BASELINE

INFORMATIEBEVEILIGING

(WONING)CORPORATIES

BASELINE INFORMATIEBEVEILIGING CORPORATIES

Versie 3.0 (2019)

De Baseline Informatiebeveiliging (woning)Corporaties (BIC) is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. Met klem wordt hier vermeld dat de BIC deze normen niet vervangt.

De Baseline Informatiebeveiliging (woning)Corporaties (BIC) is een toepassingshandleiding voor NEN/ISO 27001 en 27002 voor woningcorporaties. De BIC beschrijft ook de aanvullingen op NEN/ISO27001 en 27002 voor de woningcorporaties. In deze baseline zijn die aanvullingen gemerkt met een [A] van aanvullend.

NEN/ISO 27001 en 27002 beschrijven details voor implementatie, zogenaamde implementatierichtlijnen, en eisen voor wat betreft de procesinrichting (o.a. het ISMS uit NEN/ISO 27001). Die documenten geven dus de details voor toepassing en kunnen naast de BIC gebruikt worden.

Deze Baseline is gemaakt door de Special Interest Group Informatiebeveiliging (kortweg aangeduid als SIG-BIC) van CorpoNet, een vereniging van en voor functionarissen verantwoordelijk voor het beleid gericht op Informatiemanagement en ICT van woningcorporaties en bevat de basis set aan beveiligingsmaatregelen die nodig zijn als stabiele en veilige basis voor een woningcorporatie.

Met dank aan de SIG-BIC, aan versie 3.0 (2019) werkten mee:

Joop Schoppers, De Woonplaats
Leen Spaans, Woonforte
Benno Boeijink, Haag Wonen
Rino Kalker, Volkshuisvesting Arnhem
José van Wandelen, Arcade mensen en wonen
Tom Jurgens, Eigen Haard
Maria Petrarca, Havensteder

Aan eerdere versie(s) werkten mee:

Birgitta Schutter, Haag Wonen
Edmond Janssen, Woonwenz
Aletta Hoogeveen, Parteon

En met dank voor de ondersteuning aan de consultants/eindredactie van B-able:

Hilko Batterink

en aan eerdere versie(s) Mohamed Fahmy

Gerelateerde documenten

Titel	Auteur	Jaartal	Omschrijving
NEN-ISO/IEC-27001/27002:2013 NL	NEN	2013-2015	De code voor informatiebeveiliging
AVG	EU	2016	Algemene Verordening Gegevensbescherming (EU/2016/679)
Beleidsregels Meldplicht Datalekken	Autoriteit Persoonsgegevens (voorheen CBP)	2015	Beleidsregels behorende bij artikel 32 t/m 34, AVG
BIR familie	Min. van BZK	2017	Baseline Informatiebeveiliging Rijksdienst
BIG familie	VNG	2013	Baseline Informatiebeveiliging Gemeenten
BIA	ISF	2007	Business Impact Analyse
CORA	Vereniging CorpoNet		COrporatie Referentie Architectuur (CORA)
VERA	Stichting VERA		Volkshuisvesting Enterprise Referentie Architectuur (VERA)

Managementsamenvatting

De Baseline Informatiebeveiliging (woning)Corporaties is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van woningcorporatie informatie-(systemen) bevordert. Deze Baseline is een richtlijn die een totaalpakket aan informatiebeveiligingsrichtlijnen en -maatregelen omvat die voor iedere woningcorporatie geldt.

Deze Baseline is opgezet rondom bestaande normen; de NEN/ISO 27001:2013 en NEN/ISO 27002:2013. Deze standaard is door de Nederlandse (semi-)Overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Voor specifieke maatregelen is in onderhavige Baseline ook gebruik gemaakt van de AVG, en andere voor de sector relevante normenkaders en regelingen.

Achtergrond

Door de toenemende digitalisering is het zorgvuldig omgaan met informatie en gegevens van huurders en organisaties ook voor woningcorporaties van groot belang. Uitval van computers of telecommunicatiesystemen, het gecorrumpeerd raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van woningcorporaties. Hieraan zijn bestuurlijke consequenties verbonden en het kan het imago van de woningcorporatie en daarmee van de sector in het algemeen schaden.

Onderzoek van TNO geeft aan dat cybercrime de Nederlandse economie jaarlijks ongeveer €10 miljard kost. Deze raming betekent dat de schade door cybercrime voor de woningcorporaties naar verwachting ook significant is.

De beveiligingsincidenten gaan over meer dan geld alleen. Woningcorporaties beheren ook veel persoonsgegevens. Het waarborgen van de privacy en vertrouwelijkheid van informatie is essentieel.
De belangrijkste les uit eerder voorgevallen incidenten is dan ook dat er behoefte is aan een richtlijn voor (de inrichting van) informatieveiligheid bij woningcorporaties.

Opdracht

CorpoNet heeft opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging (woning)Corporaties. De Baseline Informatiebeveiliging (woning)Corporaties is bedoeld om:

1. Woningcorporaties op een vergelijkbare manier efficiënt te laten werken aan (de inrichting van) hun informatiebeveiliging.
2. Woningcorporaties een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
3. De auditlast bij woningcorporaties te verminderen.
4. Woningcorporaties een aantoonbaar betrouwbare partner te laten zijn.

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de bedrijfsprocessen bij woningcorporaties. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, het is bittere noodzaak geworden.

De Baseline beschrijft de basis normen en maatregelen ten behoeve van controle en risicomanagement. Deze Baseline beschrijft deze aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2013. De in dit document opgenomen beheersmaatregelen gelden als Baseline (basis dus) voor de woningcorporatie sector.

Versies

Versie 1.0 kwam tot stand in 2016 op basis van de toen meest actuele bestaande normen NEN/ISO 27001:2013 en NEN/ISO 27002:2013.

In 2017 werd deze versie opgevolgd door een versie 2.0 waarin hoofdstuk 3 en 4 zijn herschreven en de basis van Risico Management alsmede het belang van organisatorische borging middels een ISMS (Management Systeem) is toegevoegd.

Versie 3.0 is afgerond in 2018 en verscheen in 2019, met als belangrijkste motief voor deze update de inmiddels actueel geworden Privacy wetgeving, de Algemene Verordening Gegevensbescherming (EU/2016/679) die van kracht werd per 25 mei 2018.

Leeswijzer

Structuur

De indeling van dit document is als volgt:

1. Het algemene deel over de Baseline, uitleg, relaties met architectuur frameworks, hoe met deze Baseline kan worden omgegaan etc.

Hoofdstuk 1 tot en met 4

2. Een Baseline met de basis set aan maatregelen die voor alle woningcorporaties geldt.

Hoofdstuk 5 tot en met 18

3. Een bijlage met een verklaring van begrippen.

Doelgroepen

Deze Baseline bevat aandachtsgebieden voor verschillende functionarissen binnen de doelgroep woningcorporaties. Hieronder worden per functionaris de hoofdstukken genoemd die relevant zijn.

IB functionarissen (Dat wil zeggen, Informatiebeveiligingsfunctionarissen van alle niveaus[1])
Alle hoofdstukken

Managers in hun personeelsverantwoordelijkheid
Hoofdstukken 6 en 7
De manager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken.

Managers in hun verantwoordelijkheid voor de uitvoering van de processen
Hoofdstukken 6, 12, 16 en 17
De manager is verantwoordelijk voor het uitvoeren van activiteiten in processen (algemene procesverantwoordelijkheid) op basis van de beschreven inrichting ervan. De verantwoordelijkheid voor de naleving van specifieke beveiligingsaspecten hangt af van het soort proces.

Beleidsmakers
Hoofdstukken 4, 5, 6, 12 en 17
De beleidsmaker is verantwoordelijk voor het ontwikkelen van een veilig en werkbaar beleid. Het beleid moet goed uitvoerbaar en controleerbaar zijn.

Personeelszaken

[1] Afhankelijk van de grootte van de woningcorporatie zijn er meer of minder beveiligingsfunctionarissen. Voor dit document speelt dat geen rol. Samenhang van maatregelen (procedureel, technisch of organisatorisch) is essentieel en om die reden dienen op alle niveaus alle beveiligingsfunctionarissen kennis te nemen van deze Baseline.

Hoofdstuk 7
Personeelszaken is verantwoordelijk voor werving, selectie en algemene zaken rond het functioneren van personeel. Inclusief bewustwording en gedrag.

Fysieke beveiliging
Hoofdstuk 11
Fysieke beveiliging is vaak belegd bij Facility Management of bewakingsdiensten. Zij zijn verantwoordelijk voor de beveiliging van percelen, panden en ruimtes.

ICT-diensten en ICT-infrastructuren
Hoofdstukken 6, 8, 9, 10, 12, 13, 14, 15, 16 en 17
De ICT-diensten en -infrastructuren zijn ondersteunend aan bijna alle processen. De eisen die aan ICT-voorzieningen gesteld worden, zijn hierdoor zeer ingrijpend en bepalen voor een belangrijk deel de inrichting van het ICT-landschap.

Applicatie-eigenaren en systeemeigenaren
Hoofdstukken 8, 9, 10, 12 en 14
Applicatie-eigenaren en systeemeigenaren zijn verantwoordelijk voor de veilige en correcte verwerking van de relevante data binnen de applicatie.
Een belangrijk onderdeel van informatiebeveiliging vormen de eindgebruikers. Zij dienen kennis te hebben van de gevolgen van hun gedrag op beveiliging.

Informatiebeveiligingsadviseurs en ICT-auditors
Alle hoofdstukken
Bij het helpen bepalen welke maatregelen relevant zijn en het controleren of de maatregelen daadwerkelijk genomen zijn, is het doornemen van het hele document relevant.

Externe leveranciers
Alle hoofdstukken
De externe leveranciers zijn een bijzondere doelgroep. De opdrachtgever/ systeemeigenaar is altijd verantwoordelijk voor de kwaliteit en veiligheid van de uitbestede diensten. De opdrachtgever eist van de externe leveranciers dat zij voldoen aan alle aspecten van de Baseline die voor de dienst of het betreffende systeem van belang zijn en betrekking hebben op de geleverde dienst.

INHOUDSOPGAVE

1 Waarom deze Baseline?

1.1 Inleiding

Door de toenemende digitalisering is het zorgvuldig omgaan met de gegevens van huurders voor woningcorporaties van groot belang. Uitval van computer- of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennis nemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en dienstverlening. Hieraan zijn bestuurlijke consequenties verbonden die het imago van de woningcorporatie in het algemeen en van specifieke woningcorporaties in het bijzonder schaden.

Het is niet alleen de automatisering. De samenwerking met (semi-) overheden (in ketens) en de contacten met huurders en bedrijven wordt steeds vaker digitaal van aard. Dit legt (deels nieuwe) eisen op aan de kwaliteit van de informatievoorziening en -beveiliging van de woningcorporatie. Al was het maar dat van digitale dienstverlening vaak verwacht wordt dat deze 24 uur per dag en 7 dagen per week beschikbaar is, en dat bij een calamiteit de dienstverlening weer snel op gang komt.

Daarnaast spelen wet- en regelgeving een belangrijke rol. De AVG en wet Meldplicht Datalekken zijn voorbeelden van wetten die eisen stellen aan de verwerking en opslag van informatie.

Tot slot is er de maatschappelijke verantwoordelijkheid die een woningcorporatie tegenover de huurders en bedrijven heeft. Van een woningcorporatie mag verwacht worden dat zij zorgvuldig omgaat met de gegevens die zij beheert en dat de gegevens die zij levert juist, accuraat, noodzakelijk en tijdig zijn.

Kortom, de structurele aandacht voor de betrouwbaarheid van de informatievoorziening, het domein van informatiebeveiliging, helpt de woningcorporatie bij een goede invulling van haar maatschappelijke taken. Een goede borging van informatiebeveiliging zorgt voor een betere betrouwbaarheid van de informatievoorziening en een hogere continuïteit van de bedrijfsvoering.

CorpoNet heeft opdracht gegeven voor de ontwikkeling van deze Baseline. De totale Baseline Informatiebeveiliging (woning)Corporaties is bedoeld om alle woningcorporaties op een vergelijkbare manier te laten werken met informatiebeveiliging.

Deze Baseline wordt later aangevuld met meerdere sets van voorbeelden voor beleid en operationele procedures.

Deze Baseline Informatiebeveiliging (woning)Corporaties is opgesteld door de Special Interest Group Informatiebeveiliging, waarin deelnemers vanuit diverse woningcorporaties zitting hebben. Daarnaast is de koepelorganisatie Aedes geïnformeerd over deze ontwikkeling.

Deze Baseline kan niet gedeeltelijk worden geïmplementeerd, er bestaat geen stukje informatiebeveiliging. De Baseline is het afgewogen minimale beveiligingsniveau waaraan een woningcorporatie moet willen voldoen. De maatregelen hebben een onderlinge samenhang. Dus indien gekozen wordt voor het invoeren van deze Baseline, dan kan dat alleen zoals deze is, tenzij er goede redenen zijn om hiervan af te wijken.

Hiervoor geldt 'comply or explain' of 'pas toe of leg uit' ten aanzien van de maatregelen in deze Baseline.

1.2 Scope

De scope van deze Baseline omvat de bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de woningcorporatie in de meest brede zin van het woord. Deze Baseline is van toepassing op alle ruimten van de huisvesting van een woningcorporatie en aanverwante gebouwen, alsmede op (mobiele) apparatuur die door woningcorporatie medewerkers gebruikt worden bij de uitoefening van hun taak op diverse locaties. De Baseline heeft betrekking op de informatie die daarbinnen verwerkt wordt. Ook als systemen niet binnen de woningcorporatie draaien is deze Baseline van toepassing.[2]

Binnen de scope van deze Baseline vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging, die door derden aan de woningcorporatie zijn opgelegd. Deze Baseline bevat daarbij behorende relevante maatregelen en brengt ze met elkaar in verband.

Binnen de scope is ook rekening gehouden met de verregaande digitalisering van de woningcorporatie en met de in de toekomst nog volgende digitalisering.

1.3 Randvoorwaarden

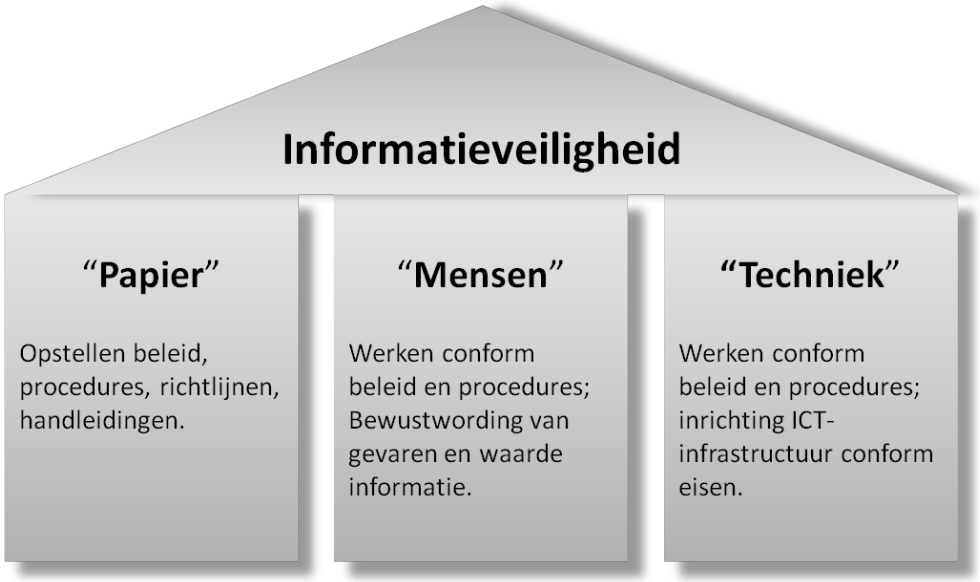
De randvoorwaarden voor de Baseline zijn:

1. Informatiebeveiliging is en blijft een verantwoordelijkheid van het management/de directie.
2. Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement.
3. De klassieke informatiebeveiligingsaanpak, waarbij inperking van mogelijkheden de boventoon voert, maakt plaats voor het zoeken naar een werkbare balans tussen gebruiksgemak en toch veilig werken (lees: veilig faciliteren).
4. De focus van informatiebeveiliging verschuift van netwerkbeveiliging naar gegevensbeveiliging.
5. Bewust en verantwoord gedrag van mensen is essentieel voor een goede informatiebeveiliging.
6. De Baseline wordt woningcorporatie breed afgesproken en wettelijke kaders en maatregelen worden nationaal of Europees afgesproken, waarbij de door de woningcorporatie gekozen brede kaders en maatregelen geënt worden op die wettelijke kaders. In uitzonderingsgevallen wordt – in overleg – afgeweken.
7. Kennis en expertise zijn essentieel voor een toekomst vaste informatiebeveiliging en moeten geborgd worden.
8. Informatiebeveiliging vereist een integrale aanpak, zowel binnen de woningcorporatie zelf als voor eventuele gemeenschappelijke voorzieningen.
9. Deze Baseline is gebaseerd op de ISO 27001:2013 en ISO 27002:2013.
10. Deze Baseline kan gefaseerd worden ingevoerd.

[2] Denk aan een SaaS-oplossing, uitbesteding van taken et cetera.

1.4 Werkingsgebied

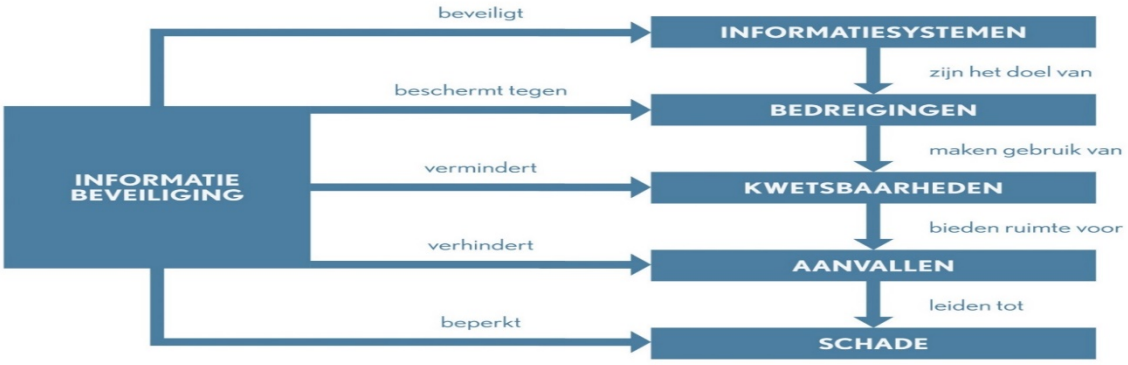
Informatiebeveiliging gaat over meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen,



kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook over mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk policy, hoe om te gaan met mobiele apparaten en aanwijzingen voor telewerken.

1.5 Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van een woningcorporatie. Het verlies van gegevens, uitval van ICT, het door (on)bevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de primaire taakuitvoering en/of de bedrijfsvoering en kan leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor huurders, leveranciers, partners en de eigen organisatie en haar bestuurders. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.



In deze Baseline zijn de laatste uitgangspunten van de woningcorporaties, voor zover dat mogelijk is, gegeven de huidige stand van de techniek, verwerkt.

Open standaarden

Er is gekozen voor een optimale aansluiting bij de wereld van geaccepteerde standaarden, ISO 27001:2013 en ISO 27002:2013. Indien een organisatieonderdeel of een toeleverancier haar zaken op orde heeft volgens ISO 27001:2013, rekening houdend met de implementatiemaatregelen uit ISO 27002:2013, dan hoeft die organisatie slechts te controleren op de aanvullende bepalingen.

1.6 Wetten en regels

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de AVG. Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De AVG stelt dat organisaties maatregelen moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen (art.32 AVG). Voor wat betreft de woningcorporatie is uitgegaan van verwerken van persoonsgegevens, conform beschreven in de AVG. Er zijn veel wetten en regelgeving van toepassing op de woningcorporatie. De woningcorporatie, als toegelaten instelling, dient zich aan al deze wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging. Wetten en regelingen die van toepassing zijn (niet limitatief):

- Algemene Verordening Gegevensbescherming (AVG)
- Wet Openbaarheid van Bestuur (WOB), art.1a
- Woningwet
- Wet Computercriminaliteit II
- Telecommunicatiewet, art. 11
- Auteurswet
- Besluit Beheer Sociale Huursector (BBSH)
- Code voor Informatiebeveiliging (ISO 27001:2013 en ISO 27002:2013)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Wet op de identificatieplicht
- Richtlijnen van het Nationaal Cyber Security Centrum (NCSC).

Inrichting

Woningcorporaties doen er goed aan om een brede rol in te voeren, in de vorm van een Coördinator Informatie Beveiliging (CIB of Security Officer, SO). Daarnaast is er vanuit de wet AVG een rol voor een Functionaris Gegevensbescherming (FG) of Privacy Officer (PO). De rollen van SO en PO worden bij voorkeur bij twee verschillende functionarissen belegd. De FG is een onafhankelijk (intern) toezichthouder, die het werk van de SO en/of PO moet toetsen, en de directie gevraagd en ongevraagd van advies mag dienen.

We praten voor de Coördinator Informatie Beveiliging nadrukkelijk over een rol. Bij woningcorporaties kan deze rol ook in deeltijd uitgevoerd worden, waarbij het ook mogelijk is om deze rol te verdelen over verschillende medewerkers of te combineren over verschillende woningcorporaties heen (de coalitie zoeken).

1.7 Basis beveiligingsniveau

Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen vertrouwelijkheid, integriteit, beschikbaarheid. Deze Baseline sluit aan bij dit onderscheid.

Vertrouwelijkheid

De Baseline beschrijft de maatregelen die nodig zijn voor het basis vertrouwelijkheidsniveau (voor woningcorporaties) zijnde vertrouwelijke informatie, normale persoonsgegevens en bijzondere persoonsgegevens.

Het algemene dreigingsprofiel voor woningcorporaties, categorie Vertrouwelijk, is voor de Baseline vastgesteld op onder andere de volgende bedreigende factoren:

- de onbetrouwbare medewerker
- de wraakzuchtige medewerker
- de wraakzuchtige huurder
- de verontruste huurder
- de actiegroep
- de criminele opportunist
- de ingehuurde medewerker
- de vreemde overheden
- Georganiseerde misdaad

Hierbij zijn onder andere de volgende bedreigingen gedefinieerd voor woningcorporaties categorie Vertrouwelijk:

- infiltratie light
- social engineering
- publiek benaderbare sociale netwerken
- verhoor (fysiek geweld tegen personen)
- hacking op afstand
- malware (met en zonder remote control)
- crypto kraken
- ransomware
- (draadloze)netwerken interceptie
- (draadloze)netwerken actief benaderen
- inpluggen op fysiek netwerk
- verlies/diefstal van media
- publieke ruimtes
- achterblijven van patches
- beproeving van fysieke, technische en elektronische weerstand

Naast de bovenstaande specifieke bedreigingen gaat de Baseline ook uit van een set algemene dreigingen waarvan de hoofdgroepen zijn:

- onopzettelijk menselijk handelen
- opzettelijk menselijk handelen
- niet-beïnvloedbare externe factoren
- technisch falen

Uitgesloten zijn de volgende bedreigers: terreurgroep

Integriteit

Het onderwerp integriteit op informatiebeveiligingsvlak valt normaliter in twee delen uiteen: de integriteit van de datacommunicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het proces zelf), en de integriteit van de informatie in de applicaties of fysiek (d.w.z. gerelateerd aan het proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatieafhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Beschikbaarheid

Deze Baseline definieert een basis set aan eisen voor beschikbaarheid voor de informatie-infrastructuur van de woningcorporatie. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de (SaaS[3]) leverancier.

Dit houdt in dat voor de beschikbaarheid van de informatievoorziening een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

1.8 Bedreigingen

Onopzettelijke menselijke bedreigingen

Mensen kunnen onopzettelijk schade toebrengen. Iemand drukt op de delete-toets en let niet goed op de vraag of hij het wel zeker weet. Iemand steekt vreemde apparatuur besmet met een virus in het netwerk en brengt op die manier het virus over op een heel netwerk. Iemand gebruikt in paniek een poederblusser om een beginnend brandje te blussen en vernietigt daarmee een server.

Opzettelijke menselijke bedreigingen

Er kunnen diverse redenen zijn waarom mensen opzettelijk schade toebrengen aan informatiesystemen. Dat kunnen oorzaken van buitenaf zijn, zoals een hacker of hackergroep die iets heeft tegen de woningcorporatie en daarom binnendringt of de toegang voor huurders en/of medewerkers tot woningcorporatie systemen ontzegt.

Het kan ook een medewerker zijn die ontevreden is over de gang van zaken binnen de woningcorporatie en die uit boosheid data vernietigt. Het kan ook een frauderende medewerker zijn die uit persoonlijk gewin gegevens manipuleert in systemen of gegevens verkoopt.

Niet beïnvloedbare externe factoren

Invloeden van buitenaf zoals blikseminslag, brand, overstroming en stormschade zijn voorbeelden van niet-menselijke dreigingen. Deze bedreigingen zijn mede afhankelijk

[3] SaaS = Software as a Service, zie https://nl.wikipedia.org/wiki/Software_as_a_Service

van de locatie van de woningcorporatie, maar ook van de locatie van de belangrijkste informatiesystemen en apparatuur van de woningcorporatie. Er kunnen zelfs verschillen zijn tussen woningcorporaties onderling, bijvoorbeeld de ene woningcorporatie ligt grotendeels onder NAP en de andere er boven.

Technisch falen
Er kan tot slot ook sprake zijn van technisch falen, zoals uitvallen van ICT infrastructuur componenten, waardoor ondersteunende faciliteiten zoals applicaties, tekstverwerking, mail faciliteiten, telefonie en dergelijke niet meer beschikbaar zijn.

1.9 De Baseline en Risicomanagement

Informatiebeveiliging wordt bereikt door een geschikte verzameling beheersmaatregelen in te zetten, waaronder beleid, werkwijzen, procedures, organisatiestructuren en technische hulpmiddelen.

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.

Informatiebeveiligingsbeleid
Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces.

Risicomanagement

Risicomanagement is het systematisch opzetten, uitvoeren en bewaken van acties om risico's te identificeren, te prioriteren, te analyseren en voor deze risico's oplossingen te bedenken, te selecteren en uit te voeren.

Deze baseline gaat er vanuit dat er een koppeling tussen risicomanagement en informatiebeveiliging plaatsvindt.

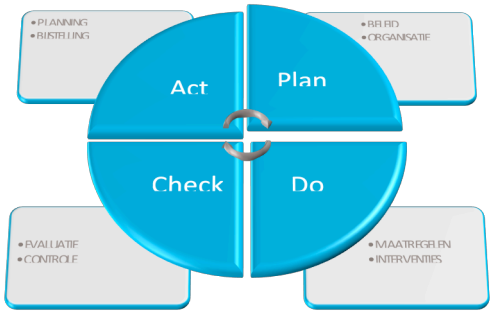
Incidentmanagement
Een incident, in het kader van incidentmanagement, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentmanagement is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van bedrijfsvoeringprocessen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen.

Bedrijfscontinuïteitsmanagement
Bedrijfscontinuïteitsmanagement is een proces waarbij de organisatie de nodige maatregelen treft om ongeacht de omstandigheden de continuïteit van de meest kritische processen te garanderen. In geval van een onderbreking van een of meerdere van deze processen moet de organisatie in staat zijn snel en kordaat op te treden, zodat deze activiteiten binnen de kortst mogelijke termijn kunnen worden hersteld.

Een product van Bedrijfscontinuïteitsmanagement is een BCP – Bedrijfscontinuïteitsplan, waarin de maatregelen en belangrijke gegevens van de

bedrijfsprocessen van de organisatie worden beschreven, die tot doel hebben de onderbrekingstijd tot een minimum te beperken.

ISMS en PDCA
Een ISMS (Informatie Security Management System) is een systeem, waarbij je stappen ten aanzien informatiebeveiliging continue blijft uitvoeren. Het is het uitvoeren van een PDCA cyclus (Plan, Do, Check, Act), waarbij je voor je ISMS een scope aangeeft. Plan (wat is er bedrijfskritiek en heb je een risicoanalyse?), Do (wat moet je verbeteren?), Check (heb je assessments, interne audits etc.?) en Act (acteren op de eerdere stappen, verbeteren van je proces).



De ISO27001:2013 norm veronderstelt dat de organisatie met behulp van het ISMS een koppeling maakt met Risicomanagement systeem.

Daarvoor zijn de volgende stappen relevant:

Risicobeoordeling van informatiebeveiliging
De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die:

1. risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder:
   a. de risicoacceptatiecriteria; en
   b. criteria voor het verrichten van risicobeoordelingen van informatiebeveiliging;

2. waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, geldige en vergelijkbare resultaten opleveren;

3. de informatiebeveiligingsrisico's identificeert:
   a. het risicobeoordelingsproces voor informatiebeveiliging toepassen om de risico's in verband met het verlies van vertrouwen in, integriteit van en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren;
   b. de risico-eigenaren identificeren;

4. de informatiebeveiligingsrisico's analyseert:
   a. de potentiële gevolgen beoordelen indien de risico's die zijn vastgesteld, zich zouden voordoen;
   b. de realistische waarschijnlijkheid beoordelen van het voorkomen van de risico's die zijn vastgesteld

c. de risiconiveaus vaststellen;

5. de informatiebeveiligingsrisico's evalueert:
   a. de resultaten vergelijken van risicoanalyses met de risicocriteria die zijn vastgesteld;
   b. de geanalyseerde risico's prioriteren voor risicobehandeling.

De organisatie moet gedocumenteerde informatie bewaren over het risicobeoordelingsproces van informatiebeveiliging.

Behandeling van informatiebeveiligingsrisico's
De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen om:

a) passende opties voor het behandelen van informatiebeveiligingsrisico's te kiezen, rekening houdend met de resultaten van de risicobeoordeling;

b) alle beheersmaatregelen vast te stellen, die nodig zijn om de gekozen optie(s) voor het behandelen van informatiebeveiligingsrisico's te implementeren;

OPMERKING: Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen.

c) de beheersmaatregelen die zijn vastgesteld te vergelijken met die in deze Baseline en om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten.

1.10 Opzet, beheer en onderhoud van de Baseline

CorpoNet is eigenaar van dit document en daarmee verantwoordelijk voor het beheer en onderhoud van de Baseline. Deze Baseline is gemaakt door de Special Interest Group Informatiebeveiliging van CorpoNet (kortweg aangeduid als SIG-BIC) en bevat de basis set aan beveiligingsmaatregelen die nodig zijn voor een stabiele en veilige basis voor een woningcorporatie.

Dit document en de daarin opgenomen maatregelen worden periodiek op inhoud, uitvoerbaarheid, invoering en werking beoordeeld en, indien nodig, aangepast om te voorkomen dat de Baseline veroudert.

De inhoudelijke toetsing en bijstelling van de Baseline vinden plaats door Special Interest Group Baseline Informatiebeveiliging Corporaties (SIG-BIC) binnen CorpoNet.

Herziening is mede afhankelijk van wijzigingen in de wetgeving, de onderliggende normen en het beleid en de beheerorganisatie. Beveiligingsincidenten vormen aanwijzingen waar voor de woningcorporatie specifieke kwetsbaarheden liggen. Voor de aanpassing van het basisniveau wordt dan ook gebruik gemaakt van een analyse van incidenten uit de periode voorafgaand aan het vaststellen van het nieuwe basisniveau.

Daarom wordt van de bij de **woningcorporatie verantwoordelijke functionarissen verwacht** dat zij zorg dragen voor een juiste en volledige registratie van beveiligings-incidenten en het melden daarvan, als onderdeel van de basis set van maatregelen.

2 De structuur van de norm

Hoofdstuk 3 gaat over risicomanagement en geeft aan welke stappen gezet moeten worden.

Hoofdstuk 4 beschrijft de inrichting van een managementsysteem voor informatiebeveiliging, een ISMS.

Hoofdstukken 5 t/m 18 bevatten de hoofdbeveiligingscategorieën en subcategorieën.

Bij elke subcategorie is de doelstelling (uit ISO 27001:2013, bijlage A) vermeld.

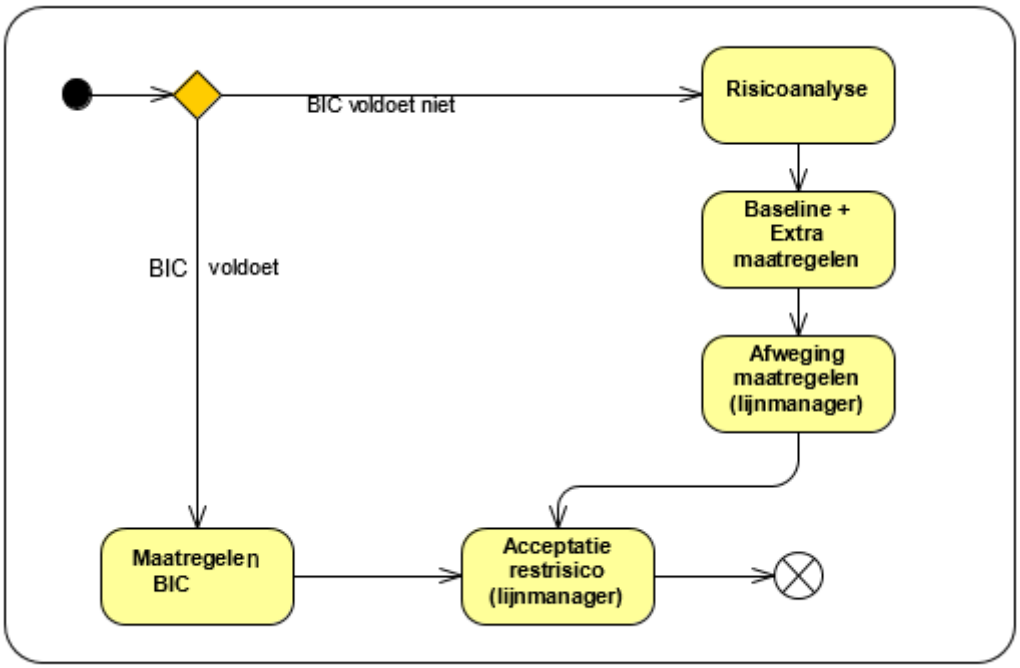
Elke subcategorie kent een aantal beheersmaatregelen, waarvan de nummering exact overeenkomt met ISO 27002:2013. De ISO 27002:2013 tekst van de beheersmaatregelen is cursief weergegeven.

Bijlage A bevat een begrippenlijst.

3. Risicomanagement

Volgens de BIC moet er risicomanagement plaatsvinden, bestaande uit het beoordelen, afwegen en aanpakken van mogelijke risico's. De methodes hiervoor zijn o.a. risicoanalyse, business impact-, afhankelijkheid- en kwetsbaarheidsanalyses.

Het beveiligingsniveau van de BIC is zo gekozen dat dit voor de primaire processen en ondersteunende ICT-voorzieningen bij woningcorporaties voldoende is. Hiermee wordt voorkomen dat er voor ieder systeem een uitgebreide risicobeoordeling uitgevoerd moet worden. Dit is schematisch weergegeven in het onderstaande figuur:



Toetsing risicomanagement

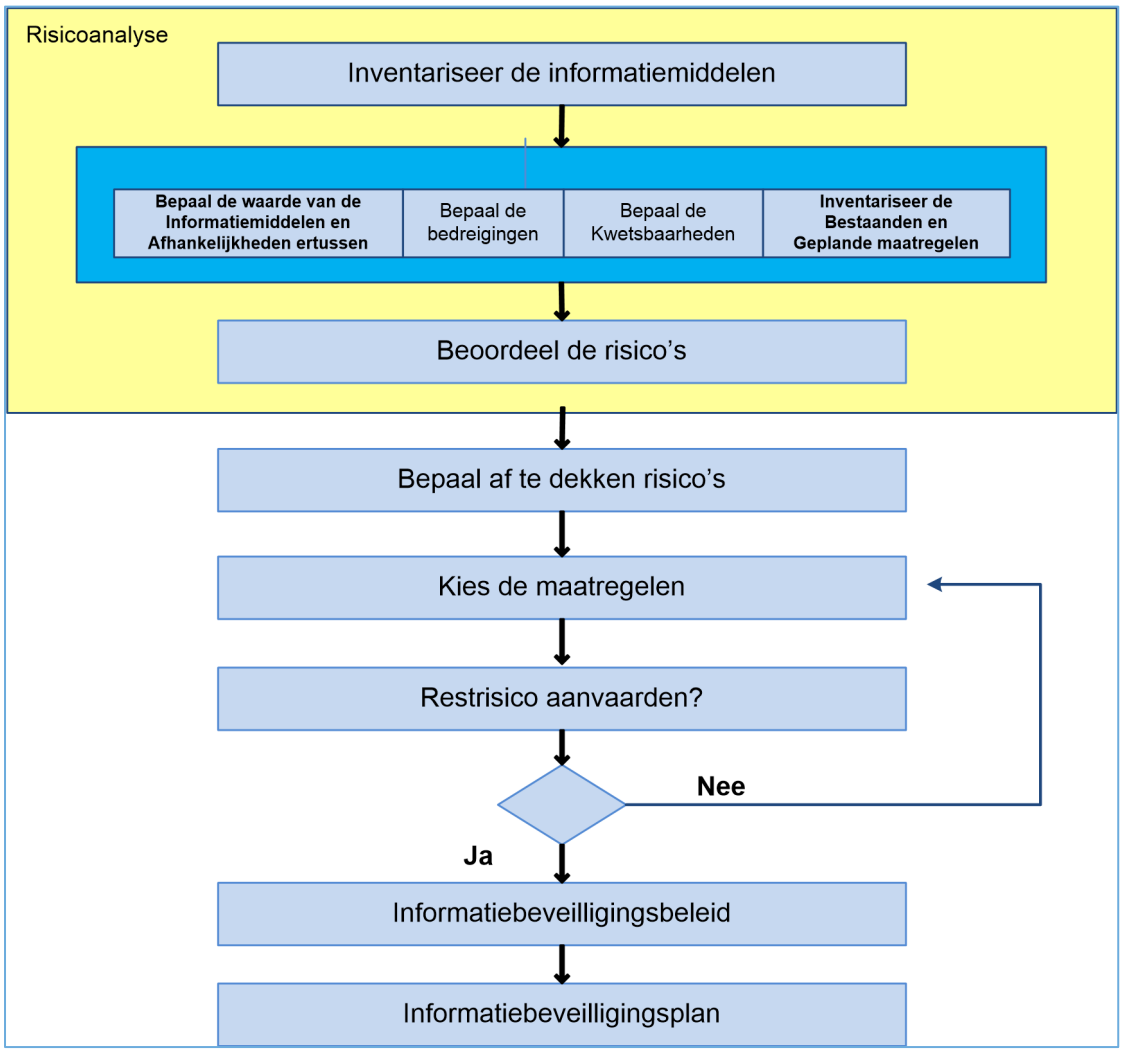
Bij de toetsing van het risicomanagement wordt onder meer bekeken of geclassificeerde informatie verwerkt wordt, of dat er sprake is van persoonsvertrouwelijke informatie zoals bedoeld in de AVG, of dat er hogere beschikbaarheidseisen vereist zijn of er dreigingen relevant zijn die niet in het dreigingsprofiel van de BIC meegenomen zijn.

3.1 Aanpak risicomanagement

Voor beveiliging vormt het beheersen van risico's het voornaamste principe. In de aanpak van Informatiebeveiliging in de BIC komen elementen van risicomanagement dan ook op verscheidene plaatsen aan de orde.

Om te bepalen aan welke risico's een organisatie bloot staat, is het nodig de bedreigingen, bedrijfsmiddelen (informatiemiddelen) en kwetsbaarheden te benoemen. Daarnaast is het van belang de gevolgen van een incident voor de organisatie te bepalen. Uit een inschatting van de waarschijnlijkheid dat een bedreiging tot een incident leidt, wordt daarmee het risico bepaald (zie 3.2). Of dit risico aanvaardbaar is, wordt bepaald aan de hand van criteria die de organisatie eerder heeft vastgesteld (zie verder 3.3).

Om de geïdentificeerde risico's te reduceren tot onder het aanvaardbare niveau zal de organisatie daarvoor geschikte beheersmaatregelen inzetten en de effectiviteit ervan voortdurend beoordelen (zie verder 3.4). In deze norm is het risicomanagement ingebed in de PDCA-cyclus (*PLAN, DO, CHECK, ACT*) van het ISMS.



Risicomanagement

3.2 Risicobeoordeling

De risicobeoordeling bestaat uit de systematische aanpak van het schatten van de omvang van de risico's (risicoanalyse) en het vergelijkingsproces van de ingeschatte risico's met risicocriteria om zo het belang van de risico's te bepalen.

Risicobeoordelingen worden periodiek uitgevoerd om in te spelen op wijzigingen in de beveiligingseisen en de risicosituatie, bijvoorbeeld wijzigingen in de bedrijfsmiddelen (informatiemiddelen), bedreigingen, kwetsbaarheden of veranderde omstandigheden. Specifieke aandacht is nodig voor de privacyaspecten van de informatiesystemen.

Adequate risicobeoordelingen identificeren en kwantificeren risico's en kennen prioriteit toe op basis van de risicostrategie en doelstellingen van de organisatie. Hierbij kunnen normen voor de sector van woningcorporaties een rol spelen, evenals reacties vanuit de buitenwereld.

De resultaten geven richting bij het bepalen van het informatiebeveiligingsbeleid en voor passende management acties en prioriteiten voor het beheersen van informatiebeveiligingsrisico's en voor het implementeren van beheersmaatregelen om de organisatie tegen deze risico's te beveiligen.

3.3 Risicostrategie

Er kan op verschillende manieren met de mogelijke risico's worden omgegaan[4]. De meest gebruikelijke strategieën zijn:

1. Risicodragend

Wil zeggen dat risico's geaccepteerd worden. Dat kan zijn omdat de kosten van de beveiligingsmaatregelen de mogelijke schade overstijgen. Het management kan ook besluiten om niets te doen, ondanks dat de kosten niet hoger zijn dan de schade die kan optreden. De maatregelen die een risicodragende organisatie neemt op het gebied van informatiebeveiliging zijn veelal van *repressieve* aard.

2. Risiconeutraal

Er worden dusdanige beveiligingsmaatregelen genomen dat dreigingen niet meer voor kunnen komen of wanneer dit toch gebeurt de schade als gevolg hiervan geminimaliseerd is. De meeste maatregelen die een risico neutrale organisatie neemt op het gebied van informatiebeveiliging zijn een combinatie van *preventieve-*, *detectieve-* en *repressieve* maatregelen.

3. Risicomijdend

Er worden maatregelen genomen waarmee de dreigingen zo veel mogelijk worden geneutraliseerd en niet meer leiden tot een incident. Veel van de maatregelen binnen deze strategie hebben een *preventief* karakter.

Welke strategie een organisatie ook kiest, de keuze dient bewust door het management te worden gemaakt en de gevolgen ervan dienen te worden gedragen.

[4] Zie voor meer achtergrond: https://nl.wikipedia.org/wiki/Informatiebeveiliging

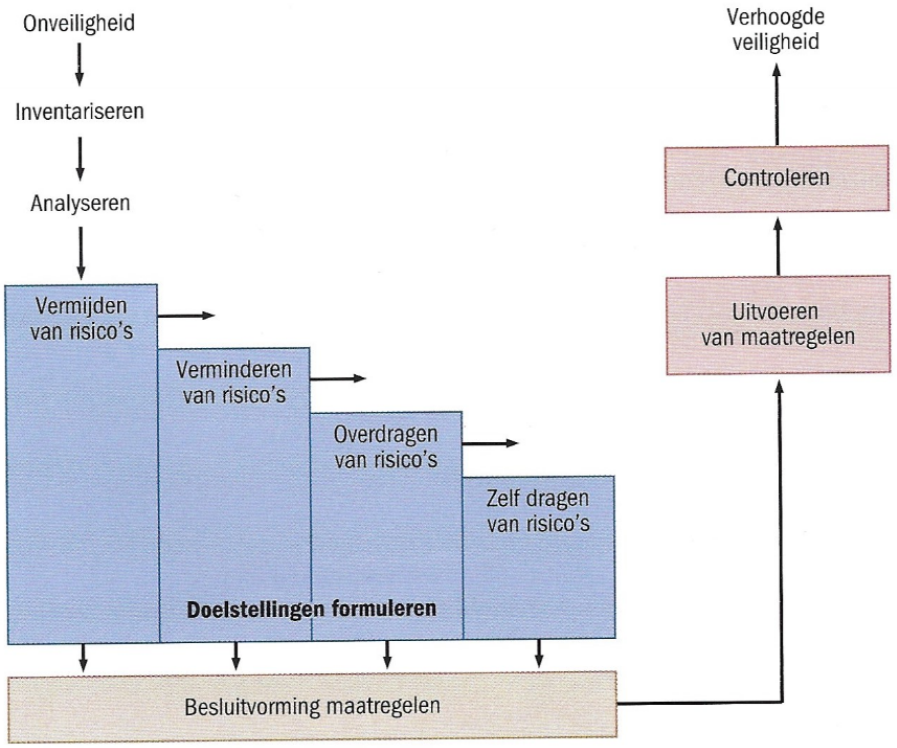
3.4 Risicobehandeling

De aanduiding 'risicobehandeling' benadrukt de activiteit van het reduceren van risico's tot aanvaardbare niveaus, waarbij wordt erkend dat er nooit afdoende middelen beschikbaar zullen zijn om volledige risicovermijding te bereiken. Het gaat om de balans tussen (ingeschatte) bedreigingen en risico's enerzijds en anderzijds de risico beperkende maatregelen, kosten en werkbaarheid.

De risicostrategie is de verantwoordelijkheid van het management van de organisatie. Dit bepaalt de wijze waarop de organisatie met risico's omgaat en rechtvaardigt de kosten voor informatiebeveiliging.

Een organisatie kan besluiten bepaalde risico's bewust te aanvaarden, mits wordt voldaan aan het beleid en de criteria voor risicoaanvaarding van de organisatie. In andere gevallen is de organisatie aangewezen op geschikte beheersmaatregelen om de risico's te verminderen. Hierbij wordt opgemerkt dat voor het verminderen van een bepaald risico vaak een combinatie van beheersmaatregelen nodig is, terwijl een beheersmaatregel aan de andere kant ook voor het verminderen van verschillende risico's van belang kan zijn.

Samengevat in een plaat:



4 Aanpak van de informatiebeveiliging

4.1 Managementsysteem voor informatiebeveiliging: ISMS

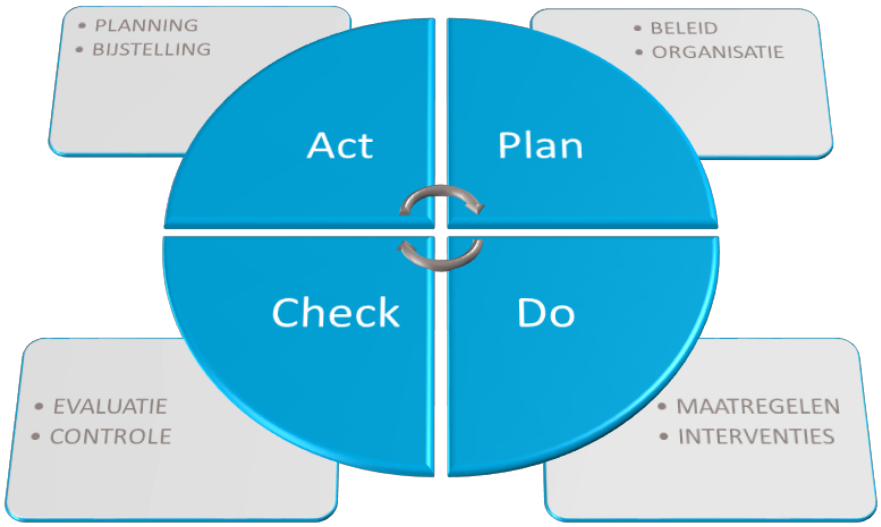
De organisatie moet een ISMS inrichten.

Een *'Information Security Management System (ISMS)*' biedt een organisatie een procesbenadering voor het beheersen van de informatiebeveiliging. De BIC is daarvoor de norm. Dit document beschrijft het cyclische proces *(plan/do/check/act)* voor het bepalen van beveiligingsdoelstellingen op basis van een risicobeoordeling, het treffen van maatregelen en het monitoren en beoordelen van de uitkomsten.

De procesbenadering in deze norm beoogt voor gebruikers het belang te onderstrepen van:
a) inzicht in de eisen van de organisatie ten aanzien van informatiebeveiliging en de noodzaak voor het vaststellen van beleid en doelstellingen voor informatiebeveiliging;
b) implementeren en uitvoeren van beheersmaatregelen om de risico's voor informatiebeveiliging voor de organisatie te beheren ten opzichte van de algemene bedrijfsrisico's van de organisatie;
c) controleren en beoordelen van de prestaties en de doeltreffendheid van het ISMS en
d) continue verbetering, gebaseerd op objectieve meting.

Volledige naleving van deze norm houdt in dat een organisatie kan aantonen dat zij een operationeel ISMS hanteert met geschikte auditprocessen om naleving te controleren.

Figuur 2 illustreert hoe het ISMS de eisen voor informatiebeveiliging en de verwachtingen van de belanghebbende partijen als input gebruikt en, door middel van de nodige maatregelen en processen, beveiliging van informatie biedt die aan die eisen en verwachtingen voldoet.



PDCA-model toegepast op ISMS-processen

Plan (het ISMS vaststellen)	Het vaststellen van het ISMS en de doelstellingen, processen en procedures die relevant zijn voor het risicomanagement en verbetering van de informatiebeveiliging, teneinde resultaten te leveren die in overeenstemming zijn met algemene beleidslijnen en doelstellingen van de organisatie.
Do (het ISMS implementeren en uitvoeren)	Het implementeren en uitvoeren van het ISMS, beheersmaatregelen, processen en procedures.
Check (het ISMS controleren en beoordelen)	Beoordelen en, voor zover van toepassing, meten van procesprestaties ten opzichte van het ISMS en de doelstellingen en ervaring uit de praktijk, en rapportage van de resultaten aan de directie ter beoordeling.
Act (het ISMS bijhouden en verbeteren)	Corrigerende en preventieve maatregelen nemen, op basis van de resultaten van de interne ISMS-audit en de directiebeoordeling of andere relevante informatie, om continue verbetering van het ISMS te bewerkstelligen.

4.2 Directieverantwoordelijkheid

4.2.1 Toewijzen verantwoordelijkheden

De directie moet verantwoordelijkheden ten aanzien van het ISMS toewijzen. Vervolgens zal dit ook moeten gebeuren ten aanzien van de verantwoordelijkheden voor de beveiliging van individuele bedrijfsprocessen, bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsprocessen.

Hierbij zijn verschillende verantwoordelijkheden te benoemen. Internationaal wordt vaak gebruik gemaakt van het zogenaamde RACI-model. Dit model maakt onderscheid naar de volgende verantwoordelijkheden:

* R: Responsible (verantwoordelijk), degene die de taak uitvoert en verantwoording aflegt aan degene die accountable is;

* A: Accountable (eindverantwoordelijk), degene die eindverantwoordelijk en beslissingsbevoegd is;

* C: Consulted (raadplegen), degene die vooraf wordt geraadpleegd en advies geeft over de te nemen beslissing;

* I: Informed (informeren), degene die achteraf over de genomen beslissing wordt geïnformeerd.

4.2.2 Actieve betrokkenheid

De directie moet bewijs kunnen leveren van haar betrokkenheid met betrekking tot het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het ISMS.

Dit kan worden bereikt door:

a) strategie en invoering van het ISMS te bepalen en het ISMS vast te stellen;

b) te bewerkstelligen dat beleid en plannen voor informatiebeveiliging worden vastgesteld;

c) rollen en verantwoordelijkheden vast te stellen ten aanzien van ontwikkeling en onderhoud van het ISMS;

d) in de organisatie het belang kenbaar te maken van het voldoen aan doelstellingen voor informatiebeveiliging en het naleven van het informatiebeveiligingsbeleid, de wettelijke verantwoordelijkheden en de noodzaak van continue verbetering;

e) afdoende middelen beschikbaar te stellen om het ISMS te ontwikkelen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren;

f) de criteria vast te stellen voor de aanvaarding van risico's en aanvaardbare risiconiveaus;

g) te bewerkstelligen dat interne ISMS-audits worden uitgevoerd;

h) directiebeoordelingen van het ISMS uit te voeren.

4.2.3 Stuurgroep

De directie kan worden ondersteund door een stuurgroep.

Het instellen van een stuurgroep voor informatiebeveiliging (of *Information Security Management Forum, ISMF*) verdient aanbeveling om toezicht te houden op informatiebeveiliging en om daar richting aan te geven. Mogelijk kan de taakstelling van een bestaande commissie daartoe worden uitgebreid, bijvoorbeeld een commissie voor risicomanagement of aansturing van de informatievoorziening.

In een dergelijke stuurgroep valt te overwegen vertegenwoordiging te zoeken van een breed scala aan functies op het gebied van informatieborging en aansturing, evenals functies uit verschillende gebruikersgroepen en belangrijke ondersteuningsfuncties. Doorgaans zijn ook functies op het gebied van interne auditing en human resources vertegenwoordigd.

4.3 PLAN: het ISMS vaststellen

PLAN: Het vaststellen van het ISMS en de doelstellingen, processen en procedures die relevant zijn voor het risicomanagement en verbetering van de informatiebeveiliging, teneinde resultaten te leveren die in overeenstemming zijn met algemene beleidslijnen en doelstellingen van de organisatie.

De directie moet het ISMS vaststellen.

4.4 DO: het ISMS implementeren en uitvoeren

DO: Het implementeren en uitvoeren van het ISMS, beheersmaatregelen, processen en procedures.

4.5 CHECK: het ISMS monitoren en beoordelen

CHECK: Beoordelen en, voor zover van toepassing, meten van procesprestaties ten opzichte van het ISMS en de doelstellingen en ervaring uit de praktijk, en rapportage van de resultaten aan de directie ter beoordeling.

4.5.1 Directiebeoordeling van het ISMS

De directie moet het ISMS van de organisatie met geplande tussenpozen beoordelen (bijvoorbeeld eenmaal per jaar), om te bewerkstelligen dat dit continu geschikt, passend en doeltreffend is. Deze beoordeling moet het onderzoeken van kansen voor verbetering omvatten alsmede de noodzaak van wijzigingen in het ISMS, waaronder het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen.

De resultaten van de beoordelingen moeten duidelijk worden gedocumenteerd.

5 Informatiebeveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Doelstelling

Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.

5.1.1 Beleidsregels voor informatiebeveiliging

Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

> *Er is een beleid voor informatiebeveiliging door de directie vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.*

5.1.2 Beoordelen van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

> *Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.*

6 Organisatie van de informatiebeveiliging

6.1 Interne organisatie

Doelstelling

Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.

1. De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving en zijn actueel. In de (bijlagen van een) arbeidsovereenkomst wordt minimaal aandacht besteed aan:
   - uitvoering van het informatiebeveiligingsbeleid
   - verantwoord omgaan met bedrijfsmiddelen
   - rapportage van beveiligingsincidenten
   - expliciete vermelding van de verantwoordelijkheden voor het verantwoord omgaan met vertrouwelijke en/of persoonsgegevens
2. [A]Alle medewerkers en tijdelijke medewerkers zijn zich bij hun aanstelling bewust van hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn gemakkelijk toegankelijk. Dit geldt ook voor de externe partijen.
3. [A]Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is dat voor indiensttreding (of bij functiewijziging), aantoonbaar duidelijk gemaakt.
4. [A]Elke manager is verantwoordelijk voor de integrale informatiebeveiliging van zijn of haar organisatieonderdeel.

6.1.2 Scheiding van taken

Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

1. Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties.

2. [A]Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

3. [A]Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.
4. [A]Verantwoordelijkheden voor beheer, wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.

6.1.3 Contact met overheidsinstanties

Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

1. [A]Het management stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, AP, enz.) wordt onderhouden.

6.1.4 Contact met speciale belangengroepen

Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.

1. Informatiebeveiliging specifieke informatie van relevante expertisegroepen, leveranciers van hardware, software en diensten wordt gebruikt om de informatiebeveiliging te verbeteren.
2. [A]De Coördinator Informatiebeveiliging onderhoudt contact met de SIG BIC van CorpoNet.

6.1.5 Informatiebeveiliging in projectbeheer

Informatie- en privacy beveiliging behoren aan de orde te komen in projectbeheer, ongeacht het soort project.

1. Informatiebeveiliging behoort te worden geïntegreerd in de projectbeheer-methode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligings-risico's worden geïdentificeerd en aangepakt als deel van een project.
   Dit geldt in het algemeen voor elk project ongeacht het karakter, bijvoorbeeld een project voor een proces voor kernactiviteiten, IT, 'facility management' en andere ondersteunende processen:
2. De gebruikte projectbeheermethoden behoren te vereisen dat:
   a) informatiebeveiligingsdoelstellingen worden opgenomen in projectdoelstellingen;
   b) een risicobeoordeling (Data Protection Impact Assessment(DPIA) ofwel Gegegevens Effect Beoordeling (GEB)) van informatiebeveiliging in een vroeg stadium van het project wordt uitgevoerd om de nodige beheersmaatregelen te identificeren;
   c) informatiebeveiliging deel uitmaakt van alle fasen van de toegepaste projectmethodologie.
3. In alle projecten behoren implicaties van informatiebeveiliging regelmatig te worden behandeld en beoordeeld.
4. Verantwoordelijkheden voor informatiebeveiliging behoren te worden gedefinieerd en toegewezen aan specifieke rollen die zijn gedefinieerd in de projectbeheermethoden.

6.2 Mobiele apparatuur en telewerken

Doelstelling

Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

6.2.1 Beleid voor mobiele apparatuur

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

1. [A]Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in niet-vertrouwde omgevingen vindt een risicoafweging plaats.
2. [A]Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.
3. [A]Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

6.2.2 Telewerken

Er behoort beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

1. Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.
2. Er wordt beleid vastgesteld met daarin de uitwerking welke systemen niet en welke systemen wel vanuit de thuiswerkplek of andere telewerkvoorzieningen mogen worden geraadpleegd. Dit beleid wordt bij voorkeur ondersteund door een MDM-oplossing (Mobile Device Management).
3. [A]De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen ('zero footprint') en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen.
   Voor printen in niet-vertrouwde omgevingen vindt een risicoafweging plaats.

7 Veilig Personeel

7.1 Voorafgaand aan het dienstverband

Doelstelling

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.

7.1.1 Screening

Verificatie van de achtergrond van kandidaten voor een dienstverband, tijdelijke personeel en externe gebruikers behoort 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.

1. [A]Voor de betreffende medewerkers (medewerkers en tijdelijke medewerkers) is minimaal een recente Verklaring Omtrent het Gedrag (VOG) vereist. Indien het een vertrouwensfunctie betreft kan er ook een veiligheidsonderzoek (Verklaring van Geen Bezwaar) worden uitgevoerd.
2. Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt over zijn arbeidsverleden en scholing geverifieerd.
3. [A]Het is noodzakelijk om de VOG of screening periodiek te herhalen volgens de voorschriften.

7.1.2 Arbeidsvoorwaarden

Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en tijdelijke gebruikers de arbeidsvoorwaarden van hun arbeidsovereenkomst te aanvaarden en te ondertekenen, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatie- en privacybeveiliging zijn vastgelegd.

7.2 Tijdens het dienstverband

Doelstelling

Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatie- en privacybeveiliging, 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.

7.2.1 Directieverantwoordelijkheid

De directie eist van werknemers, ingehuurd personeel en externe gebruikers dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

1. De directie ontwikkelt een strategie en ziet toe op implementatie van die strategie zodat blijvend over specialistische kennis en vaardigheden van medewerkers en ingehuurd personeel beschikt kan worden (onder andere die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen).
2. De directie bevordert dat medewerkers, ingehuurd personeel en (waar van toepassing) externe gebruikers van interne systemen algemene beveiligingsaspecten toepassen in hun gedrag en handelingen, overeenkomstig vastgesteld beleid.

7.2.2 Bewustwording, opleiding en training ten aanzien van informatie- en privacybeveiliging

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en/of instructie te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun rol.

1. Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.
2. [A]Bespreek het onderwerp informatie- en privacy beveiliging in functionerings- en beoordelingsgesprekken van medewerkers die risicovolle functies bekleden.

7.2.3 Disciplinaire procedure

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

1. [A]Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het informatie- en privacybeveiligingsbeleid.

7.3 Beëindiging en wijziging van dienstverband

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

7.3.1 Beëindiging of wijzigingen van verantwoordelijkheden

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

1. Voor medewerkers is vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Voor tijdelijk personeel (zowel in dienst van een derde bedrijf als individueel) is dit ook vastgelegd. Indien nodig is een geheimhoudingsverklaring ondertekend.
2. Er is een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.
3. Er is een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.

8 Beheer van bedrijfsmiddelen

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

8.1.1 Inventarisatie van bedrijfsmiddelen

Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.

1. Er is een actuele registratie van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, en diensten. Van elk middel is de waarde voor de organisatie, het vereiste beschermingsniveau en de verantwoordelijke manager bekent.

8.1.2 Eigendom van bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben.

1. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke benoemd.

8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

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

1. [A]Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name Internet, e-mail en mobiele apparatuur). Deze zijn beschreven en bekend in de organisatie. Voor extern personeel is dit in een overeenkomst vastgelegd.
2. Gebruikers hebben kennis van de regels.
3. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.
4. [A]Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.

8.1.4 Teruggeven van bedrijfsmiddelen

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, of anders overeengekomen.

8.2 Informatieclassificatie

Doelstelling

Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

8.2.1 Classificatie van informatie

Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

1. [A]De organisatie heeft richtlijnen opgesteld.
2. In overeenstemming met hetgeen in het AVG is vastgesteld, dient er een helder onderscheid te zijn in de categorie van gegevens, afhankelijk van de aard en waarde van die gegevens (art. 9, 10 en 15 AVG).

8.2.2 Informatie labelen

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.

1. [A]De verantwoordelijke heeft maatregelen getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van vertrouwelijke informatie.

8.2.3 Behandelen van bedrijfsmiddelen

Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

8.3 Behandeling van media

Doelstelling

Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

8.3.1 Beheer van verwijderbare media

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

1. [A]Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media.
2. [A]Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.
3. In het geval dat media een kortere verwachte levensduur hebben dan de gegevens die ze bevatten, worden de gegevens gekopieerd wanneer 75% van de levensduur van het medium is verstreken.
4. Gegevensdragers worden behandeld volgens de voorschriften van de fabrikant.

8.3.2 Verwijderen van media

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

1. [A]Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan door middel van een secure erase, voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.

8.3.3 Media fysiek overdragen

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

1. Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals:
   - versleuteling
   - bescherming door fysieke maatregelen, zoals afgesloten containers
   - gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen
   - persoonlijke aflevering
   - opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes
2. [A]Fysieke verzending van bijzondere informatie dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.

9 Toegangsbeveiliging

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling

Beheersen van de toegang tot informatie.

9.1.1 Beleid voor toegangsbeveiliging

Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang.

1. Eigenaren van bedrijfsmiddelen behoren passende regels voor toegangs-beveiliging, toegangsrechten en toegangsbeperkingen voor specifieke gebruikersrollen ten aanzien van hun bedrijfsmiddelen vast te stellen, waarbij de details en de striktheid van de beheersmaatregelen een afspiegeling zijn van de gerelateerde informatiebeveiligingsrisico's.
2. Toegangsbeveiligingsmaatregelen zijn zowel logisch als fysiek van aard (zie hoofdstuk 11) en behoren als een geheel te worden beschouwd. Gebruikers en dienstverleners behoren een duidelijke verklaring te ontvangen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiligingsmaatregelen moeten voldoen.
3. Het beleid behoort rekening te houden met het volgende:
   a) beveiligingseisen van de bedrijfstoepassingen;
   b) beleidsregels voor informatieverspreiding en -autorisatie, bijvoorbeeld het 'need-to-know'-principe, informatiebeveiligingsniveaus en -classificatie (zie 7.2);
   c) consistentie tussen de toegangsrechten en de beleidsregels inzake informatieclassificatie van systemen en netwerken;
   d) relevante wetgeving en contractuele verplichtingen met betrekking tot beperking aan de toegang tot gegevens of diensten (zie 17.1);
   e) het beheer van toegangsrechten in een distributie- en netwerkomgeving die alle beschikbare soorten verbindingen herkent;
   f) scheiding van toegangsbeveiligingsrollen, bijvoorbeeld toegangsverzoek, -autorisatie, -administratie;
   g) eisen voor formele autorisatie van toegangsverzoeken (zie 9.2.1 en 9.2.2);
   h) eisen voor het periodiek beoordelen van toegangsrechten (zie 9.2.5);
   i) intrekken van toegangsrechten (zie 9.2.6);
   j) archiveren van verslaglegging van alle belangrijke gebeurtenissen betreffende het gebruik en het beheer van gebruikersidentificaties en geheime authenticatie-informatie;
   k) rollen met speciale toegangsrechten (zie 9.2.3).

9.1.2 Toegang tot netwerk en netwerkdiensten

Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Een beleid voor het gebruik van netwerken en netwerkdiensten behoort te worden geformuleerd. Dit beleid behoort te omvatten:

a) de netwerken en netwerkdiensten waartoe toegang wordt verleend;
b) autorisatieprocedures om vast te stellen wie toegang krijgt tot welk netwerk en welke netwerkdiensten;

c) beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en -diensten te beschermen;
d) de middelen die worden gebruikt om toegang te krijgen tot netwerken en netwerkdiensten (bijvoorbeeld VPN of draadloos netwerk);
e) eisen voor gebruikersauthenticatie voor de toegang tot de verschillende netwerkdiensten;
f) monitoren van het gebruik van netwerkdiensten.

Het beleid voor het gebruik van netwerkdiensten behoort aan te sluiten bij het toegangsbeveiligingsbeleid van de organisatie (zie 8.1.1).

9.2 Beheer van toegangsrechten van gebruikers

Doelstelling

Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

9.2.1 Registratie en uitschrijving van gebruikers

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.

1. Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
2. Authenticatiegegevens worden bijgehouden in één bronbestand zodat consistentie is gegarandeerd.
3. Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

9.2.2 Gebruikers toegang verlenen

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

De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties behoort te omvatten:
a) autorisatie verkrijgen van de eigenaar van het informatiesysteem of de informatiedienst voor het gebruik van het informatiesysteem of de informatiedienst (zie beheersmaatregel 8.1.2); afzonderlijke goedkeuring voor toegangsrechten door de directie is mogelijk ook relevant;
b) verifiëren dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang (zie 9.1) en consistent is met andere eisen zoals een scheiding van taken (zie 6.1.2);
c) waarborgen dat toegangsrechten niet worden geactiveerd (bijvoorbeeld door dienstverleners) voordat de autorisatieprocedures zijn afgerond;
d) bijhouden van een centraal overzicht van toegangsrechten die aan een gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en -diensten;
e) aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren;
f) met eigenaren van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie 9.2.5).

9.2.3 Beheer van (speciale) toegangsrechten

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

1. Gebruikers hebben toegang tot speciale toegangsrechten voor zover dat voor de uitoefening van hun taak noodzakelijk is (need-to-know, need-to-use).
2. Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
3. Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties en commando's.
4. Er is aandacht voor het wijzigen van toegangsrechten bij verandering van functie/afdeling.

9.2.4 Beheer van geheime authenticatie-informatie van gebruikers

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

1. Het proces behoort de volgende eisen te bevatten:
   a) gebruikers behoren te worden verplicht een verklaring te ondertekenen dat zij persoonlijke geheime authenticatie-informatie geheimhouden en groepsinformatie, d.w.z. gedeelde geheime authenticatie-informatie, binnen de groep houden; deze getekende verklaring kan worden opgenomen in de arbeidsvoorwaarden (zie 7.1.2);
   b) als gebruikers hun eigen geheime authenticatie-informatie moeten onderhouden behoort hun eerst tijdelijke geheime authenticatie-informatie te worden gegeven die zij bij het eerste gebruik moeten wijzigen;
   c) er behoren procedures te worden vastgesteld om de identiteit van een gebruiker vast te stellen voordat nieuwe, vervangende of tijdelijke geheime authenticatie-informatie wordt verstrekt;
   d) tijdelijke geheime authenticatie-informatie behoort op een veilige manier aan gebruikers te worden gegeven;
   e) gebruikmaken van externe partijen of onbeschermde e-mailberichten (niet-gecodeerde tekst) behoort te worden vermeden
   f) tijdelijke geheime authenticatie-informatie behoort uniek voor een persoon te zijn en behoort niet te kunnen worden geraden;
   g) gebruikers behoren de ontvangst van geheime authenticatie-informatie te bevestigen;
   h) 'default' geheime authenticatie-informatie van een leverancier behoort te worden gewijzigd na de installatie van systemen of software

2. Ten aanzien van wachtwoorden geldt:
   a) Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
   b) Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
   c) Gebruikers bevestigen de ontvangst van een wachtwoord.
   d) Wachtwoorden zijn alleen bij de gebruiker bekend.
   e) Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
   f) Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.

9.2.5 Beoordeling van toegangsrechten van gebruikers

Het management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

1. Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.

9.2.6 Toegangsrechten intrekken of aanpassen

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

1. Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatie verwerkende faciliteiten en diensten te worden ingetrokken of opgeschort. Hierdoor kan worden vastgesteld of het noodzakelijk is om toegangsrechten in te trekken.
2. Wijzigingen in het dienstverband behoren te worden weerspiegeld in het intrekken van alle toegangsrechten die niet voor het nieuwe dienstverband zijn goedgekeurd. De toegangsrechten die behoren te worden ingetrokken of aangepast omvatten ook de fysieke en logische toegangsrechten. Intrekking of aanpassing kan plaatsvinden door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatie verwerkende faciliteiten of abonnementen. Elk document dat toegangsrechten van medewerkers en contractanten identificeert, behoort de intrekking of aanpassing van toegangsrechten weer te geven.
3. Indien een medewerker die uit dienst gaat of een externe gebruiker wachtwoorden kent van gebruikersidentificaties die actief blijven, dan behoren deze bij beëindiging of wijziging van dienstverband, contract of overeenkomst te worden gewijzigd.
4. Toegangsrechten voor informatie en bedrijfsmiddelen die samenhangen met informatie verwerkende faciliteiten behoren te worden verminderd of ingetrokken voordat het dienstverband eindigt of wijzigt, afhankelijk van de evaluatie van risicofactoren zoals:
   a) of de beëindiging of wijziging is geïnitieerd door de medewerker, de externe gebruiker of door de directie, en de reden voor de beëindiging;
   b) de huidige verantwoordelijkheden van de medewerker, externe gebruiker of overige gebruikers;
   c) de waarde van de bedrijfsmiddelen die op dat moment toegankelijk zijn.

9.3 Gebruikersverantwoordelijkheden

Doelstelling

Voorkomen van onbevoegde toegang door gebruikers en van beschadiging of diefstal van informatie en ICT-voorzieningen.

9.3.1 Geheime authenticatie informatie gebruiken

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

1. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:
   - Wachtwoorden worden niet opgeschreven.
   - Gebruikers delen hun wachtwoord nooit met anderen.
   - Wachtwoorden mogen niet opeenvolgend zijn.
   - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
   - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).

9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling

Voorkomen van onbevoegde toegang tot systemen en toepassingen.

9.4.1 Beperken van toegang tot informatie

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

1. In de soort toegangsregels wordt tenminste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
2. [A]Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
3. [A]Bij extern gebruik vanuit een niet-vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
4. [A]Een beheerder gebruikt two-factor authenticatie voor het beheer van kritische apparaten. Bijvoorbeeld een sleutel tot beveiligde ruimte en een password of een token en een password.

9.4.2 Beveiligde inlogprocedures

Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

1. [A]Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van two-factor authenticatie.
2. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
3. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
4. Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
5. [A]Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen blokkade

periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze blokkade op te heffen of het wachtwoord te resetten.

9.4.3 Systeem voor wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
2. [A]Wachtwoorden hebben een geldigheidsduur. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
3. [A]Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
   - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthentiseerd.
   - Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.

9.4.4 Speciale systeemhulpmiddelen gebruiken

Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.

Time-out van sessies
Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.

1. [A]De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.

Beperking van verbindingstijd
De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.

1. [A]De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding. Met two-factor authenticatie en tunneling.

9.4.5 Toegangsbeveiliging op programmabroncode

De toegang tot broncode van programmatuur behoort te worden beperkt.

1. De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.
2. Broncode staat op aparte (logische) systemen.

10 Cryptografie

10.1 Cryptografische beheersmaatregelen

Doelstelling

Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

1. De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
2. Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen.
3. [A]De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).

10.1.2 Sleutelbeheer

Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

1. In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
2. De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.
3. De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
4. Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.
5. [A]Bij voorkeur is sleutelmanagement ingericht volgens een algemeen aanvaarde standaard, zoals bijvoorbeeld de PKI Overheid.

11 Fysieke beveiliging en beveiliging van de omgeving

11.1 Beveiligde gebieden

Doelstelling

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

11.1.1 Fysieke beveiligingszone

Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

1. De gebouwen van de woningcorporatie en haar omgeving worden ingedeeld in verschillende zones.
2. Voor voorzieningen (binnen of buiten het gebouw) zijn duidelijke beveiligingsgrenzen bepaald.
3. Gebouwen bieden voldoende weerstand (bepaald op basis van een risicoafweging) bij gewelddadige aanvallen zoals inbraak en IT gericht vandalisme.
4. [A]Er zijn op verschillende plekken maatregelen voor de persoonlijke veiligheid van het personeel genomen, dit is met name van belang voor de publieke ruimtes en de spreekkamers en die ruimtes waar bezoekers in contact komen met medewerkers.
5. Er is minimaal periodieke surveillance en een inbraakalarm gekoppeld aan een alarmcentrale.
6. [A]Van ingehuurde bewakingsdiensten is vooraf geverifieerd dat zij voldoen aan de wettelijke eisen gesteld in de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus. Deze verificatie wordt periodiek herhaald.
7. In gebouwen met serverruimtes houdt (beveiligings)personeel toezicht op de toegang. Hiervan wordt een registratie bijhouden.
8. [A]Voor toegang tot speciale ruimten is een doelbinding vereist, dat wil zeggen dat personen op grond van hun werkzaamheden toegang kan worden verleend. (bijvoorbeeld Beheer, BHV etc.).

11.1.2 Fysieke toegangsbeveiliging

Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel[5] wordt toegelaten.

1. Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie.
2. [A]De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het toegangsbeleid.
3. In gebouwen met beveiligde zones houdt (beveiligings)personeel toezicht op de toegang. Hiervan wordt een registratie bijgehouden.

[5] Bevoegd personeel kan ook ingehuurd personeel zijn

4. De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering.
5. De uitgifte van toegangsmiddelen wordt geregistreerd.
6. Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.
7. Apparatuur en bekabeling in kabelverdeelruimtes en patchruimtes voldoen aan dezelfde eisen t.a.v. toegangsbeveiliging zoals die worden gesteld aan computerruimtes.
8. [A]Er vindt periodiek een controle/evaluatie plaats op de autorisaties voor fysieke toegang.

Bovenstaande zaken kunnen ook worden geregeld in een beleid rondom bezoekers en fysieke toegang.

11.1.3 Kantoren, ruimten en faciliteiten beveiligen

Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden toegepast.

1. Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen.
2. [A]Er is een actief onderhouden sleutelplan met procedures voor wijziging, ten behoeve van opslag van geclassificeerde informatie.
3. [A]Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices.

11.1.4 Bescherming tegen bedreigingen van buitenaf

Er behoren preventieve maatregelen tegen calamiteiten te worden toegepast.

1. Reserve apparatuur en back-ups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de back-up/reserve locatie niet meer toegankelijk zijn.
2. [A]Beveiligde ruimten waarin zich bedrijf kritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.
3. Gevaarlijke of brandbare materialen zijn op een zodanige afstand van een beveiligde ruimte opgeslagen dat een calamiteit met deze materialen geen invloed heeft op de beveiligde ruimte.
4. [A]Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.

11.1.5 Werken in beveiligde gebieden

Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.

1. Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin IT-voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.
2. Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.
3. Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.

11.1.6 Laad- en loslocatie

Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen.

1. [A]Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.

11.2 Beveiliging van apparatuur

Doelstelling

Het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

11.2.1 Plaatsing en bescherming van apparatuur

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.

1. Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.
2. Standaard accounts in apparatuur worden gewijzigd en de bijbehorende standaard wachtwoorden van leveranciers worden gewijzigd bij ingebruikname van apparatuur.
3. Gebouwen zijn beveiligd tegen blikseminslag.
4. Eten en drinken zijn verboden in computerruimtes.
5. Een informatiesysteem voldoet altijd aan de hoogste beveiligingseisen die voor kunnen komen bij het verwerken van informatie. Indien dit niet mogelijk is wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden.

11.2.2 Nutsvoorzieningen

Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

11.2.3 Beveiliging van bekabeling

Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen onderbreking of beschadiging te worden beschermd.

11.2.4 Onderhoud van apparatuur

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

1. [A]Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.

11.2.5 Verwijdering van bedrijfsmiddelen

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

11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Apparatuur buiten de terreinen behoort te worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

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

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

a) apparatuur en media die buiten het terrein worden gebracht behoren niet onbeheerd te worden achtergelaten in openbare ruimten;
b) voorschriften van de fabrikant voor het beschermen van de apparatuur behoren te allen tijde in acht te worden genomen, bijvoorbeeld bescherming tegen blootstelling aan sterke elektromagnetische velden;
c) beheersmaatregelen voor locaties buiten het terrein, zoals locaties voor thuiswerken, telewerken en tijdelijke locaties, behoren op basis van een risicobeoordeling te worden vastgesteld, en passende beheersmaatregelen behoren voor zover relevant te worden toegepast, bijvoorbeeld afsluitbare archiefkasten, 'clear desk'-beleid, toegangsbeveiligingsmaatregelen voor computers en beveiligde communicatie met het kantoor;
d) als apparatuur buiten het terrein tussen verschillende personen of externe partijen wordt overgedragen, behoort een overzicht te worden bijgehouden dat de bewakingsketen voor de apparatuur definieert, met daarin opgenomen ten minste de namen en organisaties die voor de apparatuur verantwoordelijk zijn.

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

11.2.7 Veilig verwijderen of hergebruiken van apparatuur

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.

1. [A]Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt geregistreerd.
2. [A]Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode.

11.2.8 Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

1. De gebruiker vergrendelt de werkplek tijdens afwezigheid.

11.2.9 'Clear desk' en 'clear screen' beleid

Er behoort een clear desk-beleid voor papier en verwijderbare opslagmedia en een clear screen-beleid voor ICT-voorzieningen te worden ingesteld.

1. In het clear desk-beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).
2. Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie 'beveiligd afdrukken' (pincode verificatie).
3. [A]Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
4. [A]Toegangsbeveiligingsvergrendeling wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).

12 Beveiliging bedrijfsvoering

12.1 Bedieningsprocedures en -verantwoordelijkheden

Doelstelling

Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

12.1.1 Gedocumenteerde bedieningsprocedures

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

1. Bedieningsprocedures bevatten informatie over opstarten, afsluiten, backup- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.
2. Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.

12.1.2 Wijzigingsbeheer

Wijzigingen in ICT-voorzieningen en informatiesystemen behoren te worden beheerst.

1. In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:
   - het administreren van significante wijzigingen
   - impactanalyse van mogelijke gevolgen van de wijzigingen
   - goedkeuringsprocedure voor wijzigingen
2. [A]Instellingen van informatiebeveiligingsfuncties (bijvoorbeeld security software) op het koppelvlak tussen interne en externe netwerken, worden automatisch op wijzigingen gecontroleerd.

12.1.3 Capaciteitsbeheer

Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

1. [A]De ICT-voorzieningen voldoen aan het voor de bedrijfsvoering overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen).

   Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.

   Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheid eis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
2. [A]In koppelpunten met externe zones worden maatregelen getroffen om aanvallen te signaleren en hierop te reageren.

12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen

Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

1. Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.
2. Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.
3. [A]Persoonsgegevens in alle systemen die geen productieomgeving zijn, dienen geanonimiseerd of gepseudonimiseerd te zijn.
4. [A]Indien er een experimenteer of laboratorium omgeving is, is deze voldoende gescheiden van de productieomgeving.

12.2 Bescherming tegen malware

Doelstelling

Beschermen van de integriteit van programmatuur en informatie.

12.2.1 Beheersmaatregelen tegen malware

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

Hierbij kan gedacht worden aan onder andere de volgende maatregelen:
1. [A]Bestanden worden geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent en (automatisch) plaats.
2. [A]Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent en (automatisch) plaats.
3. In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur anti-virusprogrammatuur van verschillende leveranciers toegepast.
4. [A]Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijvoorbeeld quarantaine en compartimentering).
5. Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.
6. Op mobiele apparatuur wordt anti-virusprogrammatuur toegepast.

12.3 Back-up

Doelstelling

Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen.

12.3.1 Backup van informatie

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

1. Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2. Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.
3. Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.
4. Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.
5. De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.

12.4 Verslagleggen en monitoren

Doelstelling

Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

12.4.1 Gebeurtenissen registreren

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.

1. Van logbestanden worden rapportages gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden. De logging van financiële systemen kan bijvoorbeeld dagelijks nagelopen worden. Controle van het Internetgebruik kan bijvoorbeeld per maand of kwartaal.
2. Een log-regel bevat minimaal:
   - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
   - de gebeurtenis
   - waar mogelijk de identiteit van het werkstation of de locatie
   - het object waarop de handeling werd uitgevoerd
   - het resultaat van de handeling
   - de datum en het tijdstip van de gebeurtenis
3. [A]In een log-regel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).
4. [A]Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een Security Information and Event Management systeem (SIEM), waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.

12.4.2 **Registratie** van storingen

Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.

12.4.3 Bescherming van informatie in logbestanden

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

1. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
2. [A]Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
3. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
4. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden, zal daarbij altijd het vier ogen principe toegepast worden.
5. [A]De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar.
6. Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld een logserver die niet bereikbaar is).

12.4.4 Logbestanden van beheerders en operators

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

12.4.5 Kloksynchronisatie

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

1. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.

12.5 Beheersing van operationele software

12.5.1 Software installeren op operationele systemen

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

1. Alleen geautoriseerd personeel kan software installeren of functies activeren.
2. Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.
3. Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
4. Er worden alleen door de leverancier onderhouden (versies van) software gebruikt.
5. Van updates wordt een log bijgehouden.
6. Er is een rollbackstrategie.

12.6 Beheer van technische kwetsbaarheden

Doelstelling

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

12.6.1 Beheersing van technische kwetsbaarheden

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

1. Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal het melden van incidenten, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
3. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
4. [A]Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en de daar uit voortvloeiende schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.
5. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de leverancier(s) of het NCSC.

13 Communicatiebeveiliging

Doelstelling

Het voorkomen van onbevoegde toegang tot netwerkdiensten.

13.1 Beheer van netwerkbeveiliging

Doelstelling

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

13.1.1 Beheersmaatregelen voor netwerken

Netwerken behoren adequaat te worden beheerd en beheerst om deze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

1. Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid en beschikbaarheid van het netwerk niet in het geding komt.
2. [A]Gegevensuitwisseling tussen interne en externe zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
3. [A]Bij transport van vertrouwelijke informatie over externe netwerken, zoals het Internet, dient altijd encryptie te worden toegepast.
4. Er zijn procedures voor beheer van apparatuur op afstand.

13.1.2 Beveiliging van netwerkdiensten

Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze bevoegd zijn.

1. Er is een gedocumenteerd beleid met betrekking tot het gebruik van netwerken en netwerkdiensten. Gebruikers krijgen slechts toegang tot de netwerkdiensten die voor het werk noodzakelijk zijn.

13.1.3 Scheiding van netwerken

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

Hierbij kan gedacht worden aan bijvoorbeeld het volgende:

1. [A]Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
2. [A]De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.

3. [A]Elke zone heeft een gedefinieerd beveiligingsniveau. Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in het beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
4. [A]Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
5. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

13.2 Uitwisseling van informatie

Doelstelling

Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met een externe partij.

13.2.1 Beleid en procedures voor informatietransport

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.

Informatie kan worden overgedragen via het gebruik van een aantal verschillende communicatiefaciliteiten, waaronder e-mail, telefoon, fax en video.
Software kan worden overgedragen via een aantal verschillende media, waaronder downloaden van het Internet en verkrijgen via leveranciers die standaardproducten verkopen.
De zakelijke, wettelijke en beveiligingsimplicaties die samenhangen met elektronische gegevensuitwisseling, elektronische handel en elektronische communicatie en de eisen voor beheersmaatregelen behoren in overweging te worden genomen.

13.2.2 Overeenkomsten over informatietransport

Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

1. Er zijn afspraken of overeenkomsten gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid - waaronder traceerbaarheid en onweerlegbaarheid - van gegevens te waarborgen zijn beschreven en getoetst.
2. Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.
3. Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd.
4. [A]Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

13.2.3 Elektronisch berichten

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

1. [A]Digitale documenten binnen de woningcorporatie waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van certificaten voor tekenen en/of encryptie.
2. Er is een (spam)filter geactiveerd voor e-mailberichten.
3. [A]Bijzondere persoonsgegevens (BSN, et cetera) worden verwijderd.

13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid of voor een geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.

1. [A]De geheimhoudingsplicht voor medewerkers is geregeld in de (bijlage van de) arbeidsovereenkomst.

14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14.1 Beveiligingseisen voor informatiesystemen

Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

14.1.1 Analyse en specificatie van informatiebeveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligings- en privacymaatregelen te worden opgenomen.

1. In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp (Privacy by Design/Privacy by Default). Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
2. In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten. Waar mogelijk wordt gebruikt gemaakt van bestaande richtlijnen.
3. Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.
4. Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
5. Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria.
6. Er is expliciet aandacht voor leveranciers accounts, hardcoded wachtwoorden en mogelijke ‘achterdeurtjes’.

14.1.2 Toepassingsdiensten op openbare netwerken beveiligen

Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.

Toepassingen die toegankelijk zijn via publieke netwerken staan bloot aan een reeks netwerk gerelateerde dreigingen zoals frauduleuze activiteiten, geschillen over contracten of openbaarmaking van informatie.
Daarom zijn gedetailleerde risicobeoordelingen en een juiste keuze van beheersmaatregelen onmisbaar.

Vereiste beheersmaatregelen behelzen vaak cryptografische methoden voor het authentiseren en beveiligen van gegevensoverdracht.
Toepassingen kunnen gebruikmaken van beveiligde authenticatiemethoden, bijvoorbeeld toepassing van een asymmetrisch cryptografiesysteem en digitale handtekeningen (zie hoofdstuk 10) om de risico’s te verminderen. Ook kan gebruik worden gemaakt van betrouwbare derden als dergelijke diensten nodig zijn.

14.1.3 Transacties van toepassingsdiensten beschermen

Informatie die een rol speelt bij online-transacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten,

onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.

1. Een transactie wordt bevestigd (geautoriseerd) door een (gekwalificeerde) elektronische handtekening of een andere wilsuiting van de gebruiker.
2. Een transactie is versleuteld, de partijen zijn geauthentiseerd en de privacy van betrokken partijen is gewaarborgd.

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling

Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

14.2.1 Beleid voor beveiligd ontwikkelen

Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.

1. Beveiligd ontwikkelen is een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem. In een beleid voor beveiligd ontwikkelen behoren de volgende aspecten in overweging te worden genomen:
   a) DPIA;
   b) Privacy by Design/Privacy by Default;
   c) beveiliging van de ontwikkelomgeving;
   d) richtlijnen betreffende beveiliging in de levenscyclus van softwareontwikkeling:
      1) beveiliging in de software ontwikkelmethodologie;
      2) beveiligde coderingsrichtlijnen voor elke programmeertaal die wordt gebruikt.
   e) beveiligingseisen in de ontwikkelfase;
   f) beveiligingscontrolepunten binnen de mijlpalen van het project;
   g) beveiligde informatiecentra;
   h) beveiliging van de versiecontrole;
   i) vereiste kennis over toepassingsbeveiliging;
   j) het vermogen van de ontwikkelaar om kwetsbaarheden te vermijden, te vinden en te repareren.
2. Technieken voor beveiligd programmeren behoren zowel te worden gebruikt voor nieuwe ontwikkelingen als in scenario's voor hergebruik van codes waarvan de normen die voor de ontwikkeling zijn toegepast niet bekend zijn of niet consistent waren met de huidige 'best practices'.
3. Toepassing van beveiligde coderingsnormen behoort te worden overwogen en indien relevant verplicht te worden gesteld.
4. Ontwikkelaars behoren te worden getraind in het toepassen van codering, en het gebruik behoort te worden geverifieerd door te testen en de codes te beoordelen.
5. Indien ontwikkelactiviteiten worden uitbesteed behoort de organisatie zich ervan te vergewissen dat de externe partij deze regels voor veilig ontwikkelen naleeft (zie 14.2.7).

14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen

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

1. Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL en voor applicaties ASL.

14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform

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

1. Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen.

14.2.4 Beperkingen op wijzigingen in softwarepakketten

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

1. Bij het instellen van besturingsprogrammatuur en softwareprogrammapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

14.2.5 Principes voor engineering van beveiligde systemen

Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.

1. Procedures voor de engineering van beveiligde informatiesystemen, gebaseerd op principes voor beveiligde engineering, behoren te worden vastgesteld, gedocumenteerd en toegepast op interne engineeringactiviteiten met betrekking tot informatiesystemen.
2. Beveiliging behoort te worden ontworpen in alle lagen van de architectuur (commercieel, gegevens, toepassingen en technologie), waarbij de behoefte aan informatiebeveiliging behoort te worden afgewogen tegen de behoefte aan toegankelijkheid.
3. Nieuwe technologie behoort te worden geanalyseerd op veiligheidsrisico's en het ontwerp behoort te worden beoordeeld aan de hand van bekende aanvalspatronen.
4. Deze principes en de vastgestelde engineeringprocedures behoren regelmatig te worden beoordeeld om te waarborgen dat ze doelmatig bijdragen aan verbeterde normen voor beveiliging binnen het engineeringproces.
5. Deze principes behoren ook regelmatig te worden beoordeeld om ervoor te zorgen dat ze actueel blijven in de zin dat ze nieuwe potentiële bedreigingen afwenden en toepasbaar blijven bij verbeteringen die worden toegepast in de technologieën en oplossingen.
6. De voor engineering vastgestelde beveiligingsprincipes behoren indien van toepassing te worden toegepast op uitbestede informatiesystemen via de contracten en andere bindende overeenkomsten (verwerkersovereenkomst) tussen de organisatie en de leverancier aan wie de organisatie uitbesteedt. De organisatie behoort te bevestigen dat de strikte toepassing van de beveiligingsprincipes voor engineering vergelijkbaar is met het gebruik in de eigen organisatie.

14.2.6 Beveiligde ontwikkelomgeving

Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.

1. Een beveiligde ontwikkelomgeving omvat personen, processen en technologie die in verband staan met systeemontwikkeling en integratie.
2. Organisaties behoren risico's te beoordelen die samenhangen met individuele verrichtingen betreffende systeemontwikkeling en beveiligde ontwikkelomgevingen vast te stellen voor specifieke verrichtingen op het gebied van systeemontwikkeling, rekening houdend met:
   a) de gevoeligheid van de gegevens die door het systeem worden verwerkt, opgeslagen en verstuurd;
   b) toepasselijke externe en interne eisen, bijvoorbeeld van regelgeving of beleidsregels zoals Privacy by Design en Privacy by Default;
   c) beheersmaatregelen voor beveiliging die al door de organisatie zijn geïmplementeerd ter ondersteuning van systeemontwikkeling;
   d) betrouwbaarheid van personeel dat in de omgeving werkt (zie 7.1.1);
   e) de graad van uitbesteding met betrekking tot systeemontwikkeling;
   f) de behoefte aan scheiding tussen verschillende ontwikkelomgevingen;
   g) toegangsbeveiliging voor de ontwikkelomgeving;
   h) monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes;
   i) de beheersmaatregel dat back-ups worden bewaard op veilige externe locaties;
   j) controle over bewegingen van gegevens van en naar de omgeving.
3. Als het beschermingsniveau voor een specifieke ontwikkelomgeving is vastgesteld, behoren organisaties corresponderende processen in veilige ontwikkelprocedures te documenteren en deze beschikbaar te stellen aan alle personen die ze nodig hebben.

14.2.7 Uitbestede ontwikkeling van programmatuur

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

1. Uitbestede ontwikkeling van programmatuur komt tot stand onder supervisie en verantwoordelijkheid van de uitbestedende organisatie. Er worden maatregelen getroffen om de kwaliteit en vertrouwelijkheid te borgen (bijvoorbeeld stellen van veiligheidseisen, regelen van beschikbaarheid en eigendomsrecht van de code, certificatie, kwaliteitsaudits, testen en aansprakelijkheidsregelingen).

14.2.8 Testen van systeembeveiliging

Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.

Tijdens de ontwikkelprocessen zijn voor nieuwe en geactualiseerde systemen uitvoerige tests en verificatie nodig, met inbegrip van het opstellen van een gedetailleerd schema van activiteiten en tests van inputs en verwachte outputs onder diverse omstandigheden.

Voor interne ontwikkelactiviteiten behoren dergelijke tests in eerste instantie te worden uitgevoerd door het ontwikkelteam.

Vervolgens behoren onafhankelijke tests te worden uitgevoerd (zowel voor interne als voor uitbestede ontwikkelactiviteiten) om te bewerkstelligen dat het systeem uitsluitend werkt zoals voorzien (zie 14.1.1 en 14.2.9). De omvang van het testen behoort in verhouding te staan tot de belangrijkheid en de aard van het systeem.

14.2.9 Systeemacceptatietests

Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

1. [A]Van acceptatietests wordt een log bijgehouden.
2. Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP[6] of gelijkwaardig.

14.3 Testgegevens

14.3.1 Bescherming van testgegevens

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.

Het voor testdoeleinden gebruiken van operationele databases met persoonsgegevens of enige andere vertrouwelijke informatie behoort te worden vermeden. Indien persoonsgegevens of anderszins vertrouwelijke informatie wordt gebruikt voor testdoeleinden, behoren alle gevoelige details en inhoud te worden beschermd door deze te verwijderen of te wijzigen (anonimisering/pseudonimisering).

[6] Zie voor achtergrond informatie www.owasp.org

15. Leveranciersrelaties

15.1 Informatiebeveiliging in leveranciersrelaties

Doelstelling

De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties

Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.

1. De organisatie behoort beheersmaatregelen voor informatiebeveiliging vast te stellen en verplicht te stellen om specifiek de toegang van de leverancier tot de informatie van de organisatie beleidsmatig aan te pakken.
2. Deze beheersmaatregelen behoren betrekking te hebben op de door de organisatie te implementeren processen en procedures.

Informatie kan in gevaar worden gebracht door leveranciers met een inadequaat informatiebeveiligingsbeheer. Om toegang voor leveranciers tot informatie verwerkende faciliteiten te beheren, behoren beheersmaatregelen te worden vastgesteld en toegepast. Indien er bijvoorbeeld een speciale behoefte is om de informatie vertrouwelijk te houden, kunnen geheimhoudingsovereenkomsten en verwerkersovereenkomsten worden gebruikt.

15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten en verwerkersovereenkomst

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligings- en privacy eisen te zijn opgenomen.

1. De noodzakelijk geachte maatregelen behorend bij 15.1.1 zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.
2. Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
3. In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
4. In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.
5. Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.
6. In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
7. Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is

verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.

8. De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst.

15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.

Overwogen behoort te worden de volgende onderwerpen op te nemen in leveranciersovereenkomsten betreffende beveiliging van de toeleveringsketen:

a) informatiebeveiligingseisen definiëren die gelden voor acquisitie van producten of diensten op het gebied van informatie- en communicatietechnologie naast de algemene informatiebeveiligingseisen voor leveranciersrelaties;

b) met betrekking tot diensten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers de beveiligingseisen van de organisatie in de gehele toeleveringsketen bekendmaken indien leveranciers delen van diensten op het gebied van informatie- en communicatietechnologie die zij aan de organisatie leveren, uitbesteden;

c) met betrekking tot producten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers passende beveiligingspraktijken in de gehele toeleveringsketen bekendmaken indien deze producten componenten bevatten die van andere leveranciers worden betrokken;

d) een monitorproces en aanvaardbare methoden implementeren om te valideren dat geleverde producten en diensten op het gebied van informatie- en communicatietechnologie in overeenstemming zijn met verklaarde beveiligingseisen;

e) een proces implementeren voor het vaststellen van componenten van producten of diensten die essentieel zijn voor het handhaven van de functionaliteit en daardoor verhoogde aandacht en toezicht vereisen als deze buiten de organisatie worden gebouwd, in het bijzonder indien de eindleverancier delen van componenten van producten of diensten aan andere leveranciers uitbesteedt;

f) zekerheid verkrijgen dat essentiële componenten en de herkomst ervan in de toeleveringsketen kunnen worden nagespeurd;

g) zekerheid verkrijgen dat de geleverde producten op het gebied van informatie- en communicatietechnologie functioneren zoals voorzien zonder onverwachte of ongewenste verschijnselen;

h) regels definiëren voor het delen van informatie met betrekking tot de toeleveringsketen en potentiële kwesties en compromissen tussen de organisatie en leveranciers;

i) specifieke processen implementeren voor het beheren van de levenscyclus en de beschikbaarheid van de componenten van de informatie- en communicatietechnologie en samenhangende beveiligingsrisico's. Hiertoe behoort het beheren van de risico's van componenten die niet langer beschikbaar zijn doordat leveranciers niet meer bestaan of doordat leveranciers deze componenten niet meer leveren in verband met verbeterde technologie.

15.2 Beheer van dienstverlening van leveranciers

15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

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

1. Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
2. De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt periodiek.
3. Er zijn voor beide partijen eenduidige aanspreekpunten.

15.2.2 Beheer van veranderingen in dienstverlening van leveranciers

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.

16. Beheer van Informatiebeveiligingsincidenten

16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling

Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

16.1.1 Verantwoordelijkheden en procedures

Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.

Met betrekking tot het beheer van informatiebeveiligingsincidenten behoren de volgende richtlijnen voor directieverantwoordelijkheden en -procedures in overweging te worden genomen:

1. er behoren directieverantwoordelijkheden te worden vastgesteld om te bewerkstelligen dat de volgende procedures adequaat binnen de organisatie worden ontwikkeld en gecommuniceerd:
    a. [A]Procedure voor de wet Meldplicht datalekken;
    b. procedures voor incident responsplanning en -voorbereiding;
    c. procedures voor het monitoren, opsporen, analyseren en rapporteren van informatiebeveiligingsgebeurtenissen en -incidenten;
    d. procedures voor de verslaglegging van beheeractiviteiten betreffende incidenten;
    e. procedures voor het omgaan met forensisch bewijs;
    f. procedures voor het beoordelen van en besluitvorming over informatiebeveiligingsgebeurtenissen en beoordeling van zwakke plekken in de informatiebeveiliging;
    g. responsprocedures met inbegrip van procedures voor escalatie, beheerst herstel van een incident en communicatie aan in- en extern personen of organisaties.
2. vastgestelde procedures behoren te bewerkstelligen dat:
    a. competent personeel de kwesties behandelt die verband houden met informatiebeveiligingsincidenten binnen de organisatie;
    b. een contactpunt voor het opsporen en rapporteren van beveiligingsincidenten wordt geïmplementeerd;
    c. passende contacten worden onderhouden met instanties, externe belangengroepen of fora die aangelegenheden behandelen die verband houden met informatiebeveiligingsincidenten.
3. rapportageprocedures behoren de volgende aspecten te omvatten:
    a. formulieren voorbereiden voor het rapporteren van informatiebeveiligingsgebeurtenissen ter ondersteuning van de rapportage-actie en om te bevorderen dat de rapporterende persoon aan alle nodige acties denkt die in geval van een informatiebeveiligingsgebeurtenis moeten worden verricht;
    b. de procedures die in geval van een informatiebeveiligingsgebeurtenis moeten worden uitgevoerd, bijvoorbeeld onmiddellijk alle details noteren, zoals aard van niet-naleving of overtreding, optredende storing, berichten

op het scherm, en onmiddellijk rapporteren aan het contactpunt en alleen gecoördineerde actie ondernemen;

c. verwijzing naar een vastgestelde disciplinaire formele procedure voor het omgaan met medewerkers die beveiligingsovertredingen begaan;

d. passende feedbackprocedures om te bewerkstelligen dat de personen die informatiebeveiligingsgebeurtenissen melden, worden geïnformeerd over de resultaten nadat de kwestie is behandeld en afgesloten.

De doelstellingen voor het beheer van informatiebeveiligingsincidenten behoren met de directie te worden overeengekomen en er behoort te worden gewaarborgd dat de personen die verantwoordelijk zijn voor het beheer van informatiebeveiligingsincidenten op de hoogte zijn van de prioriteiten van de organisatie voor het behandelen van informatiebeveiligingsincidenten.

16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen

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

1. Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen 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 beveiligingsincident.
2. [A]Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.
3. Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd naar de Coördinator Informatiebeveiliging.
4. Vermissing of diefstal van apparatuur of media die gegevens van de organisatie kunnen bevatten wordt altijd aangemerkt als informatiebeveiligingsincident.
5. Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De Coördinator Informatiebeveiliging bekijkt periodiek – bij voorkeur maandelijks - een samenvatting van de informatie.

16.1.3 Rapportage van zwakke plekken in de beveiliging

Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

1. Er is een proces om eenvoudig en snel beveiligingsincidenten en zwakke plekken in de beveiliging te melden. Het rapporteringsmechanisme behoort zo eenvoudig, toegankelijk en beschikbaar te zijn als mogelijk is.

16.1.4 Beoordeling van en besluitvorming over informatiebeveiligings-gebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.

1. Het contactpunt behoort elke informatiebeveiligingsgebeurtenis te beoordelen op basis van het overeengekomen classificatieschema voor gebeurtenissen en incidenten betreffende informatiebeveiliging, en te besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident.
2. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen.
3. In gevallen waarin de organisatie beschikt over een responsteam voor informatiebeveiligingsincidenten (ISIRT), kunnen de beoordeling en het besluit worden doorgestuurd naar het ISIRT voor bevestiging of herbeoordeling.
4. Resultaten van de beoordeling en het besluit behoren in een verslag te worden vastgelegd ten behoeve van toekomstige verwijzing en verificatie.

16.1.5 Respons op informatiebeveiligingsincidenten

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

1. Op informatiebeveiligingsincidenten behoort te worden gereageerd door een aangewezen contactpunt en andere relevante personen van de organisatie of externe partijen (zie 16.1.1).
2. De respons behoort de volgende aspecten te omvatten:
   a) zo snel mogelijk na de gebeurtenis bewijs verzamelen;
   b) indien vereist, forensische analyse van de informatiebeveiliging uitvoeren (zie 16.1.7);
   c) escaleren indien vereist;
   d) bewerkstelligen dat alle betrokken responsactiviteiten op de juiste manier worden vastgelegd voor latere analyse;
   e) het bestaan van het informatiebeveiligingsincident of relevante details daarvan communiceren aan andere in- en externe personen of organisaties met een ‘need-to-know’;
   f) behandelen van de zwakke plek(ken) in de informatiebeveiliging waarvan is vastgesteld dat deze het incident heeft/hebben veroorzaakt of eraan heeft/hebben bijgedragen;
   g) het incident formeel afsluiten en verslaglegging bijhouden zodra het incident met succes is behandeld.
3. Om de bron van het incident te identificeren behoort post incident analyse plaats te vinden.

16.1.6 Leren van informatiebeveiligingsincidenten

Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.

1. Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd
2. De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

16.1.7 Verzamelen van bewijsmateriaal

De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

Bij het omgaan met bewijs ten behoeve van disciplinaire en wettelijke actie behoren interne procedures te worden ontwikkeld en gevolgd.

In het algemeen behoren deze bewijsprocedures processen in te houden voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs in overeenstemming met de verschillende soorten media, apparaten en de status van de apparaten, bijvoorbeeld in- of uitgeschakeld. De procedures behoren rekening te houden met de:

a. bewakingsketen;
b. veiligheid van bewijs;
c. veiligheid van personeel;
d. rollen en verantwoordelijkheden van het betrokken personeel;
e. competentie van personeel;
f. documentatie;
g. instructie.

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

Forensisch bewijs kan grenzen van organisaties of rechtsgebieden overschrijden. In zulke gevallen behoort te worden gewaarborgd dat de organisatie het recht heeft de vereiste informatie als forensisch bewijs te verzamelen. De eisen van verschillende rechtsgebieden behoren ook in aanmerking te worden genomen om de kans zo groot mogelijk te maken dat het bewijs wordt toegelaten in de relevante rechtsgebieden.

17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

17.1 Informatiebeveiligingscontinuïteit

Doelstelling

Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

17.1.1 Informatiebeveiligingscontinuïteit plannen

Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

1. Een organisatie behoort vast te stellen of de continuïteit van de informatiebeveiliging onder het beheerproces van de bedrijfscontinuïteit valt of onder het beheerproces van rampenherstel. Informatiebeveiligingseisen behoren te worden vastgesteld als (ook) de planning voor bedrijfscontinuïteit en rampenherstel wordt gemaakt. Bij afwezigheid van een formele planning voor bedrijfscontinuïteit en rampenherstel behoort het informatiebeveiligingsbeheer ervan uit te gaan dat informatiebeveiligingseisen in ongunstige situaties hetzelfde blijven als in normale uitvoeringsomstandigheden. In het andere geval kan een organisatie een bedrijfsimpact analyse (BIA) uitvoeren voor informatiebeveiligingsaspecten om de informatiebeveiligingseisen vast te stellen die van toepassing zijn op ongunstige situaties.
2. [A]Calamiteitenplannen worden gebruikt in de periodieke bewustwording-, training- en testactiviteiten.

17.1.2 Informatiebeveiligingscontinuïteit implementeren

Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen de interne organisatie afgesproken tijd te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

1. In de continuïteitsplannen wordt minimaal aandacht besteed aan:

- Communicatie intern en externe bereikbaarheid;
- Identificatie van essentiële procedures voor bedrijfscontinuïteit;
- Wie mag het continuïteitsplan wanneer activeren;
- Wanneer wordt er gecontroleerd teruggegaan naar de standaard situatie;
- Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
- Prioriteiten en volgorde van herstel en reconstructie;
- Documentatie van systemen en processen;
- Kennis en kundigheid van personeel om de processen weer op te starten.

17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

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

1. [A]Er worden periodiek oefeningen en/of testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.
2. Veranderingen betreffende de organisatie, procedures, processen of van technische aard, hetzij in een context van uitvoering, hetzij van continuïteit, kunnen leiden tot veranderingen in de eisen betreffende informatiebeveiligingscontinuïteit. In dergelijke gevallen behoort de continuïteit van processen, procedures en beheersmaatregelen voor informatiebeveiliging te worden beoordeeld tegen de achtergrond van deze veranderde eisen.
3. Organisaties behoren de continuïteit van hun informatiebeveiligingsbeheer te verifiëren door:
    a. de functionaliteit van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te oefenen en te testen om te waarborgen dat ze consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit;
    b. de kennis en routine voor het uitvoeren van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te oefenen en te testen om te waarborgen dat de prestaties consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit;
    c. de deugdelijkheid en doeltreffendheid van maatregelen voor informatiebeveiligingscontinuïteit te beoordelen als informatiesystemen, informatiebeveiligingsprocessen, -procedures en -beheersmaatregelen, of de procedures en oplossingen van bedrijfscontinuïteitsbeheer of rampenherstelbeheer veranderen.

17.2 Redundante componenten

Doelstelling
Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

17.2.1 Beschikbaarheid van informatie verwerkende faciliteiten

Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

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

Indien van toepassing behoren redundante informatiesystemen te worden getest om te waarborgen dat de automatische omschakeling van de ene op de andere component bij storing werkt zoals voorzien.

18. Naleving

18.1 Naleving van wettelijke voorschriften

Doelstelling

Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.

18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen

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

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

Managers behoren alle wetgeving die toepasselijk is op hun organisatie vast te stellen om te voldoen aan de eisen voor hun soort bedrijfsactiviteit.

18.1.2 Intellectuele eigendomsrechten

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.

1. Er is toezicht op het naleven van wettelijke verplichtingen m.b.t. intellectueel eigendom, auteursrechten en gebruiksrechten.

18.1.3 Bescherming van registraties

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

Bij besluitvorming over bescherming van specifieke registraties van de organisatie behoort de classificatie daarvan, gebaseerd op het classificatieschema van de organisatie, in overweging te worden genomen.

Registraties behoren te worden gecategoriseerd naar type, bijvoorbeeld boekhoudkundige registraties, databaserecords, transactielogbestanden, auditlogbestanden en operationele procedures. Bij elk type behoort de bewaartermijn en toegestane soorten opslagmedia te worden vermeld, bijvoorbeeld papier, microfiche, magnetische of optische opslag.

Gerelateerde cryptografische sleutels en programma's die samenhangen met versleutelde archieven of digitale handtekeningen (zie hoofdstuk 10), behoren ook te

worden bewaard om decodering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties.

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

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

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

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

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

a. er behoren richtlijnen te worden verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie;
b. er behoort een bewaarschema te worden opgesteld waarin registraties en de periode dat ze moeten worden bewaard, zijn vastgelegd;
c. er behoort een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.

18.1.4 Privacy en bescherming van persoonsgegevens

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

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

Naleving van dit beleid en van alle relevante wet- en regelgeving betreffende het beschermen van de privacy van personen en de bescherming van persoonsgegevens vereist een geschikte beheerstructuur en beheersing. Vaak kan dit het beste worden bereikt door een persoon te benoemen die hiervoor verantwoordelijk is, zoals een Functionaris Gegevensbescherming (FG) of een Privacy Officer, die richtlijnen behoort te geven aan managers, gebruikers en aanbieders van diensten over hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Het toewijzen van verantwoordelijkheid voor het hanteren van persoonsgegevens en

het waarborgen dat medewerkers zich bewust zijn van de privacy principes behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving zoals de AVG. Er behoren passende technische en organisatorische maatregelen te worden geïmplementeerd om persoonsgegevens te beschermen (art.32, AVG).

De Europese verordening AVG (= Algemene Verordening Gegevensbescherming) heeft de meldingsplicht vervangen door een verantwoordingsplicht en geeft een administratieve verzwaring voor verantwoordelijken en verwerkers. De belangrijkste veranderingen betreffen de verplichte transparantie en verstevigde rechten van betrokkenen zoals bijvoorbeeld de controlemogelijkheden voor bijvoorbeeld de huurder waar het de verwerking van zijn gegevens betreft. Dit betekent aangescherpte verplichtingen van de verantwoordelijken, met name op het punt van:

- informatievoorziening over de inrichting van de gegevenshuishouding;
- de wijze waarop de verantwoordelijke bijdraagt aan de uitoefening van de (inzage) rechten van bijvoorbeeld de huurder;
- de toegepaste beveiliging en daarbij gemaakte afwegingen bij verschillende soorten gegevensverwerkingen met betrekking tot het inrichten van werkprocessen, toepassen van principes als Privacy by design en privacy-enhancing technologies en het cyclisch verbeteren van de beveiliging;
- meldplicht datalekken bij al dan niet gebleken inbreuken op de beveiliging;
- 100% accountability voor het voldoen aan deze verplichtingen.
- het in dienst nemen van een Functionaris gegevensbescherming (FG), dat is een interne toezichthouder, wanneer de verwerkingsverantwoordelijke een overheids- of bestuursorgaan is, meer dan 250 medewerkers in dienst heeft dan wel een particuliere onderneming die verwerkingen van persoonsgegevens verricht die aan bepaalde kenmerken voldoen (qua omvang, gevoeligheid).

Verder is er sprake van verscherping van het toezicht door de toezichthouder (Autoriteit Persoonsgegevens) en zijn diens sanctiemogelijkheden fors uitgebreid.

18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

1. Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen.

18.2 Informatiebeveiligingsbeoordelingen

Doelstelling

Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

18.2.1 Onafhankelijke beoordeling van informatiebeveiliging

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid,

processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.

1. [A]Het informatiebeveiligingsbeleid wordt periodiek geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld.
2. [A]Periodieke beveiligingsaudits worden uitgevoerd in opdracht van de directie/het management.
3. Over het functioneren van de informatiebeveiliging wordt, conform de Planning & Control cyclus, jaarlijks gerapporteerd aan het management/de directie.

18.2.2 Naleving van beveiligingsbeleid en -normen

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

1. Het management/de directie is verantwoordelijk voor de uitvoering en de beveiligingsprocedures en de toetsing daarop. Conform deze Baseline zorgt de Coördinator Informatiebeveiliging, namens de organisatie, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of in opdracht van de Coördinator Informatiebeveiliging, dan wel door interne of externe auditteams.
2. [A]In de Planning & Control cyclus wordt gerapporteerd over informatiebeveiliging.

18.2.3 Beoordeling van technische naleving

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

1. Technische naleving behoort bij voorkeur te worden beoordeeld met behulp van geautomatiseerde instrumenten die technische rapporten vervaardigen, die vervolgens door een technisch specialist worden geïnterpreteerd. Als alternatief kunnen handmatige beoordelingen (indien nodig ondersteund door passende software-instrumenten) door een ervaren systeemtechnicus worden uitgevoerd.
2. Indien penetratietests of kwetsbaarheidsbeoordelingen worden toegepast is voorzichtigheid geboden omdat dergelijke activiteiten de beveiliging van het systeem kunnen compromitteren. Dergelijke tests behoren te worden gepland en gedocumenteerd en behoren herhaalbaar te zijn.
3. Beoordeling van technische naleving behoort uitsluitend te worden uitgevoerd door competente, bevoegde personen of onder toezicht van dergelijke personen.

Overige informatie

1. Beoordelingen van technische naleving omvatten onderzoek van productiesystemen om te waarborgen dat beheersmaatregelen voor hardware en software correct zijn geïmplementeerd. Dit soort beoordeling van naleving vereist specialistische technische expertise.
2. Beoordelingen van naleving behelzen bijvoorbeeld ook penetratietests en kwetsbaarheidsbeoordelingen die kunnen worden uitgevoerd door onafhankelijke deskundigen die specifiek voor dit doel zijn gecontracteerd.
3. Dit kan nuttig zijn om in het systeem kwetsbaarheden op te sporen en om te onderzoeken hoe doeltreffend de beheersmaatregelen zijn in het voorkomen van

onbevoegde toegang als gevolg van deze kwetsbaarheden. Penetratietests en kwetsbaarheidsbeoordelingen geven een momentopname van een systeem in een bepaalde staat op een bepaald moment. De momentopname is beperkt tot die delen van het systeem die werkelijk tijdens de penetratiepoging(en) zijn getest.

4. Penetratietests en kwetsbaarheidsbeoordelingen zijn geen vervanging van een risicobeoordeling.

Bijlage A: Begrippen

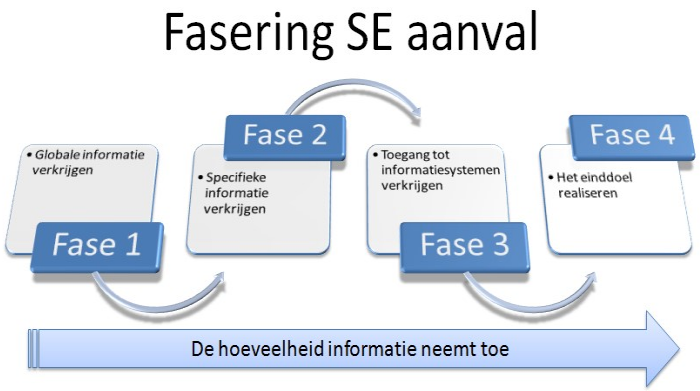
Audit trail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
A&K analyse	Een analyse methode om de afhankelijkheden en kwetsbaarheden in kaart te brengen.
Anonimiseren	Indien persoonsgegevens worden geanonimiseerd zijn de gegevens niet meer te herleiden tot natuurlijke personen. Dit in tegenstelling tot pseudonimiseren waarbij via een zogenaamd "koppelbestand" de identiteit van de natuurlijke persoon nog wel valt te achterhalen.
Basis beveiligingsniveau	Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuïty Management en waaraan de BIC een nadere uitwerking geeft, onder meer door normen voor ICT-voorzieningen.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen en informatiesystemen.
Betrokkene	De betrokkene is in de AVG wetgeving de persoon van wie persoonsgegevens zijn vastgelegd, worden onderhouden, bewerkt, doorgegeven of verwijderd.
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuity Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijvoorbeeld onbevoegde toegang tot ICT voorzieningen.
Beveiligings-instellingen	In ICT-voorzieningen kunnen in veel gevallen functionaliteit - die invloed heeft op beveiliging - geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.

Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere werkelijkheden of representaties daarvan, zodat objectieve oordeelsvorming mogelijk wordt.
Datalek	Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie.
Elektronische handtekening	Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van technieken van de asymmetrische cryptografie. De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie 'ondertekent'. De technieken worden toegepast met behulp van een PKI.
Filtering	Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.
Firewall	Het geheel van software en eventueel ook hardware voorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de veiligheid in de laatstgenoemde te verhogen.
Hardening	Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
IB-functie	Een geheel van automatische informatiebeveiligingsverwerkingen die logisch met elkaar samenhangen.
ICT-voorzieningen	Applicaties en technische infrastructuur, of wel het geheel van ICT-voorzieningen.

In control statement	Binnen de gebruikelijke Planning en Control cyclus moet door de Bestuurder een in control statement worden afgegeven over het BIC. De in control verklaring moet inzicht geven aan welke BIC normen wordt voldaan en voor welke BIC normen een explain ('leg uit') is gedefinieerd.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Integrale beveiliging	Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen (TBB) door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de woningcorporaties: het management is integraal verantwoordelijk en dus ook voor de beveiliging van de TBB.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Logging	Vastlegging van systeemhandelingen.
Malware	Software met ongewenste functies, zoals virussen en trojans.
Mobile code	Code afkomstig van een ander systeem die lokaal uitgevoerd wordt, bijvoorbeeld Javascript, Flash of Silverlight.
Niet-vertrouwd	Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau.
Onweerlegbaarheid	Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).

Patch	Klein onderdeel van software dat de leverancier van software uitgeeft om fouten in door hem vervaardigde software te repareren.
Persoonsgegevens	Een persoonsgegeven is een gegeven aan de hand waarvan een persoon kan worden geïdentificeerd. Een persoon *kan* worden geïdentificeerd als degene die het persoonsgegeven gebruikt de persoon kan identificeren zonder een bijzondere inspanning te leveren. Er zijn drie soorten persoonsgegevens: 1. Persoonsgegevens 2. Bijzondere persoonsgegevens 3. Gevoelige persoonsgegevens
Privacy by Default/ Privacy by Design	We spreken van *Privacy by Default* als de instellingen van een programma, app, website of dienst zodanig zijn dat maximale privacy wordt betracht. Let wel: dat is de maximale stand van dat programma of die dienst. Het kan zijn dat het absoluut gezien niet bijzonder privacyvriendelijk is. Het gaat niet alleen om opties die kunnen worden ingesteld, ook zaken als algemene voorwaarden moeten privacyvriendelijk zijn. Dus geen verstopte privacy-onderwerpen op een plek waar ze niet thuishoren. Geen opt-out regime, maar opt-in: pas als iemand zich ergens voor heeft aangemeld ontvangt hij informatie (opt-in), niet het automatisch ontvangen totdat het wordt stopgezet (opt-out). Privacy by Default wordt vaak in verband gebracht met *Privacy by Design*. Het zijn verwante begrippen; Privacy by Design geeft aan dat privacy bij het ontwikkelen van informatiesystemen en diensten vanaf het begin moet worden omarmd. Privacy by Default en Privacy by Design zijn als concept verankerd in artikel 23 van de Algemene Verordening Gegevensbescherming (AVG).
Pseudonimiseren	Indien persoonsgegevens worden geanonimiseerd zijn de gegevens niet meer te herleiden tot natuurlijke personen. Dit in tegenstelling tot pseudonimiseren waarbij via een zogenaamd "koppelbestand" de identiteit van de natuurlijke persoon nog wel valt te achterhalen.
Query	Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie alleen voor raadpleegdoeleinden.

Social Engineering	Bij social engineering wordt gebruik gemaakt van kwaadwillende personen om van medewerkers informatie te ontfutselen. Dit kan gaan om bedrijfsgeheimen of informatie die niet voor iedereen bestemd is uit woningcorporatie systemen. Denk hier aan bijvoorbeeld wachtwoorden, ontwikkelingsplannen, verblijfplaatsen van mensen. De social engineer maakt gebruik van zwakheden in de mens om zijn doel te bereiken. Meestal is men zich hier niet goed van bewust. Het is heel normaal om een onbekende op de gang aan te spreken en te vragen of ze hulp nodig hebben. Toch hebben veel mensen hier moeite mee en gebeurt het niet. Het is ook goed om je af te vragen met wie je spreekt aan de telefoon en jezelf de vraag te stellen 'waarom wordt me deze vraag gesteld'. Fasering Social Engineer (SE) aanval:



Bedenk dat een social engineer van buiten en van binnen kan komen.

Security by Design	Het vanaf het ontwerp van programmatuur al inbouwen en voorzien van informatiebeveiliging.
Technische infrastructuur	Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.

Two-factor authenticatie	Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: • Iets dat de gebruiker weet (bijvoorbeeld password, PIN); • Iets dat de gebruiker heeft (bijvoorbeeld toegangspas, sleutel); en • Iets dat de gebruiker is (bijvoorbeeld biometrische eigenschap zoals een vingerafdruk).
Verantwoordelijke	De verantwoordelijke is in de context AVG wetgeving diegene die (eind)verantwoordelijk is voor de aan haar toevertrouwde persoonsgegevens van individuele personen. De verantwoordelijke is een natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Vertrouwd	In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken.
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie	Informatie die niet algemeen bekend mag worden (bron: van Dale). In het kader van de BIC worden maatregelen beschreven die voldoen voor de behandeling van geclassificeerde informatie tot en met persoonsgegevens en bijzondere persoonsgegevens..
Verwijderbare media	Opslagmiddelen die van apparatuur kunnen worden verwijderd en meegenomen. Zoals CD-ROM, USB stick, verwijderbare schijven, tapes of gedrukte media.
Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen