eisen met betrekking tot verzekering

Cryptografie kan (mede) een maatregel zijn voor het beheersen van (een aantal van) bovenstaande zaken.

Naast de maatregelen die de toepassingen in de praktijk beschermen, dienen er ook afspraken of schriftelijke overeenkomsten tussen partners te zijn die hen houdt aan de voorwaarden van de diensten en alle punten hierboven.

Ook de veiligheid van de communicerende informatiesystemen (firewalls / servers) en capaciteit van datalijnen en tussenliggende technische onderdelen.

Overige informatie
Toepassingen die toegankelijk zijn, of met informatie gevoed worden via, publieke netwerken staan bloot aan frauduleuze activiteiten, geschillen over contracten of openbaarmaking van informatie. Denk aan webshops of geïntegreerde afroep- en (maatwerk)productiesystemen. De potentiele schade is groot en om deze reden is een goede beoordeling van het daadwerkelijke risico, voor en na het invoeren van maatregelen, noodzakelijk. Naast cryptografie zijn er ook (diverse niveaus) van digitale handtekeningen (welke ook onder wetgeving vallen).

14.1.3 Transacties van toepassingen beschermen

Beheersmaatregel
Informatie die (binnen en voor transacties) uitgewisseld wordt tussen toepassingen moet worden beschermd zodat deze volledig, juist gerouteerd, ongewijzigd en afdoende vertrouwelijk kan plaatsvinden.

Implementatierichtlijn
Bij de beveiliging van transacties van toepassingen moet het volgende overwogen worden:
a. het toepassen van elektronische handtekeningen door bij de transactie betrokken partijen;
b. de specifieke aspecten van de transactie zelf, wat inhoudt:
   - dat (geheime) authenticatie-informatie geldig en geverifieerd is;
   - dat de transactie vertrouwelijk blijft;
   - dat de privacy van alle betrokken partijen in stand gehouden wordt.
c. versleutelende communicatiekanalen tussen de betrokken partijen / toepassingen;
d. beveiliging van communicatieprotocollen;
e. ervoor zorgen dat transactiegegevens niet op een publiek toegankelijke
f. omgeving bewaard worden of toegankelijk zijn;
g. bij eventueel gebruik van een certificaat (ter beveiliging van handtekeningen / digitale kanalen), het opnemen van dat certificaat in het beheer van certificaten van het bedrijf.

Overige informatie
Toepassingen kunnen informatie uitwisselen die als status een formele transactie tussen twee partijen tot stand brengt. De juistheid en veiligheid hiervan is van belang voor beide (of ‘alle’ partijen) die bij de transactie

betrokken zijn. De beheersmaatregelen voor transacties tussen systemen moeten daarom afgestemd zijn op het (potentiele) belang of risico dat ontstaat uit deze transacties.

De transactie valt onder tenminste één rechtsgebied. De transacties (en hun beheersmaatregelen) moeten dus voldoen aan de wet- en regelgeving van dat gebied. Daarbij is het van belang dat de transactie op verschillende plekken kan worden geïnitieerd, verwerkt, uitgevoerd of opgeslagen / gearchiveerd.

14.2 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doel: Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

Managers die verantwoordelijk zijn voor toepassingssysteem, behoren ook verantwoordelijk te zijn voor de beveiliging van de projectomgeving of ondersteunende omgeving.

14.2.1 Beleid voor beveiligd ontwikkelen

Beheersmaatregel
Het ontwikkelen van software en/of systemen moet gebonden zijn aan vastgestelde regels welke ook moeten worden toegepast op de eigen ontwikkelactiviteiten binnen de organisatie.

Implementatierichtlijn
Beveiligd ontwikkelen is het vertrekpunt voor het realiseren van beveiligde dienstverlening, architecturen, software en/of een beveiligd systeem. Overwegingen voor het beleid rondom ontwikkeling zijn:

a. de beveiliging van de ontwikkelomgeving (software, netwerk, fysieke locatie);
b. richtlijnen hoe te handelen t.o.v. beveiliging gedurende de levenscyclus van softwareontwikkeling;
   - beveiliging in de toegepaste ontwikkelmethodologie;
   - obfuscatie / beveiligdecoderingsrichtlijnen voor elke programmeertaal die wordt gebruikt.
b. overige beveiligingseisen specifiek voor de ontwikkelfase (mensen, informatiebeheer, enz.);
c. beveiligingscontrolepunten of testen binnen de mijlpalen of oplevering van deelproducten van het project;
d. beveiligde informatiecentra binnen of buiten de eigen organisatie;
e. beveiliging van de versiecontrole en sourcecodebeheer;
f. vereiste kennis over toepassingsbeveiliging (waaronder ontwerpprincipes voor toepassingen);
g. de vaardigheden en voorzieningen van de ontwikkelaar die hem in staat stellen om kwetsbaarheden te voorkomen, opsporen en corrigeren/repareren.

Veilig programmeren, en de toegepaste technieken en beheersmaatregelen moeten gelden voor nieuwe ontwikkelingen en voor oude code (‘legacy’) waarvoor in het verleden andere normen golden en minder geavanceerde beveiligingstechnieken beschikbaar waren.

(Ook) wanneer derde partijen ontwikkelen voor de organisatie dient de organisatie er op toe te zien en te borgen dat deze organisatie zich houdt aan dezelfde richtlijnen.

Overige informatie
Ook binnen toepassingen kan ontwikkeling plaatsvinden, zoals binnen kantoortoepassingen (Office pakketten), scripting, browsers en databases. De impact van dit soort ontwikkeling en de risico’s die ermee gepaard gaan kunnen sterk verschillen. Ook betekent dit dat er mogelijk ontwikkelomgevingen binnen de organisatie zijn die onvoldoende bekend zijn, en dat er medewerkers betrokken zijn bij ontwikkelwerkzaamheden waarvan dit niet bekend is.

14.2.2 Procedures voor wijzigingsbeheer van informatiesystemen

Beheersmaatregel
De implementatie van wijzigingen in informatiesystemen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.

Implementatierichtlijnen
Er behoren formele procedures voor wijzigingsbeheer te worden gedocumenteerd en afgedwongen om de kans op corrumperen van informatiesystemen tot een minimum te beperken. Het invoeren van nieuwe systemen en belangrijke wijzigingen in bestaande systemen behoort een formeel proces te volgen van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie.
In dit proces behoort een risicobeoordeling, een analyse van de gevolgen van wijzigingen en een specificatie van de benodigde beveiligingsmaatregelen te zijn opgenomen. Dit proces behoort ook te waarborgen dat bestaande beveiligings- en beheersingsprocedures niet gecompromitteerd worden, dat ondersteunende programmeurs uitsluitend toegang wordt verleend tot die onderdelen van het systeem die ze voor hun werk nodig hebben en dat formele instemming en goedkeuring wordt verkregen voor alle wijzigingen.
Waar mogelijk behoren procedures voor wijzigingsbeheer voor toepassingsprogrammatuur en voor de operationele omgeving te worden geïntegreerd. De wijzigingsprocedures behoren de volgende punten te omvatten:

a. bijhouden van een registratie van overeengekomen autorisatieniveaus;
b. waarborgen dat wijzigingen alleen worden doorgevoerd door bevoegde gebruikers;
c. beoordelen van beheersmaatregelen en integriteitprocedures om te waarborgen dat deze niet door de wijzigingen gecompromitteerd worden;
d. identificatie van alle programmatuur, informatie, databases en apparatuur die wijziging behoeven;
e. vooraf verkrijgen van formele goedkeuring voor voorstellen voor wijziging;
f. waarborgen dat bevoegde gebruikers de wijzigingen aanvaarden voordat ze worden geïmplementeerd;
g. waarborgen dat de systeemdocumentatie na elke wijziging wordt geüpdatet en dat oude documentatie wordt gearchiveerd of verwijderd;
h. versiebeheer uitvoeren voor alle programmatuur-updates;
i. bijhouden van een ‘audit trail’ van alle wijzigingsaanvragen;
j. waarborgen dat de bedrijfsdocumentatie en gebruikersprocedures worden veranderd zover noodzakelijk om toepasbaar te blijven;
k. waarborgen dat de implementatie van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.

Overige informatie
Wijzigingen in programmatuur kunnen invloed hebben op de bedrijfsomgeving.
Een goede procedure omvat het testen van nieuwe programmatuur in een omgeving die gescheiden is van zowel de productie- als de ontwikkelingsomgevingen.

14.2.3 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

Maatregel
Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

Implementatierichtlijnen
Dit proces behoort te omvatten:

a) beoordelen van de toepassingbeheersmaatregelen en integriteitprocedures voor de toepassing om te waarborgen dat zij niet gecompromitteerd worden door de wijzigingen in het besturingssysteem;

b) waarborgen dat in het jaarlijkse onderhoudsplan en -budget rekening wordt gehouden met beoordeling en testen als gevolg van wijzigingen in het besturingssysteem;
c) waarborgen dat wijzigingen in het besturingssysteem tijdig worden aangekondigd, zodat de noodzakelijke tests en beoordelingen kunnen worden uitgevoerd voordat de wijzigingen worden geïmplementeerd;
d) waarborgen dat de benodigde wijzigingen worden aangebracht in de bedrijfscontinuïteitsplannen.

Een persoon (systeembeheerder) behoort te worden belast met de verantwoordelijkheid voor het controleren van zwakke plekken en van herstelprogramma's ('patches') en reparaties ('fixes') van leveranciers.

14.2.4 Beperkingen op wijzigingen in programmatuurpakketten

Beheersmaatregel
Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen en alle wijzigingen behoren strikt te worden beheerst.

Implementatierichtlijnen
Voor zover mogelijk en praktisch uitvoerbaar behoort kant-en-klaar geleverde programmatuur ongewijzigd te worden gebruikt. Waar wijzigingen in deze programmatuur noodzakelijk zijn, behoort rekening te worden gehouden met de volgende punten:
a. het risico dat ingebouwde beheersmaatregelen en integriteitprocessen gecompromitteerd raken;
b. toestemming van de leverancier behoort te worden verkregen;
c. de mogelijkheid de gewenste wijzigingen te verkrijgen van de leverancier in de vorm van standaard programma-updates;
d. de impact op de organisatie als deze verantwoordelijk wordt gehouden voor toekomstig onderhoud van de programmatuur als gevolg van wijzigingen.

Indien wijzigingen noodzakelijk zijn, behoort de oorspronkelijke programmatuur te worden bewaard en behoren de wijzigingen te worden aangebracht in een duidelijk gemarkeerde kopie. Er behoort een beheerproces voor programmatuur-updates te worden ingevoerd om te waarborgen dat de meest recente goedgekeurde herstelprogramma's en updates van toepassingen voor alle goedgekeurde programmatuur zijn geïnstalleerd. Alle wijzigingen behoren volledig te worden getest en gedocumenteerd, zodat ze indien nodig opnieuw kunnen worden aangebracht in toekomstige upgrades van de programmatuur.

14.2.5 Principes voor engineering van beveiligde systemen

Beheersmaatregel
Voor het engineeren van beveiligde systemen dienen principes te zijn vastgesteld, gedocumenteerd, onderhouden en in de praktijk worden gehandhaafd voor alle handelingen die uitgevoerd worden voor het implementeren van informatiesystemen.

Implementatierichtlijn
Beveiligde systemen worden opgebouwd door een gelaagde architectuur (business/UI/commercie, data, toepassingen en technologie) waarbij elke laag zijn eigen veiligheidsrisico's, beheersmaatregelen en gebruikersbehoeften kent. Voor deze gelaagde architectuur dient de organisatie een aantal geldende principes en/of procedures op te stellen, waaraan elk totaal systeem dient te voldoen. Deze principes moeten rekening houden met bekende aanvalsmethoden op het totale systeem.

De procedures/principes moeten regelmatig worden beoordeeld, geëvalueerd en geactualiseerd.

Dezelfde principes dienen te worden toegepast voor externe ontwikkeling van systemen en bij nieuwe toepassing van externe systemen, waarna de garantstelling voor voldoen aan deze principes via contracten of verdere overeenkomsten geregeld wordt.

14.2.6 Beveiligde ontwikkelomgeving

Beheersmaatregel
Organisaties moeten de beveiligde ontwikkelomgeving vaststellen en daadwerkelijk passend beveiligen voor werkzaamheden die betrekking hebben op (de hele levenscyclus van) systeemontwikkeling en systeemintegratie.

Implementatierichtlijn
Een beveiligde ontwikkelomgeving beschouwt en beheerst technologie, maar ook mensen en (werk)processen. De risico's die horen bij individuele handelingen voor systeemontwikkeling en de bij systeemontwikkeling passende beveiligde omgeving dienen worden vastgesteld. Daarbij moet rekening gehouden worden met:

a. de classificatie (gevoeligheid, beschikbaarheid, enz.) van de gegevens die door het systeem worden verwerkt, opgeslagen en/of verstuurd;
b. reeds geldende of nieuw op te stellen/te verwachtend externe en interne eisen, bijv. van regelgeving of beleidsregels;
c. reeds bestaande beheersmaatregelen voor beveiliging die bijdragen aan de veiligheid van de ontwikkelomgeving;
d. betrouwbaarheid van personeel dat in de omgeving werkt;
e. welke aspecten van systeemontwikkeling (al) wel of niet uitbesteed worden;
f. de eventuele noodzaak verschillende ontwikkelomgevingen te scheiden;
g. toegangsbeveiliging;
h. monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes;
i. back-ups van de ontwikkelomgeving in veilige locaties in combinatie met code/versiebeheer;
j. controle over bewegingen van gegevens van en naar de omgeving (en eventuele omvorming van gegevens naar minder gevoelige classificatie indien noodzakelijk).

Na het vaststellen van de beveiligingseisen voor een omgeving moeten organisaties de corresponderende processen documenteren en ervoor zorgen dat de betrokken personen deze kennen en toepassen.

14.2.7 Uitbestede ontwikkeling van programmatuur

Beheersmaatregel
Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.

Implementatierichtlijnen
Waar ontwikkeling van programmatuur wordt uitbesteed, behoort rekening te worden gehouden met de volgende punten:

a. licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten;
b. certificatie van de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
c. zorgen voor een borg in geval een derde partij in gebreke blijft;
d. toegangsrechten voor het uitvoeren van een audit op de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
e. contractuele eisen voor de kwaliteit en beveiligingsfunctionaliteit van de broncode;
f. testen voorafgaand aan installatie, om eventuele virussen en Trojans te ontdekken.

14.2.8 Testen van systeembeveiliging

Beheersmaatregel
De beveiligingstechnieken / - functionaliteit dient tijdens de ontwikkeling getest te worden.

Implementatierichtlijn
Testen van nieuwe of geactualiseerde systemen dienen grondig en verifieerbaar uitgevoerd te worden, op basis van een gedefinieerd schema van testen, inclusief tests van input- en outputbestanden volgens alle belangrijke scenario's. Voor interne ontwikkelactiviteiten worden deze in eerste instantie door de eigen ontwikkelaars uitgevoerd, waarna onafhankelijke tests noodzakelijk zijn (door derden of door klant). Afhankelijk van het belang van het systeem en de gebruikte ontwikkelmethode (waterfall / agile) dient de omvang van het testen groter of kleiner te zijn.

14.2.9 Systeemacceptatietests

Beheersmaatregel
Nieuwe informatiesystemen (inclusief nieuwe versies en updates/upgrades) moeten uitgevoerd worden conform een programma van acceptatietesten.

Implementatierichtlijn
Bij een systeemacceptatietest moeten eisen voor informatiebeveiliging mede worden getoetst, op passende wijze bij de overige geldende beleidsregels. De acceptatietest zelf dient tevens veilig uitgevoerd te (kunnen) worden in een afdoende representatieve testomgeving (waarbij zoveel mogelijk externe systemen die in de productieomgeving aanwezig zijn ook in de testomgeving aanwezig zijn), met fallback procedure. De test kunnen (deels) geautomatiseerd uitgevoerd worden (scanmethoden) op code, toepassing, data of andere onderdelen van de architectuur (waaronder ontvangen componenten en geïntegreerde systemen).

14.3 Testgegevens

Doel: Beschermen van gegevens die voor testen worden gebruikt.

14.3.1 Bescherming van testgegevens

Beheersmaatregel
Testgegevens moeten te worden gekozen, beschermd, eventueel geanonimiseerd en gecontroleerd.

Implementatierichtlijn
Diverse paragrafen onder 14.2 beschrijven de noodzaak tot testen, bij voorkeur met zo realistisch mogelijk gegevens. Recente productiegegevens komen hiervoor het meest in aanmerking, maar kunnen gevoelige en/of vertrouwelijke informatie bevatten. Bij het gebruik van productiegegevens (of andere gegevenssets) dient er zorg voor te zijn dat de gevoelige inhoud beschermd is (verwijderen of overschreven).

15 LEVERANCIERSRELATIES

15.1 Informatiebeveiliging in leveranciersrelaties

Doel: bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers beschermen.

15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties

Beheersmaatregel
Met leveranciers die toegang hebben tot bedrijfsmiddelen van de organisatie moeten gedocumenteerde (informatiebeveiligings-)eisen formeel overeengekomen worden.

Implementatierichtlijn
Om de werkzaamheden van de leverancier te beheersen, en daarbinnen specifiek de toegang van de leveranciers tot informatie, moeten gepaste beheersmaatregelen verplicht gesteld worden. De (te overwegen)

processen en procedures waar een leverancier zich aan moet committeren, behelzen onder andere (waar nodig per (type) informatie/leverancier):

a. vaststellen en documenteren welke soorten leveranciers, bijv. IT-diensten, logistieke voorzieningen, financiële diensten, IT-infrastructuurcomponenten, monteurs, certificerende instellingen er zijn (waarvan de organisatie de toegang tot de informatie wil toestaan);
b. een standaard proces voor het beheren van leveranciersrelaties (waaronder evaluatie);
c. definiëren van de soorten informatietoegang die verschillende soorten leveranciers wordt toegestaan, en deze toegang monitoren en controleren, eventueel door begeleiding;
d. de minimale informatiebeveiligingseisen die gelden voor elk soort informatie en elk soort toegang. Dit dient als basis voor leveranciersovereenkomsten met elke leverancier, passend bij het risicoprofiel of informatieclassificatie;
e. processen en procedures voor het monitoren van de naleving van vastgestelde
f. informatiebeveiligingseisen, waarbij indien nodig ook externe controle ingezet wordt
g. beheersmaatregelen om de integriteit van de informatie of informatieverwerking die elke partij biedt te borgen (controle van nauwkeurigheid en volledigheid);
h. de soorten verplichtingen om de informatie van de organisatie te beschermen die van toepassing (moeten) zijn op leveranciers;
i. hoe bij een incident of noodsituatie omgegaan wordt met toegang voor leveranciers, met
j. duidelijke verdeling van de verantwoordelijkheden van zowel de organisatie als van de leveranciers;
k. i) afspraken en voorzieningen voor flexibiliteit (schaalbaarheid en beschikbaarheid van respons) en voor herstel en noodsituaties om de beschikbaarheid te waarborgen van de informatie, informatiesystemen of de informatieverwerking die door elk van de partijen wordt geboden;
l. bewustzijnstraining voor de medewerkers die betrokken zijn bij inkoop en/of acquisitie (of om andere reden nauw contact met leveranciers onderhouden) over het toepasselijke beleid en bijbehorende processen, procedures, methoden en/of instructies.
m. trainingen voor verhogen van het bewustzijn en betrokkenheid van personeel van de organisatie dat contact heeft met personeel van de leverancier. Dit zodat het personeel op basis van regels het juiste gedrag kan vertonen naar de verschillende soorten leveranciers.
n. de manier waarop voorwaarden en eisen in overeenkomsten moeten worden vastgelegd.
o. bij het overbrengen van (grotere hoeveelheden) informatie en/of informatieverwerkende systemen moeten alle aspecten van informatie tijdens de hele transitieperiode gelden.

Overige informatie
Bij het vaststellen van overeenkomsten kunnen geheimhoudingsovereenkomsten toegepast worden.

De organisatie dient te beseffen dat er een wettelijke verantwoordelijk voor het veilig houden van informatie bij zichzelf ligt. Ook in gevallen waar er sprake is van bewerkersovereenkomsten is er een eigen verantwoordelijkheid. Bij grensoverschrijdende informatieoverbrenging kunnen meerdere jurisdicties van toepassing zijn.

Monteurs of andere leveranciers welke niet direct toegang tot primaire informatieverwerkende systemen hebben zijn vaak slecht in beeld als partijen welke alsnog een hoog niveau van toegang kunnen verkrijgen (en eventueel, al dan niet met gebruik van een eigen computer, gegevens kunnen zien in en rondom de apparatuur die ze onderhouden) en welke langere periode zonder supervisie in de organisatie verblijven.

15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Beheersmaatregel
Alle toegepaste en benodigde eisen voor informatiebeveiliging moeten daadwerkelijk worden vastgesteld en overeengekomen met alle leveranciers die toegang hebben tot de IT infrastructuur of die bewerkingen (inclusief opslag en communicatie) doen op de informatie van de organisatie.

Implementatierichtlijn
Niet alleen het beleid voor leveranciers dient er te zijn, de daadwerkelijke leveranciers-overeenkomsten dienen gedocumenteerd te zijn om de verplichtingen van beide partijen duidelijk en zonder misverstanden vast te leggen. De volgende voorwaarden kunnen in deze overeenkomsten relevant zijn:

a. Een omschrijving van de te verschaffen of toegankelijk te maken informatie en de manier waarop dit zal gebeuren.
b. Classificatie van die informatie conform het schema van de organisatie (zie 8.2). Indien de leverancier ook een schema hanteert, een duiding hoe de verschillende schema's zich met elkaar verhouden (een 'mapping').
c. De relevante wettelijke en regelgevende eisen, waaronder bescherming van (persoons)gegevens, intellectueel eigendom, auteursrecht (handelsnamenrecht, merkenrecht) en hoe de overeenkomst conform deze wetten zorgt voor de juiste bescherming.
d. De verplichtingen van elke partij om (en eventueel welke (typen)) bescherming te implementeren en handhaven (toegangsbeveiliging (fysiek en netwerk), monitoring en rapportage en auditing
e. Een omschrijving van het aanvaardbaar gebruik, en uitsluiten van onaanvaardbaar (of overig) gebruik
f. Eventueel een expliciete lijst van personeel van de leveranciers dat toegang mag hebben tot de informatie (of deze mag ontvangen en bewerken), óf een omschrijving van de procedure waarop personeel autorisatie kan verkrijgen en hoe deze weer ingetrokken wordt.
g. Opname van de betreffende beleidsregels in het betreffende contract;
h. De manier waarop omgegaan wordt met incidenten (met specifieke aandacht voor tijdige alarmering betreffende het incident en de wijze van samenwerken om het incident op te lossen).
i. Training, voorlichting en bewustzijnseisen voor beveiligingsmaatregelen en –eisen in het contract voor zover nodig.
j. Geldende regelgeving voor het type zakelijke onderaanneming / uitbesteding
k. Tekenbevoegde en overige betrokken partners (inclusief contactpersonen) bij de overeenkomst
l. Eventueel noodzakelijke screening van personeel van leveranciers en de procedures die voor de screening gevolgd moeten worden, met name melding van twijfelachtige resultaten van de screening
m. Het recht om de beheersmaatregelen en procedures van de leverancier te auditen (binnen de scope van het contract)
n. De werkwijze voor het oplossen van mankementen en conflicten
o. De rapporten die de leverancier stuurt om aan te tonen dat de ingestelde beheersmaatregelen afdoende werken en hoe eventuele afwijkingen opgelost worden.
p. De algemene verplichting van de leverancier om te handelen conform de beveiligingseisen van de organisatie en hierdoor aan de eisen te voldoen.

Overige informatie
Er kunnen grote verschillen zijn de overeenkomsten en eisen die daarbinnen nodig zijn. De overeenkomsten moeten passend zijn bij de aard en omvang van de betrokken beveiligingsrisico's. Voor de overeenkomsten moet (meestal) ook geregeld zijn dat deze ook van toepassing zijn op onderaannemers van de leverancier, die met dezelfde zorgvuldigheid moeten handelen.

Indien er een risico is dat de organisatie haar producten en diensten niet meer kan leveren bij wegvallen of vertraging bij de leverancier, kan het noodzakelijk zijn om hiervoor procedures op te stellen.

15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Beheersmaatregel
Naast de algemene eisen voor leveranciersrelaties dienen overeenkomsten met leveranciers van producten en diensten van informatie- en communicatietechnologie aanvullende eisen te bevatten voor de hele toeleveringsketen van deze technologie.

Implementatierichtlijn
De eisen voor de toeleveringsketen die de organisatie moet overwegen zijn:
a. welke specifieke eisen gedefinieerd moeten worden voor (de acquisitie van) producten of diensten op het gebied van informatie- en communicatietechnologie
b. de eis dat leveranciers de eisen betreffende diensten op het gebied van informatie- en communicatietechnologie in de hele toeleveringsketen bekend maken (en bekrachtigen) indien zij zelf diensten uitbesteden
c. de eis dat leveranciers de eisen betreffende producten op het gebied van informatie- en communicatietechnologie in de hele toeleveringsketen bekend maken (en bekrachtigen) indien de producten van de directie leveranciers componenten bevatten die uit de keten worden aangeleverd
d. een manier om te valideren en monitoren dat de geleverde producten en diensten daadwerkelijk voldoen aan de opgestelde beveiligingseisen
e. een proces waardoor de organisatie vaststelt welke componenten van producten of diensten essentieel zijn en waardoor aanvullende aandacht nodig is als de directie leverancier deze aan andere leveranciers heeft uitbesteedt;
f. de methoden waardoor de herkomst van de componenten in de keten kan worden bewezen
g. de testen waardoor zekerheid ontstaat dat de geleverde producten op het gebied van informatie- en communicatietechnologie inderdaad werken zoals beoogd;
h. de regels die gelden voor het delen van informatie over de toeleveringsketen, potentiële kwesties en compromissen tussen de organisatie en leveranciers;
i. eisen voor alle fasen van de levenscyclus van de componenten van de informatie- en communicatietechnologie en samenhangende beveiligingsrisico's. Daar valt ook onder verouderde componenten die niet meer leverbaar zijn of niet meer ondersteund worden.

Overige informatie
De eisen uit deze paragraaf betreffen de toeleveringsketen van informatie- en communicatietechnologie (in de vorm van producten én diensten, dus bijvoorbeeld ook cloud technologie). Specifiek hiervoor zijn dus aanvullende eisen gesteld, die geen van de eerdere eisen vervangen. Zoals alle eisen dient de omvang van aanvullende eisen gebaseerd te zijn op het daarmee gepaarde risico en de kosten van beheersing hiervan. Voor veel bedrijven zal de mate van invloed op de toeleveringsketen beperkt zijn. Mede om deze reden is het verstandig om de keuze van de directe leverancier goed te maken en een leverancier te gebruiken die goed samenwerkt en op de hoogte is van ontwikkelingen van (kwetsbaarheden) in de toeleveringsketens.

15.2 Beheer van de dienstverlening door een derde partij

Doel: Geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

De organisatie behoort de implementatie van overeenkomsten te controleren, naleving van de overeenkomsten te bewaken en wijzigingen te beheren om te waarborgen dat de geleverde diensten aan alle eisen voldoen die met de derde partij zijn overeengekomen

15.2.1 Controle en beoordeling van dienstverlening door een derde partij

Beheersmaatregel
De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld.

Implementatierichtlijnen
Controle en beoordeling van dienstverlening door derden behoort te waarborgen dat de voorwaarden van de overeenkomsten voor de informatiebeveiliging worden nageleefd en dat informatiebeveiligingsincidenten en

problemen goed worden afgehandeld. Hiertoe behoort tussen de organisatie en de derde partij een proces voor het beheer van de dienstverlening te bestaan om:

a. de prestatieniveaus van de dienstverlening te controleren op overeenstemming met de overeenkomsten;
b. de dienstverleningsrapportage opgesteld door de derde partij te beoordelen en voor zover nodig volgens de overeenkomsten, voortgangsoverleg te organiseren;
c. informatie te verstrekken over informatiebeveiligingsincidenten en beoordeling van deze informatie door de derde partij en/of de organisatie, als onderdeel van de overeenkomst;
d. de 'audit trails' van de derde partij en registraties van beveiligingsgebeurtenissen, operationele problemen, weigeringen, opsporen van storingen en onderbrekingen verband houdend met de geleverde dienst te beoordelen;
e. vastgestelde problemen op te lossen en te beheren.

De verantwoordelijkheid voor het onderhouden van de relatie met een derde partij behoort te worden toegewezen aan een daarvoor aangewezen persoon. De organisatie behoort verder te waarborgen dat de derde partij de verantwoordelijkheden toewijst voor het controleren van de naleving en het dwingend uitvoeren van de eisen van de overeenkomsten. Er behoren voldoende technische vaardigheden en middelen beschikbaar te worden gesteld voor het controleren van de naleving van de informatiebeveiligingseisen. Er behoort passende actie te worden ondernomen wanneer er manco's in de dienstverlening worden waargenomen.
De organisatie behoort voldoende beheersing te houden over en zicht te houden op alle beveiligingsaspecten voor gevoelige of kritische informatie of IT voorzieningen, waartoe toegang wordt verkregen of die worden beheerd of verwerkt door een derde partij.

Overige informatie
De organisatie behoort zich in geval van uitbesteding te realiseren dat de uiteindelijke verantwoordelijkheid voor de informatie die door een externe partij wordt verwerkt, bij de organisatie blijft berusten.

15.2.2 Beheer van wijzigingen in dienstverlening door een derde partij

Beheersmaatregel
Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

Implementatierichtlijnen
Het proces voor het beheer van wijzigingen in een dienst verleend door een derde partij behoort rekening te houden met:

a. Implementeren van wijzigingen die door de organisatie worden aangedragen:
   - verbeteringen in de huidige geleverde diensten;
   - ontwikkeling van nieuwe toepassingen en systemen;
   - wijzigingen in of updates van het beleid en de procedures van de organisatie
   - koppelingen met andere toepassingen of systemen;
   - nieuwe beheersmaatregelen voor het oplossen van informatiebeveiligingsincidenten en om de beveiliging te verbeteren;
b. implementeren van wijzigingen in de diensten van een derde partij:
   - gebruik van nieuwe technologieën of werkwijzen;
   - aanvaarding van nieuwe producten of nieuwere versies/uitgaven;
   - nieuwe ontwikkelingstools en omgevingen;
   - wijzigingen van de fysieke locatie van dienstvoorzieningen;

- wijziging van achterliggende hosting organisatie en bijbehorende infrastructuur en onderliggende contracten;
- wijziging van leveranciers.

16 CONTROLE OP- EN NALEVING VAN HET SYSTEEM VAN INFORMATIEBEVEILIGING

16.1 Beheer van informatiebeveiligingsincidenten en –verbeteringen

Doel: Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

Er behoren verantwoordelijkheden en procedures te zijn voor het doeltreffend behandelen van informatiebeveiligingsgebeurtenissen en zwakke plekken, zodra ze zijn gerapporteerd. Er behoort een proces van continue verbetering te worden toegepast op het reageren op, controleren, beoordelen en beheer van informatiebeveiligingsincidenten.

16.1.1 Verantwoordelijkheden en procedures

Beheersmaatregel
Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

Implementatierichtlijnen
Naast het rapporteren van informatiebeveiligingsgebeurtenissen en zwakke plekken behoort controle van systemen, waarschuwingen en kwetsbaarheden te worden gebruikt voor het ontdekken van informatiebeveiligingsincidenten. Voor procedures voor het beheer van informatiebeveiligingsincidenten behoren de volgende richtlijnen te worden overwogen:

a. er behoren procedures te worden vastgesteld voor verschillende typen informatiebeveiligingsincidenten, waaronder storingen van informatiesystemen en misbruik van informatiesystemen;
b. naast de gebruikelijke continuïteitsplannen behoren de procedures ook de volgende aspecten te omvatten:
   - analyse en identificatie van de oorzaak van het incident;
   - inperking;
   - zo nodig planning en implementatie van corrigerende maatregelen om herhaling te voorkomen;
   - communicatie met degenen die worden getroffen door of zijn betrokken bij het herstel van het incident;
   - rapporteren van de genomen maatregelen aan de desbetreffende autoriteit;
c. ‘audit trails’ en soortgelijk bewijsmateriaal behoort te worden verzameld en veilig te worden opgeslagen zodat ze geschikt zijn voor probleemanalyse;
d. Het toepassen van corrigerende maatregelen en herstelmaatregelen.

16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen

Beheersmaatregel
Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Implementatierichtlijnen
Er behoort een formele procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen te worden vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een informatiebeveiligingsgebeurtenis. Informatiebeveiligingsincidenten zijn informatiebeveiligings-gebeurtenissen die (aanzienlijke) negatieve gevolgen hebben voor de organisatie. Er behoort een contactpersoon te worden aangewezen waaraan informatiebeveiligingsgebeurtenissen worden gerapporteerd. Alle werknemers, ingehuurd personeel en externe gebruikers behoren op de hoogte te worden gebracht van hun verantwoordelijkheid om elk informatiebeveiligingsgebeurtenis zo snel mogelijk te melden. Ze behoren tevens op de hoogte te zijn van de procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen en van de contactpersoon. In de rapportageprocedures behoren te zijn opgenomen:

a. geschikte feedbackprocessen om te waarborgen dat degenen die een informatiebeveiligingsgebeurtenis rapporteren ook worden geïnformeerd over de resultaten nadat de kwestie is afgehandeld;
b. instructies voor het rapporteren van een informatiebeveiligingsgebeurtenis om het rapporteren te ondersteunen en om degene die rapporteert te helpen herinneren aan alle noodzakelijke handelingen in het geval van een informatiebeveiligingsgebeurtenis;
c. het juiste gedrag in het geval van een informatiebeveiligingsincident, d.w.z.
   - onmiddellijk noteren van alle belangrijke details (bijvoorbeeld soort niet-naleving of beveiligingslek, optredende storing, schermboodschappen, vreemd gedrag);
   - zelf geen enkele actie ondernemen, maar onmiddellijk rapporteren aan de contactpersoon;
d. verwijzing naar een vastgesteld formeel disciplinair proces voor het omgaan met werknemers, ingehuurd personeel of externe gebruikers die de beveiliging doorbreken.

Voorbeelden van informatiebeveiligingsgebeurtenissen en -incidenten zijn: verlies van dienst, apparatuur of voorzieningen, systeemstoringen, menselijke fouten of storingen aan apparatuur.

16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Beheersmaatregel
Personen (medewerkers, contractanten en waar mogelijk gebruikers) die gebruik maken van informatiesystemen en –diensten van de organisatie moeten geobserveerde of vermeende zwakke plekken in de beveiliging registreren en rapporteren. Hiertoe moet de organisatie de juiste eis opstellen en definiëren.

Implementatierichtlijn
Bij het melden van (vermeende) zwakke plekken is de snelheid van reactie van primair belang. De methode van melden moet dus eenvoudig en goed toegankelijk zijn.

Overige informatie
Wanneer personen een zwakke plek vermoeden, is het een vaak voorkomende reactie om te testen of zwakheid daadwerkelijk bestaat. Medewerkers en contractanten moeten geïnformeerd worden dit niet te doen, omdat deze pogingen kunnen worden gezien en uitgelegd als potentieel misbruik of poging tot verwerving van ongeoorloofde toegang. Hierdoor kan schade ontstaan aan het systeem en kan er wettelijke aansprakelijkheid ontstaan.

16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Beheersmaatregel
Voorvallen (informatiebeveiligingsgebeurtenissen) moeten worden beoordeeld, hieruit moet volgen of gebeurtenissen worden geclassificeerd als incidenten.

Implementatierichtlijn
De ontvanger van meldingen dient elke melding of anderszins zichtbaar geworden gebeurtenis te beoordelen op basis van een vastgesteld classificatieschema voor gebeurtenissen en incidenten (binnen het aandachtsgebied van informatiebeveiliging) en op basis hiervan de gebeurtenis al dan niet te classificeren als incident. Deze classificatie geeft daarmee ook een prioriteit weer die de gevolgen van een incident duidelijk maakt (/helpt maken).
De ontvanger van meldingen kan eventueel beschikken over een incidententeam (ook wel response team of ISIRT) en gebeurtenissen en/of incidenten direct naar hen doorsturen of ter latere evaluatie.
De resultaten van de beoordeling dienen te worden vastgelegd voor latere analyse of verificatie.

16.1.5 Respons op informatiebeveiligingsincidenten

Beheersmaatregel
Op elke informatiebeveiligingsincident moet conform gedocumenteerde procedures worden gereageerd.

Implementatierichtlijn
De persoon of personen die moeten reageren op incidenten moeten aangewezen zijn, al dan niet ondersteund door externen (zie 16.1.1). Bij die respons hoort:

a. zo snel mogelijk bewijs verzamelen;
b. forensische analyse van de informatiebeveiliging waar nodig (zie 16.1.7);
c. escaleren wanneer nodig;
d. vastleggen van de responsactiviteiten voor latere analyse;
e. het bestaan van het informatiebeveiligingsincident of relevante details daarvan communiceren aan
f. personen of organisatie met een ‘need to know’.
g. het eventuele toepassen van tijdelijke noodmaatregelen om verdere schade van de incident te beperken
h. corrigeren van de zwakke plek(ken) in de informatiebeveiliging waarvan bleek dat deze oorzaak waren van het incident of er aan bijdroegen.
i. formele afsluiting van het incident en verslaglegging zodra het incident succesvol is behandeld.

Om de bron van het incident te identificeren dient analyse na het incident plaats te vinden.

16.1.6 Leren van informatiebeveiligingsincidenten

Beheersmaatregel
Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

Implementatierichtlijnen
De informatie verkregen uit het beoordelen van informatiebeveiligingsincidenten behoort te worden gearchiveerd en gebruikt om terugkerende incidenten te identificeren en adequaat aan te pakken.

16.1.7 Verzamelen van bewijsmateriaal

Beheersmaatregel
Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel, arbeidsrechtelijk of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Implementatierichtlijnen
Er behoren interne procedures te worden ontwikkeld en gevolgd bij het verzamelen en presenteren van bewijsmateriaal ten behoeve van disciplinaire maatregelen die binnen een organisatie worden afgehandeld:

In het algemeen hebben deze regels voor bewijsmateriaal betrekking op:
a. de toelaatbaarheid van het bewijs;
b. het gewicht van het bewijsmateriaal: de kwaliteit en volledigheid van het bewijsmateriaal;

Om te bereiken dat bewijsmateriaal wordt toegelaten, behoren organisaties te waarborgen dat hun informatiesystemen in overeenstemming zijn met praktijkcodes voor het genereren van toelaatbaar bewijsmateriaal.

17 INFORMATIEBEVEILIGINGSASPECTEN VAN BEDRIJFCONTINUITEITSBEHEER

17.1 Continuïteit van Informatiebeveiliging

Doel: Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen en om tijdig herstel te bewerkstelligen, door informatiebeveiliging op te nemen in het algemene kader van bedrijfscontinuïteit van de organisatie.

17.1.1 Plannen van informatiebeveiligingscontinuiteit

Beheersmaatregel
De organisatie moet de eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer tijdens ongunstige situaties vaststellen.

Implementatierichtlijn
Een organisatie moet bepalen of en hoe de continuïteit van de informatiebeveiliging onder het beheerproces van de bedrijfscontinuïteit valt of onder het beheerproces van rampenherstel (noodplannen).

Informatiebeveiligingseisen behoren te worden vastgesteld als de planning voor bedrijfscontinuïteit en rampenherstel wordt gemaakt, of deze planning dient met deze aanvullende eisen aangepast te worden.

Als er geen formele planning voor bedrijfscontinuïteit en/of rampenherstel (noodplan) is moet het informatiebeveiligingsbeheer ervan uitgaan dat de informatiebeveiligingseisen hetzelfde blijven als bij normale omstandigheden. Eventueel kan een organisatie een impactanalyse uitvoeren voor informatiebeveiligingsaspecten om de informatiebeveiligingseisen vast te stellen die van toepassing zijn op ongunstige situaties.

Overige informatie
Het wordt aanbevolen om informatiebeveiliging mee te nemen in de normale evaluatie en impactanalyse van het bedrijfscontinuïteitsbeheer of van het rampenherstelbeheer (noodplan).

17.1.2 Continuïteitsplannen ontwikkelen en implementeren

Beheersmaatregel
Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

Implementatierichtlijnen
Het proces van continuïteitsplanning behoort de volgende punten te omvatten:
a. identificatie van en instemmen met alle verantwoordelijkheden en procedures voor bedrijfscontinuïteit;
b. identificatie van aanvaardbaar verlies van informatie en diensten;

c. implementatie van procedures om herstel en reconstructie van bedrijfsprocessen en beschikbaarheid van informatie mogelijk te maken binnen de vereiste tijdspanne; er behoort in het bijzonder aandacht te worden besteed aan de beoordeling van interne en externe afhankelijkheden en lopende contracten en de mogelijkheid de dienstverlening zoveel mogelijk door te laten lopen;
d. operationele procedures die volgen op het afronden van herstel en reconstructie;
e. documentatie van overeengekomen procedures en processen;
f. geschikte opleiding van personeel in de overeengekomen procedures en processen, waaronder crisisbeheer;
g. testen en updaten van de plannen.

17.1.3 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

Beleidsmaatregel
Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdatet, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

Implementatierichtlijnen
Bedrijfscontinuïteitsplannen behoren te waarborgen dat alle leden van het herstelteam en andere betrokken medewerkers op de hoogte zijn van de plannen en van hun verantwoordelijkheid voor bedrijfscontinuïteit en informatiebeveiliging en hun rol kennen wanneer een plan in werking wordt gesteld.
In het testschema voor het (de) bedrijfscontinuïteitsplan(nen) behoort te worden aangegeven hoe en wanneer elk onderdeel van het(de) continuïteitsplan(nen) wordt getest. Elk onderdeel van de plannen behoort regelmatig te worden getest.
Er kunnen verschillende technieken behoren te worden gebruikt om er zeker van te zijn dat het (de) plan(nen) daadwerkelijk functioneren. Dit behoort te omvatten bijvoorbeeld:
a. gezamenlijk doorlopen van diverse scenario's (bespreking van de bedrijfsherstelprocedures aan de hand van voorbeelden van onderbrekingen);
b. simulaties (in het bijzonder om mensen te trainen in hun rol na een incident en bij crisisbeheer);
c. testen van technische herstelprocedures (om te waarborgen dat informatiesystemen doeltreffend kunnen worden hersteld);
d. testen van herstel op een andere locatie (waarbij bedrijfsprocessen parallel aan hersteloperaties worden uitgevoerd, op een andere plaats dan de hoofdlocatie);
e. testen van voorzieningen en diensten van leveranciers (om te waarborgen dat externe diensten en producten in overeenstemming zijn met contractuele verplichtingen);
f. realistische oefeningen (waarbij wordt getoetst dat organisatie, personeel, apparatuur, voorzieningen en processen bestand zijn tegen onderbrekingen).

Deze technieken kunnen door elke organisatie worden gebruikt. Ze behoren te worden toegepast op een manier die past bij het specifieke herstelplan. De testresultaten behoren te worden vastgelegd, en handelingen om waar nodig de plannen te verbeteren behoren te worden uitgevoerd.
Er behoren verantwoordelijkheden te worden toegewezen voor regelmatige beoordeling van elk bedrijfscontinuïteitsplan. Het vaststellen van veranderingen in de werkwijze van de organisatie die nog niet hun neerslag hebben gevonden in de bedrijfscontinuïteitsplannen, behoort te worden gevolgd door een adequate update van het desbetreffende plan. Dit formele proces van wijzigingenbeheer behoort te waarborgen dat de geüpdatet plannen worden verspreid en bekrachtigd door regelmatige beoordeling van het plan als geheel.

17.2 Redundante componenten

Doel: Zorgen voor voldoende beschikbaarheid van informatieverwerkende faciliteiten.

17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten

Beheersmaatregel
Informatieverwerkende faciliteiten moeten voldoende redundant (meervoudig uitgevoerd) zijn zodat ze aan de beschikbaarheidseisen voldoen.

Implementatierichtlijn
Organisaties moeten de eisen voor beschikbaarheid van informatiesystemen vast te stellen. Als de beschikbaarheid niet voldoende kan worden gegarandeerd door de bestaande systeemarchitectuur moeten redundante componenten of architecturen in overweging te worden genomen. Voor extern geleverde systemen is deze beschikbaarheidseis vastgelegd in overeenkomsten met de leverancier (zie hoofdstuk 15).

Voor redundante toepassingen die niet simultaan operationeel zijn (load balanced) moet worden getest dat overschakeling van een component naar een andere daadwerkelijk werkt wanneer deze noodzakelijk is.

Overige informatie
Door de introductie van redundante componenten kunnen er nieuwe risico's voor de integriteit of vertrouwelijkheid ontstaan. Hier moet bij het ontwerpen van het systeem of introduceren van deze componenten rekening worden gehouden.

18 NALEVING

18.1 Naleving van wettelijke voorschriften

Doel: Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

18.1.1 Identificatie van toepasselijke wetgeving

Beheersmaatregel
De relevante wettelijke en regelgevende eisen en contractuele verplichtingen van de organisatie moeten expliciet worden vastgesteld, samen met de wijze waarop de organisatie aan deze wijze voldoet. Dit moet worden gedocumenteerd en actueel gehouden voor elk informatiesysteem en voor de organisatie.

Implementatierichtlijnen
De specifieke beheersmaatregelen en individuele verantwoordelijkheden om aan deze eisen te voldoen, behoren eveneens te worden gedefinieerd en gedocumenteerd. Bijzondere aandacht vereist de omgang met adressenbestanden, o.a. voor direct mail acties, op basis van de Wet Bescherming Persoonsgegevens. Voor het gebruik en de verwerking van adresdata zijn richtlijnen beschikbaar. Voor Nederland kan daarover contact worden gelegd met de sectororganisatie(s) KVGO en/of DDMA (zie www.ddma.nl). Ook de wetten betreffende intellectueel eigendom (auteurswet, handelsnamenrecht en merkenrecht) hebben gevolgen voor bedrijven.

18.1.2 Intellectuele eigendomsrechten

Beheersmaatregel
Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.

Implementatierichtlijnen
De volgende richtlijnen behoren te worden overwogen om materiaal te beschermen dat als intellectueel eigendom kan worden beschouwd:

a. het intern formuleren van beleid ten aanzien van de naleving van intellectuele eigendomsrechten, waarin wettig gebruik van programmatuur, informatieproducten en beeld, tekst en video materiaal waar rechten op berusten wordt gedefinieerd;
b. programmatuur alleen aanschaffen via bekende en erkende leveranciers om te waarborgen dat geen auteursrechten worden geschonden;
c. het verwijderen van het intern opgeslagen fysieke of digitaal materiaal waarop rechten berust nadat de productie is afgerond en/of het retour zenden van het materiaal aan de klant of rechthebbende toeleverancier;
d. in stand houden van het bewustzijn van het beleid voor bescherming van intellectuele eigendomsrechten, evenals van het voornemen om disciplinaire maatregelen te treffen tegen personeel dat dit beleid schendt;
e. bijhouden van relevante registers van bedrijfsmiddelen en het identificeren van alle bedrijfsmiddelen met eisen ten aanzien van het beschermen van intellectuele eigendomsrechten. Het beheer van rechten kan worden vastgelegd in een digital asset management systeem;
f. het bewaren en onderhouden van bewijzen en bewijsmateriaal waaruit blijkt over welke licenties, originele diskettes of schijven, handboeken enz. de organisatie beschikt;
g. het registreren van rechten op fysiek of digitaal materiaal die voor productie wordt gebruikt. Dit kan het best geregeld worden in een Digital Asset Management systeem.
h. controleren dat alleen geautoriseerde programmatuur en producten met licenties zijn geïnstalleerd;
i. vaststellen van beleid voor het verwijderen van programmatuur of het overdragen ervan aan anderen;
j. vaststellen van het beleid voor het beheren en verwijderen van fysiek of digitaal materiaal waar rechten van derden op berusten;
k. gebruik van geschikte audit-hulpmiddelen;
l. voldoen aan bepalingen en voorwaarden voor programmatuur en informatie die zijn verkregen via openbare netwerken;
m. niet dupliceren, converteren naar een ander formaat of extraheren van commerciële opnamen (film, audio), tenzij dit auteursrechtelijk is toegestaan;
n. niet volledig of gedeeltelijk kopiëren van boeken, artikelen, rapporten of andere documenten, tenzij dit auteursrechtelijk is toegestaan. Let op dat ook publiceren in het kader van persberichten er auteursrechten van toepassing zijn.

18.1.3 Bescherming van bedrijfsdocumenten en registraties

Beheersmaatregel
Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

Implementatierichtlijnen
Registraties behoren te worden gecategoriseerd naar type registraties. Bij elk type behoort de bewaartermijn en het type opslagmedium te worden vermeld, bijvoorbeeld papier, magnetische of optische opslag. Cryptografische sleutels of programmatuur die verband houden met versleutelde archieven of digitale handtekeningen behoren ook te worden bewaard om ontcijfering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties.
Er behoort rekening te worden gehouden met de mogelijkheid dat media die voor opslag van records worden gebruikt in kwaliteit achteruit gaan. Procedures voor opslag en behandeling van deze media behoren in overeenstemming met de aanbevelingen van de fabrikant te worden geïmplementeerd.

Waar elektronische opslagmedia worden gekozen, behoren procedures te worden vastgesteld om te waarborgen dat de informatie gedurende de gehele bewaarperiode toegankelijk blijft (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 kunnen worden opgevraagd binnen een aanvaardbare tijdspanne en in een aanvaardbaar formaat, afhankelijk van de eisen waaraan moet worden voldaan.
Het systeem waarmee gegevens worden opgeslagen en behandeld, behoort een duidelijke identificatie van registraties en waar van toepassing, van hun bewaartermijn te waarborgen, waar van toepassing in overeenstemming met nationale of regionale wet- of regelgeving. De registraties behoren na afloop van die termijn, als de organisatie ze niet meer nodig heeft, op geschikte wijze te kunnen worden vernietigd.
Om aan de verplichtingen van het veiligstellen van records te voldoen, behoren binnen een organisatie de volgende stappen te worden ondernomen:

a. er behoren richtlijnen te worden vastgesteld voor het bewaren, opslaan, behandelen en verwijderen van records en informatie;
b. er behoort een bewaarschema te worden opgesteld waarin registraties zijn vastgelegd, evenals de periode gedurende welke ze behoren te worden bewaard;
c. er behoort een inventarislijst te worden bijgehouden van de belangrijkste informatiebronnen;
d. er behoren geschikte beheersmaatregelen te worden geïmplementeerd om registraties en informatie te beschermen tegen verlies, vernietiging en vervalsing.

18.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

Beheersmaatregel
De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

Implementatierichtlijnen
Er behoort door de organisatie een beleid voor bescherming van persoonsgegevens te worden ontwikkeld en ingevoerd. Dit beleid behoort te worden gecommuniceerd naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens.
Naleving van dit beleid en alle relevante wetgeving voor gegevensbescherming en regelgeving vereist een geschikte structuur voor beheer en beveiliging. Vaak kan dit het beste worden bereikt door een verantwoordelijke aan te wijzen, zoals een functionaris die belast is met de bescherming van gegevens die ondersteuning behoort te bieden aan managers, gebruikers en dienstverlenende bedrijven met betrekking tot hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Het toewijzen van verantwoordelijkheid voor het verwerken van persoonlijke informatie en het waarborgen dat medewerkers zich bewust zijn van de uitgangpunten van bescherming van gegevens behoort te worden uitgevoerd in overeenstemming met de relevante wet- en regelgeving. Er behoren passende technische en organisatorische maatregelen te worden geïmplementeerd om persoonsgegevens te beschermen.

Overige informatie
De Nederlandse overheid heeft beleidsrichtlijnen en –regels opgesteld voor zowel de Wet Bescherming Persoonsgegevens en (daarbinnen) het melden van datalekken. Deze dienen gevolgd te worden voor de bescherming van persoonsgegevens door het bedrijf.

18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel
Cryptografische beheersmaatregelen moeten alleen worden toegepast conform alle relevante overeenkomsten, wet- en regelgeving.

Implementatierichtlijn
Voor de naleving van relevante overeenkomsten, wet- en regelgeving moet rekening gehouden worden met:
a. eventuele import- of exportbeperkingen van hardware en -software voor cryptografie;
b. eventuele import- of exportbeperkingen van hardware en -software waar cryptografische functies aan kunnen worden toegevoegd;
c. beperkingen die geplaatst zijn op het gebruik van versleuteling;
d. het eventuele recht van nationale autoriteiten van toegang tot (door hardware of software versleutelde) informatie om in de vertrouwelijkheid van de inhoud te voorzien.

De relevante wet- en regelgeving en de naleving ervan zijn specialistische onderwerpen waarover juridisch advies ingewonnen moet worden. Ditzelfde geld voordat versleutelde informatie of cryptografische technieken over grenzen van rechtsgebieden worden verstuurd.

18.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doel: Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.
De beveiliging van informatiesystemen behoort regelmatig te worden beoordeeld.
Dergelijke beoordelingen behoren te worden uitgevoerd op basis van het desbetreffende beveiligingsbeleid en technische platforms en informatiesystemen behoren te worden beoordeeld op naleving van toepasselijke normen voor de implementatie van de beveiliging en gedocumenteerde beveiligingsmaatregelen.

18.2.1 Onafhankelijke beoordeling van informatiebeveiliging

Beheersmaatregel
Periodiek én bij belangrijke veranderingen moet de aanpak van informatiebeveiliging onafhankelijk worden beoordeeld.

Implementatierichtlijn
De onafhankelijke beoordeling moet op initiatief van de directie plaatsvinden en de directie moet over de uitkomsten geïnformeerd worden. De onafhankelijke beoordeling is nodig omdat in de praktijk blijkt dat deze noodzakelijk is om te borgen dat de organisatie continue een goede aanpak van informatiebeveiliging en haar beheer hanteert. In deze beoordeling moeten ook de verbetermogelijkheden en eventuele noodzaak om wijzigingen aan te brengen beschouwd worden, inclusief beleid en haar doelstellingen.
De beoordeling moet gedaan worden door personen die onafhankelijk kunnen werken. Voorbeelden zijn een interne auditor (of auditteam), een persoon uit een andere vestiging of een gespecialiseerde externe organisatie. De personen die deze audit uitvoeren moeten hiervoor bekwaam zijn: opleiding van hen op dit punt is daardoor wellicht noodzakelijk. De resultaten van de beoordeling (audit) moeten worden vastgelegd, gerapporteerd en bewaard.

Als uit deze beoordeling blijkt dat er tekortkomingen zijn, dan dient de directie tegenmaatregelen te initiëren en bewaken.

18.2.2 Naleving van beveiligingsbeleid en -normen

Beheersmaatregel
Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

Implementatierichtlijnen
Managers behoren regelmatig te beoordelen of de informatieverwerking binnen hun verantwoordelijkheidsgebied voldoet aan het geldende beveiligingsbeleid, normen en andere beveiligingseisen.
Indien als resultaat van de beoordeling een geval van niet-naleving wordt ontdekt behoren managers:

a. de oorzaken van deze niet-naleving vast te stellen:
b. de noodzaak voor handelen te beoordelen om te waarborgen dat niet-naleving zich niet opnieuw voordoet;
c. passende corrigerende maatregelen vast te stellen en te implementeren;
d. de uitgevoerde correctieve maatregel beoordelen.

De resultaten van de beoordelingen en de corrigerende handelingen die door managers zijn uitgevoerd, behoren te worden geregistreerd en deze registraties behoren te worden bewaard. De managers behoren wanneer de onafhankelijke beoordeling plaatsvindt in hun verantwoordelijkheidsgebied de resultaten te rapporteren aan de personen die de onafhankelijke beoordelingen uitvoeren.

18.2.3 Controle op technische naleving

Beheersmaatregel
Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

Implementatierichtlijnen
Controle op naleving van technische normen behoort of handmatig door een ervaren systeemtechnicus en/of beveiligingsspecialist te worden uitgevoerd. Het werkgebied systeembeheer kent natuurlijk beveiligingsaspecten maar gaat uit van andere gezichtspunten dan het specialisme beveiliging. Een specialist kan en zal gebruik maken van (geautomatiseerde) tools en sociale hacktechnieken met als doelstelling het systeem te penetreren. Om deze reden dient de organisatie periodiek te overwegen welke mate van testen, zoals een pentest, ze laat uitvoeren.

Bij het uitvoeren van dergelijke tests dient zorgvuldigheid toegepast te worden omdat deze testen het systeem kunnen beschadigen, compromitteren of minder effectief kunnen maken. Dergelijke tests moeten worden gepland en gedocumenteerd en kunnen een risicobeoordeling niet vervangen.