TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

# Informatiebeveiligingsbeleid

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

## Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Voorbeeld Informatiebeveiligingsbeleid Gemeenten’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

## Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

### Doel

Dit document beschrijft een voorbeeld voor de invulling van het informatiebeveiligingsbeleid door organisaties binnen de Rijksoverheid. Aan de hand van dit voorbeelddocument kan een overheidsorganisatie het eigen informatiebeveiligingsbeleid ontwikkelen. De uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

### Doelgroep

Dit document is relevant voor auteurs van het beveiligingsbeleid van de eigen organisatie. Het beleid zelf richt zich op de volledige organisatie en daarmee alle medewerkers van overheidsorganisaties.

### Reikwijdte

Dit document heeft voornamelijk betrekking op maatregel 5.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische aspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot informatiebeveiligingsbeleid.

### Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR).
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007).
- GAP-analyse.

## Inhoudsopgave

# I. Inleiding

Dit document geeft een voorbeeld voor de invulling van informatiebeveiligingsbeleid voor organisaties binnen de Rijksoverheid. Aan de hand van dit voorbeelddocument kan een overheidsorganisatie het eigen informatiebeveiligingsbeleid ontwikkelen. Het beschreven beleid is gebaseerd op de BIR. Een organisatie kan binnen de kaders van wet- en regelgeving eigen invulling geven aan uitgangspunten, doelstellingen of maatregelen in het informatiebeveiligingsbeleid. Ook kunnen risicoanalyses aanleiding geven tot het nemen van additionele beveiligingsmaatregelen.

In dit document zijn een groot aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen die voor alle processen en systemen van organisaties kunnen gelden. Een beheerstructuur voor informatiebeveiliging (IB) maakt onderdeel uit van dit document. Hiermee worden verantwoordelijkheden voor informatiebeveiliging belegd en wordt informatiebeveiliging ingebed in de reguliere planning- en controlcyclus van de organisatie.

Dit voorbeelddocument is gebaseerd op de volgende hoofdstukken van de Baseline Informatiebeveiliging Rijksdienst:

- 5 Informatiebeveiligingsbeleid;
- 6 Organisatie van informatiebeveiliging;
- 7 Beheer van bedrijfsmiddelen;
- 8 Beveiliging van personeel;
- 9 Fysieke beveiliging en beveiliging van de omgeving;
- 10 Beheer van communicatie- en bedieningsprocessen;
- 11 Toegangsbeveiliging;
- 12 Verwerving, ontwikkeling en onderhoud van informatiesystemen;
- 13 Beheer van informatiebeveiligingsincidenten;
- 14 Bedrijfscontinuïteitsbeheer;
- 15 Naleving.

## Informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Het begrip ‘informatiebeveiliging’ heeft betrekking op:

- *beschikbaarheid / continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;

- *vertrouwelijkheid / exclusiviteit*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

### Waarom informatie beveiligen?

Informatie is één van de belangrijkste bedrijfsmiddelen van een organisatie. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een organisatie die zich verantwoordelijk gedraagt, en aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en die met minimale middelen, maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

### Reikwijdte en afbakening informatiebeveiliging

Informatiebeveiliging is 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 informatieverwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook 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.

### Opbouw document

Dit document bestaat uit twee delen: (1) een voorbeeld voor informatiebeveiligingsbeleid in hoofdstuk 1, en; (2) voorbeelden van concrete beleidsmaatregelen bij dit informatiebeveiligingsbeleid op basis van de BIR in hoofdstuk 2 tot en met 11.

## 1. Informatiebeveiligingsbeleid <organisatie>

Het management van de organisatie is verantwoordelijk voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van het informatiebeveiligingsbeleid van de organisatie. Het management maakt een inschatting van het belang en de risico's van verschillende delen van de informatievoorziening voor de organisatie. Het management bepaalt welke risico's acceptabel en niet acceptabel zijn.

Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, inclusief alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid past binnen het algemene beleid van de organisatie en wet- en regelgeving. Dit beleid bevat een bijlage met nadere aanwijzingen.

De <organisatie> is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- De organisatie moet voldoen aan wet- en regelgeving, zoals (niet-uitputtend): Wbp en het VIR.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Rijksdienst (BIR).
- De organisatie stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit'-principe.

Het informatiebeveiligingsbeleid is gebaseerd op de volgende uitgangspunten, welke zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIR:

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de organisatie. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn-) management, met het **verantwoordelijke bestuurder als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door **periodieke controle, organisatie brede planning en coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3. Informatiebeveiliging is een **continue verbeterproces**. 'Plan, do, check en act' vormen samen het **managementsysteem** van informatiebeveiliging.
4. De **informatiebeveiligingsfunctionaris**/Chief Information Security Officer (CISO) ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en

verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.

5. De organisatie stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
6. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de organisatie worden getraind in het gebruik van beveiligingsprocedures.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het bestuur. Hiermee komt het oude informatiebeveiligingsbeleid van de <organisatie> van <jaar> te vervallen.

Aldus vastgesteld door de bestuurlijk verantwoordelijke van *[organisatie]* op *[datum],*

[Naam. Functie] [Naam. Functie]

## 2. Uitgangspunten informatiebeveiliging <organisatie>

### 2.1 Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van de <organisatie>. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de primaire taakuitvoering, de bedrijfsvoering en leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie en de bestuurders. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

### 2.2 Visie

*De komende jaren zet de <organisatie> in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de organisatie en de basis voor het beschermen van rechten van burgers en bedrijven.[1] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.*

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie. Tegelijkertijd is informatiebeveiliging een ‘enabler’: het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus van informatiebeveiliging ligt op informatie-uitwisseling in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie. Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.[2]

### 2.3 Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende personele, organisatorische en technische maatregelen om informatie te beschermen en te waarborgen, zodat de organisatie voldoet aan relevante wet- en regelgeving. <organisatie> streeft er naar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent dat de organisatie weet welke maatregelen genomen zijn en dat er een SMART-

[1] Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.
[2] Medewerker = (1) ambtenaar in de zin van het ARAR of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor de <organisatie> verricht.

planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

## 2.4 Uitgangspunten

1. Het informatiebeveiligingsbeleid van <organisatie> is in lijn met het algemene beleid van de organisatie en de relevante wet- en regelgeving.[3]
2. Het beleid is gebaseerd op de BIR die is afgeleid van de Code voor Informatiebeveiliging (NEN/ISO 27002).
3. Het informatiebeveiligingsbeleid wordt vastgesteld door de bestuurlijk eindverantwoordelijke. Het beleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zonodig bijgesteld.

## 2.5 Risicobenadering

De aanpak van informatiebeveiliging van <organisatie> is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Rijksdienst (BIR). Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: **risico = kans x impact**.

## 2.6 Doelgroepen

Het informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers van de organisatie:

| Doelgroep | Relevantie voor informatiebeveiligingsbeleid |
|---|---|
| Directie | Integrale verantwoordelijkheid |
| Bestuurlijk verantwoordelijke[4] | Verantwoordelijkheid kaderstelling en implementatie |
| CISO (of beveiligingsfunctionaris)[5] | Functionele sturing op de kaderstelling en implementatie |
| Lijnmanagement (proceseigenaren) | Sturing op informatieveiligheid en controle op naleving |

[3] Daarbij geldt het 'comply or explain' principe (pas toe of leg uit).
[4] Afhankelijk van keuze van de directie is de verantwoordelijkheid binnen de directie belegd bij één van de directieleden.
[5] In kleinere organisaties kan de rol van CISO zijn ingevuld door de bestuurlijk verantwoordelijke binnen de directie.

| | |
|---|---|
| Medewerkers | Gedrag en naleving |
| Gegevenseigenaren | Classificatie: verantwoordelijkheid voor de beschermingseisen van informatie |
| Beleidmakers | Planvorming binnen IB-kaders |
| IB-functionarissen | Dagelijkse coördinatie van IB |
| Personeelszaken | Arbeidsvoorwaardelijke zaken |
| Facilitaire zaken | Fysieke toegangsbeveiliging |
| ICT-diensten (en -ontwikkelaars) | Technische beveiliging |
| Auditors | Onafhankelijke toetsing |
| Leveranciers en ketenpartners | Compliance |

### 2.7 Scope

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de organisatie en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit informatiebeveiligingsbeleid stelt algemene beleidskaders. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.

### 2.8 Informatiebeveiligingsbeleid en architectuur

IB is onderdeel van het architectuurbeleid. Dit architectuurbeleid beschrijft onder meer principes, richtlijnen en maatregelen op basis van verschillende beschermingsniveaus (classificatie).

### 2.9 Werking

Dit informatiebeveiligingsbeleid is in werking getreden na vaststelling door de directie. Hiermee komt het oude informatiebeveiligingsbeleid van de <organisatie> van <jaar> te vervallen.

# 3. Organisatie van de informatiebeveiliging

## 3.1 Interne organisatie

### 3.1.1 Risico's

- Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, verhindert het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.

### 3.1.2 Doelstelling:

*Beheersen van de informatiebeveiliging (IB) binnen de organisatie.*

*Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.*

*Goedkeuring door de directie, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.*

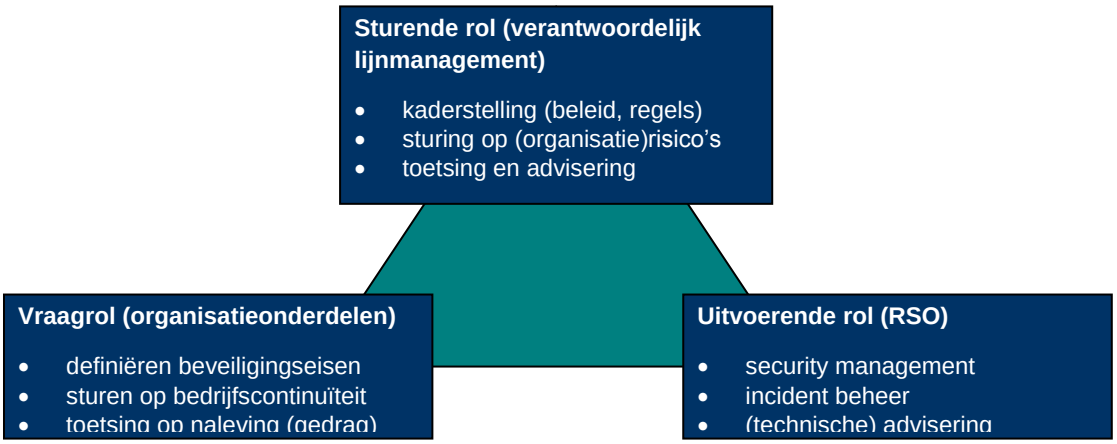
### 3.1.3 Verantwoordelijkheden

- De directie is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van <organisatie>[6], en
  - stelt kaders voor informatiebeveiliging (IB) op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;
- De bestuurlijk verantwoordelijke is verantwoordelijk voor het opstellen van de kaders en de bewaking van de implementatie.
- De CISO is namens de bestuurlijk eindverantwoordelijke (functioneel) verantwoordelijk voor de realisatie kaderstelling en sturing.
  De CISO stuurt namens de bestuurlijk eindverantwoordelijke:[7]
  - op concern risico's;
  - controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij.
- Organisatieonderdelen binnen de organisatie (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging.[8]
  Het lijnmanagement:

[6] Zie ook: Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007).
[7] Met betrekking tot de i-functie geeft de CIO op dagelijkse basis namens de bestuurlijk verantwoordelijke invulling aan de sturende rol door besluitvorming door de bestuurlijk verantwoordelijke voor te bereiden en toe te zien op de uitvoering ervan.
[8] Zie ook: Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007).

- stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie);
- is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de organisatie in de managementrapportages.

- De serviceorganisatie of gelijkwaardig (ICT, HR, bedrijfsvoering, etc., in uitvoerende rol) is verantwoordelijk voor uitvoering.[9]
  De serviceorganisatie:
  - is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
  - is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
  - verzorgt logging, monitoring en rapportage;
  - levert klanten (technisch) beveiligingsadvies.




**Figuur 1: relaties**

**Taken en rollen**

## 3.2 Taken en rollen

- De bestuurlijk eindverantwoordelijke stelt formeel het informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden door de verantwoordelijke interne of externe toezichthouder.

[9] Let op, de serviceorganisatie, stafdienst, afdeling bedrijfsvoering is tegelijk ook klant, het gaat hier echter om de uitvoerende rol.

- De CIO (Chief Information Officer) of vergelijkbare rol geeft namens de bestuurlijk eindverantwoordelijke op dagelijkse basis invulling aan de sturende rol door besluitvorming van de bestuurlijk eindverantwoordelijke voor te bereiden en toe te zien op de uitvoering ervan. De IB taken die hieruit voortvloeien zijn belegd bij de 'Chief Information Security Officer' (CISO). De CISO bevordert en adviseert gevraagd en ongevraagd over IB en rapporteert eens per kwartaal concernbreed aan de bestuurlijk verantwoordelijke over de stand van zaken.
- De coördinatie van informatiebeveiliging is belegd bij een strategische adviesfunctie binnen alle afdelingen. Uitvoerende taken zijn zoveel mogelijk belegd bij (decentrale) IB-functionarissen. De afdelingen rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de Planning & Controlcyclus.
- De (ICT-)serviceorganisatie heeft een security functionaris aangesteld voor dagelijks beheer van technische IB-aspecten. De security functionaris rapporteert aan de CISO. Informatiebeveiliging is onderdeel van de service management rapportage.

| Wie | Plan:<br><br>Kaderstelling | Do:<br><br>Uitvoering | Check:<br><br>Controle | Act:<br><br>Verbetering |
|---|---|---|---|---|
| Sturen:<br><br>Directie dagelijkse uitvoering:<br><br>CIO/CISO | Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning. | Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons. | Controle, audit, pentesten. | Bijsturen: opdrachtverstrekking voor verbeteracties.<br><br>Rapportage aan directie |
| Vragen:<br><br>Alle afdelingen | Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen. | Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management. | Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy. | Verbeteren bedrijfscontinuïteit. Rapportage aan CIO/CISO. |
| Uitvoeren:<br><br>Service organisatie (in uit-voerende rol) | Beleidsvoorbereiding, technische onderzoeken (marktverkenningen). | Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies. | Vulnerability scanning, evaluatie en rapportage. | Uitvoeren verbeteracties.<br><br>Advies aan de CIO/CISO over aanpassingen aan de informatievoorziening. |

### 3.3 Functioneel overleg

De CISO of beveiligingsfunctionaris stelt een interne organisatie voor van beveiliging gerelateerde functionarissen binnen de organisatie en de CISO organiseert tenminste eenmaal per kwartaal een (security) overleg met dit gremium. De

CISO/beveiligingsfunctionaris is voorzitter. Het overleg heeft binnen de organisatie een adviesfunctie richting de CIO of gelijkwaardig en richt zich met name op beleid en adviseert over strategische en/of tactische informatiebeveiliging kwesties.

Het onderwerp Informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van het lijnoverleg zodat er sturing plaatsvindt op de uitgevoerde activiteiten.

### 3.4 Rapportage en escalatielijn voor IB

(Decentrale) Security verantwoordelijke → CISO (→ CIO)[10] → (Bestuurlijk verantwoordelijke)[11] → directie[12]

### 3.5 Externe partijen

- Informatiebeveiligingsbeleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de organisatie samenwerkt (en informatie mee uitwisselt).[13] Ook voor externe partijen geldt hierbij het 'pas toe of leg uit'-beginsel.
- Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV dienen te worden getoetst aan informatiebeveiligingsbeleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de organisatie het recht heeft afspraken te (laten) controleren.[14]
- Voor het tot stand brengen van datakoppelingen met externe partijen, geldt naast generiek informatiebeveiligingsbeleid een procedure 'Aanvragen externe toegang Intranet'. Het doel van de procedure is risicobeheersing.
- Voor externe hosting van data en/of services gelden naast generiek informatiebeveiligingsbeleid de richtlijnen voor cloud computing.[15] De organisatie is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door de externe partij(en);
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens;[16]
  - melding bij het College bescherming persoonsgegevens (CBP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

---

[10] Afhankelik van de omvang van de ophanging van de CISO rapporteert de CISO aan de CIO of de bestuurlijk verantwoordelijke of de directie.
[11] Afhandelijk van hoe de verantwoordelijkheid binnen de directie is belegd, wordt aan de bestuurlijk verantwoordelijke of de directie gerapporteerd.
[12] De CIO is adviseur van de bestuurlijk verantwoordelijke.
[13] Beleidsregels voor externe partijen zijn beschreven in de BIR.
[14] Hiervoor kan gebruik worden gemaakt van een 'third party mededeling' (TPM) of een ISAE 3402-verklaring.
[15] Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[16] Ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen.

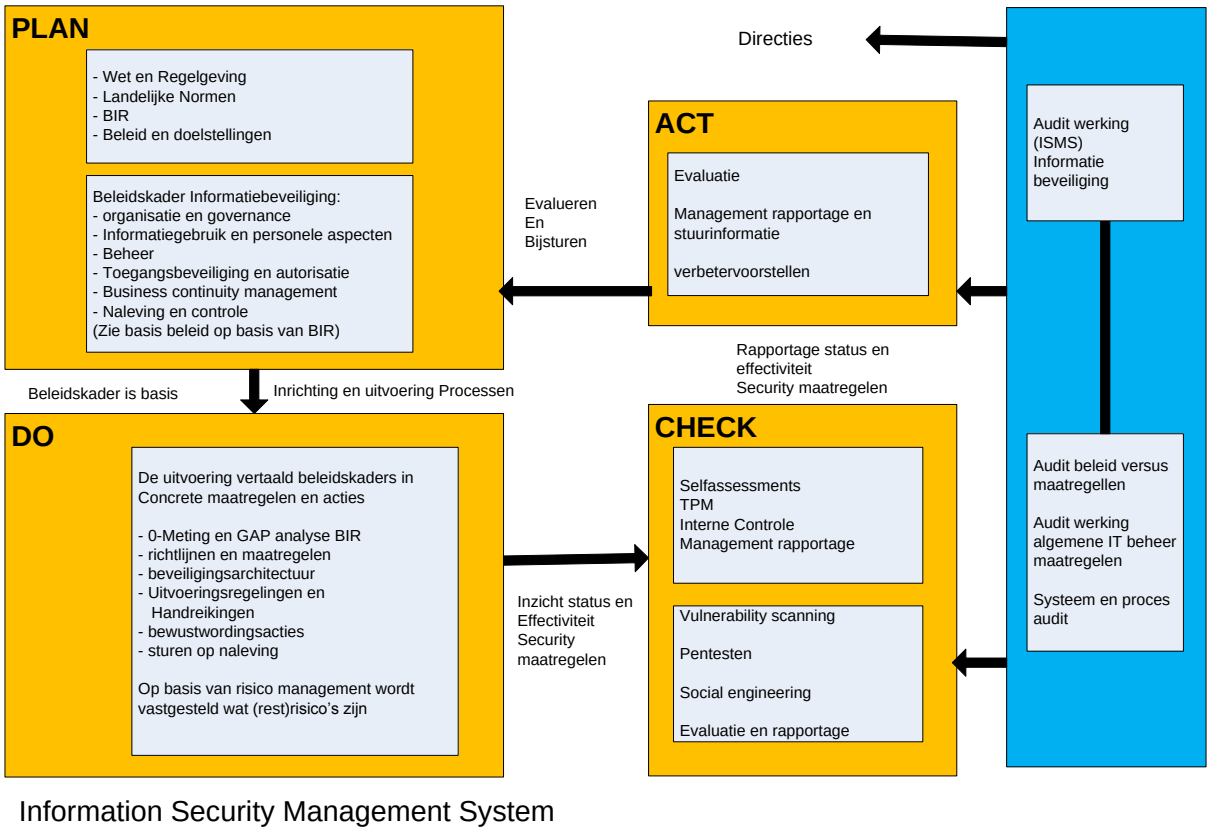
### 3.6 ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing dient een kernteam IB geïnstalleerd te zijn, bestaande uit een bestuurlijk verantwoordelijke, de CISO of functionaris informatiebeveiliging, security functionaris ICT-serviceorganisatie, relevante experts en de communicatieafdeling. De werkwijze dient te zijn vastgelegd.
- <organisatie> participeert in relevante landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde IB-platforms.

### 3.7 PDCA

- Informatiebeveiliging is een continu verbeterproces. De 'Plan, do, check en act'-methodiek vormt samen het managementsysteem van informatiebeveiliging.[17] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.
- Toelichting figuur 2:
  - Plan: De cyclus start met informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Rijksdienst (BIR) en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het CIO/ICT-jaarplan en uitgewerkt in het informatiebeveiligingsplan van organisatie. Afdelingsspecifieke activiteiten worden gepland in het afdelings-IB plan of het afdelingsinformatieplan (IM-functie).
  - Do: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
  - Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.
    - Externe controle: betreft controle buiten het primaire proces door een auditor.[18] Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd, waarbij de CIO/ICT in principe opdrachtgever is. Bevindingen worden gerapporteerd aan de CIO en de bestuurlijke verantwoordelijke.
  - Act: De cyclus is rond met de uitvoering van verbeteracties op basis van check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan de bestuurlijk verantwoordelijke. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

[17] NEN/ISO 27001.
[18] Van onder meer de accountant, Rijksoverheid (voor bijv. basisregistraties) en auditors (intern).




**Figuur 2: Information Security Management System**

# 4. Beheer van bedrijfsmiddelen

## 4.1 Verantwoordelijkheid voor bedrijfsmiddelen

### 4.1.1 Risico's:

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's, zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

### 4.1.2 Doelstellingen

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

*Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.*

### 4.1.3 Beheersmaatregelen

- Alle bedrijfsmiddelen moeten zijn geïdentificeerd in een inventaris.
- Alle informatie en bedrijfsmiddelen, die verband houden met ICT-voorzieningen, aan een 'eigenaar' (een deel van de organisatie) toewijzen.
- Regels vaststellen, documenteren implementeren voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en andere informatie van de organisatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de organisatie te waarborgen.
- Medewerkers gebruiken informatie van de organisatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van zakelijke informatie en bestanden is niet toegestaan.
- Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:
  - Illegale software mag niet worden gebruikt voor de uitvoering van het werk.
  - Er bestaat geen plicht de eigen computer te beveiligen, maar de informatie daarop wel.
  - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.
- De medewerker neemt passende technische en organisatorische maatregelen om zakelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:

- de beveiligingsclassificatie van de informatie (zie hieronder);
- de door de organisatie gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
- aan de werkplek verbonden risico's;
- het risico door het benaderen van informatie van de organisatie met andere dan door de organisatie verstrekte of goedgekeurde ICT-apparatuur.

### 4.2 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van processen en informatiesystemen worden beveiligingsclassificaties gebruikt.[19] Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV).

Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

### 4.3 Risico's:

- Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de bedrijfsprocessen.
- Onjuiste classificatie draagt bij aan het onjuist beschermen van informatie en bedrijfsmiddelen met als risico dat deze verloren kunnen gaan of openbaar worden gemaakt, terwijl dat niet de bedoeling is.

### 4.4 Doelstellingen

*Informatie heeft een geschikt niveau van bescherming.*

*Classificatie van informatie om bij verwerking de noodzaak en bescherming te kunnen aangeven.*

*Adequate niveaus van bescherming van informatie zijn gedefinieerd en de noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.*

### 4.5 Beheersmaatregelen

- Informatie classificeren met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Opstellen en uitdragen classificatiebeleid binnen de organisatie.

[19] Dit is in detail beschreven in de component architectuur Informatiebeveiliging 2014, CIO, 2014.

- Er dienen geschikte samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de classificering en verwerking van informatie overeenkomstig het classificatiesysteem dat is vastgesteld.

| Niveau | Vertrouwelijkheid | Integriteit | Beschikbaarheid |
|---|---|---|---|
| Geen | **Openbaar**<br><br>informatie mag door iedereen worden ingezien<br><br>*(bv: algemene informatie op de externe website van de organisatie* | **Niet zeker**<br><br>informatie mag worden veranderd<br><br>*(bv: templates en sjablonen)* | **Niet nodig**<br><br>gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn<br><br>*(bv: ondersteunende tools als routeplanner)* |
| Laag | **Bedrijfsvertrouwelijk**<br><br>informatie is toegankelijk voor alle medewerkers van de organisatie<br><br>*(bv: informatie op het intranet)* | **Beschermd**<br><br>het bedrijfsproces staat enkele (integriteits-) fouten toe<br><br>*(bv: rapportages)* | **Noodzakelijk**<br><br>informatie mag incidenteel niet beschikbaar zijn<br><br>*(bv: administratieve gegevens)* |
| Midden | **Vertrouwelijk**<br><br>informatie is alleen toegankelijk voor een beperkte groep gebruikers<br><br>*(bv: persoonsgegevens, financiële gegevens* | **Hoog**<br><br>het bedrijfsproces staat zeer weinig fouten toe<br><br>*(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)* | **Belangrijk**<br><br>informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk<br><br>*(bv: primaire proces informatie)* |
| Hoog | **Geheim**<br><br>informatie is alleen toegankelijk voor direct geadresseerde(n)<br><br>*(bv: zorggegevens en strafrechtelijke informatie)* | **Absoluut**<br><br>het bedrijfsproces staat geen fouten toe<br><br>*(bv: informatie op de website)* | **Essentieel**<br><br>informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten<br><br>*(bv: basisregistraties)* |

## 4.6 Uitgangspunten

- De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.
- Het object van classificatie is informatie. Classificatie vindt plaats op het niveau van informatiesystemen (of informatieservices). Alle classificaties van alle bedrijfskritische

systemen zijn centraal vastgelegd door de CISO en dienen jaarlijks gecontroleerd te worden door de eigenaren.

- Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn.
- De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen, wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt tevens wie toegang krijgt tot welke gegevens.
- Er wordt gestreefd naar een zo ‘laag’ mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar te zijn (transparante overheid).
- Er wordt gestreefd naar een balans tussen het te lopen risico en de kosten van tegenmaatregelen. Daarbij verdient een technische oplossing altijd de voorkeur boven gedragsverandering.

# 5. Beveiliging van personeel

## 5.1 Risico's

- Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

## 5.2 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.*

*De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.*

*Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder voor vertrouwensfuncties.*

*Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.*

## 5.3 Beheersmaatregelen

- Het lijnmanagement is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. De personeelszaken houdt toezicht op dit proces.
- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement geblokkeerd.
- Medewerkers die werken met vertrouwelijke of geheime informatie overleggen voor indiensttreding een Verklaring Omtrent het Gedrag (VOG). De VOG wordt indien nodig hernieuwd tijdens het dienstverband.
- Het lijnmanagement bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) dienen training te krijgen in procedures die binnen de organisatie of afdeling gelden voor informatiebeveiliging. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement.
- Regels die volgen uit dit beleid en andere regelingen van de organisatie gelden ook voor externen, die in opdracht van de organisatie werkzaamheden uitvoeren.

## 5.4 Bewustwording

- De bestuurlijk eindverantwoordelijke bevordert de algehele communicatie en bewustwording rondom informatieveiligheid.
- Het lijnmanagement bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen. Afspraken hierover worden vastgelegd in het managementcontract.
- In werkoverleggen wordt periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

# 6. Fysieke beveiliging en beveiliging van de omgeving

## 6.1 Risico's

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet-medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
- Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico ten aanzien van de vertrouwelijkheid.
- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

## 6.2 Doelstelling

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

*ICT-voorzieningen,die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.*

*Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.*

## 6.3 Beheersmaatregelen

- Alle objecten (gebouwen) van de organisatie krijgen op basis van generieke profielen een risicoprofiel toegewezen. Dit is het generieke risicoprofiel dat het beste aansluit bij het object.
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.

- In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijgehouden.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- In diverse panden van de organisatie wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is onder meer beperkt door de Wet bescherming persoonsgegevens.
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden, is voorbehouden aan bevoegd personeel. Registratie van de verleende toegang ondersteunt de uitvoering van de toegangsregeling.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.
- (Data)verbindingen worden beschermd tegen interceptie of beschadiging.
- Reserve apparatuur en back-ups zijn gescheiden in twee locaties of datacenters, om de gevolgen van een calamiteit te minimaliseren.
- Gegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd. Informatie wordt bewaard en vernietigd conform de Archiefwet 1995 en de daaruit voortvloeiende archiefbesluiten.

# 7. Beveiliging van apparatuur en informatie

## 7.1 Risico's

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- Organisaties gaan steeds meer samenwerken in ketens en besteden meer taken uit. Bij beheer van systemen en gegevens door een derde partij, blijft de organisatie verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
- Het ontbreken van een regeling voor antivirusbescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

## 7.2 Doelstelling

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

*Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.*

*Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.*

## 7.3 Beheersmaatregelen

### 7.3.1 Organisatorische aspecten

- Niemand kan geautoriseerd zijn om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.
- Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
- Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft de organisatie eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.
- Externe hosting van data en/of services is:
  - goedgekeurd door verantwoordelijk lijnmanager;

- in overeenstemming met informatiebeveiligingsbeleid en algemeen beleid;
- vooraf gemeld bij ICT voor toetsing op beheeraspecten.

### 7.3.2 Systeemplanning en –acceptatie

- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever (veelal de proceseigenaar). De test en de testresultaten worden gedocumenteerd.
- Systemen voor Ontwikkeling, Test en/of Acceptatie (OTA) zijn logisch gescheiden van Productie (P).
- Faciliteiten voor Ontwikkeling, Testen, Acceptatie en Productie (OTAP) zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
- In de OTA worden testaccounts gebruikt. Met productieaccounts wordt niet getest tenzij dit voor de test absoluut noodzakelijk is.
- Vertrouwelijke of geheime data uit de productieomgeving mag niet worden gebruikt in de ontwikkel-, test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data te vernietigen na ontwikkelen en testen.
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

### 7.3.3 Technische aspecten

- Alle gegevens anders dan classificatie ‘geen’ worden versleuteld conform beveiligingseisen in de IB-architectuur
  - Classificatieniveau ‘laag’: transportbeveiliging buiten het interne vertrouwde netwerk;
  - Classificatieniveau ‘midden’: transportbeveiliging;
  - Classificatieniveau ‘hoog’: transport en berichtbeveiliging.
- Versleuteling vindt plaats conform ‘best practices’, waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.
- Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc’s) wordt antivirus software van verschillende leveranciers toegepast.
- Alle apparatuur die is verbonden met het netwerk van de organisatie moet kunnen worden geïdentificeerd.
- ‘Mobile code’[20] wordt uitgevoerd in een logisch geïsoleerde omgeving om de kans op aantasting van de integriteit van het systeem te verkleinen. De ‘mobile code’ wordt altijd

[20] Software die wordt uitgevoerd zonder expliciete toestemming van de gebruiker, zoals scripts (Java), Java applets, ActiveX controls en Flash animaties. Dergelijke software wordt gebruikt voor functies binnen (web)applicaties.

uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet wordt aangetast.
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
- Het (ongecontroleerd) kopiëren van ‘geheime’ gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.
- Alle informatie, die wordt geplaatst op websites van de organisatie, wordt beschermd tegen onbevoegde wijziging. Op algemeen toegankelijke websites wordt alleen openbare informatie gepubliceerd.
- Groepen informatiediensten, gebruikers en informatiesystemen worden op het netwerk gescheiden zodat de kans op onbevoegde toegang tot gegevens verder wordt verkleind.
- Afhankelijk van de risico’s die verbonden zijn aan *online* transacties worden maatregelen getroffen om onvolledige overdracht, onjuiste routing, onbevoegde wijziging, openbaarmaking, duplicatie of weergave te voorkomen.
- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimumniveau (service levels) komt.

## Mobiele (privé)apparatuur en thuiswerkplek

- Beveiligingsmaatregelen hebben betrekking op zowel door de organisatie verstrekte middelen als privéapparatuur ('bring your own device' (BYOD)). Op privéapparatuur waarmee verbinding wordt gemaakt met het organisatienetwerk is de organisatie bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privéapparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
- Op verzoek van de organisatie dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan ‘mobile device management software’). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van informatie en integriteit van het organisatie netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden. Hiervoor wordt een regeling ontwikkeld.

## Back-up en recovery

- In opdracht van de eigenaar van data, maakt ICT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens.
- Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen.

- De back-up en herstelprocedures worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen.

## Informatie-uitwisseling

- Voor het gebruik van organisatie-informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het Algemeen Rijksambtenarenreglement (ARAR), geheimhoudingsverklaringen en huisregels.
- Digitale documenten van de organisatie waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKI Overheid certificaten[21] voor tekenen en/of encryptie. Hiervoor is een richtlijn PKI en certificaten opgesteld.
- Er is een (spam)filter geactiveerd voor inkomende e-mail berichten.

## Controle[22]

- Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.[23] Relevante zaken om te loggen zijn:
  - type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);
  - handelingen met speciale bevoegdheden;
  - (poging tot) ongeautoriseerde toegang;
  - systeemwaarschuwingen;
  - (poging tot) wijziging van de beveiligingsinstellingen.
- Een logregel 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.
- In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.
- Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.

[21] Public Key Infrastructure voor de overheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.
[22] Controle is nader toegelicht in de BIR.
[23] In sommige processen is het wettelijk verplicht of zeer gewenst dat geautoriseerde toegang wordt vastgelegd, zodat achteraf steeds kan worden vastgesteld wie toegang tot de gegevens heeft gehad.

## 7.4 Beheer van de dienstverlening door een derde partij

### 7.4.1 Risico's

- Organisaties gaan steeds meer samenwerken in ketens en besteden meer taken uit. Bij beheer van systemen en gegevens door een derde partij kan ook informatie van de organisatie op straat komen te liggen. De organisatie blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

### 7.4.2 Doelstelling

*Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een (bewerkers)overeenkomst, contracten en/of convenanten.*

*De organisatie controleert de implementatie van de maatregelen, die zijn vastgelegd overeenkomsten, bewaakt de naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de beveiliging aan alle eisen voldoet, die met de derde partij zijn overeengekomen.*

## 7.5 Beheersmaatregelen

- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (bewerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd.
- De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en beoordeeld en er worden periodiek audits uitgevoerd.
- Wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd.

### 7.5.1 Uitgangspunten

- In de basis-SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging.
- Er is een basiscontract voor de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin kaders staan voor de toegang tot ICT-voorzieningen door derden. In contractbeheer, applicatiebeheer en functioneel beheer is naleving van de gemaakte afspraken opgenomen.
  - Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
  - Het ontbreken van een regeling voor antivirus bescherming bij derden leidt tot hogere beveiligingsrisico's.

## 7.6 Behandeling van media

### 7.6.1 Risico's

- Verwijderbare media kan informatie bevatten, die in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal.

### 7.6.2 Doelstelling

*Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van*

*informatie en bedrijfsmiddelen.*

*Media worden beheerst en fysiek beschermd.*

*Vastgestelde procedures om documenten, opslagmedia (bijvoorbeeld USB-sticks, back-up tapes, schijven), in- en uitvoergegevens en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.*

### 7.6.3 Beheersmaatregelen

- Er dienen procedures te worden vastgesteld voor het beheer van verwijderbare media.
- Er dienen procedures te worden vastgesteld voor het op een veilige manier verwijderen van media als ze niet langer nodig zijn.
- Systeemdocumentatie dient te worden beschermd tegen onbevoegde toegang.

### 7.6.4 Uitgangspunten

- Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Harde schijven en andere media worden adequaat gewist of vernietigd bij afstoting of hergebruik. In ieder geval indien er vertrouwelijke informatie is opgeslagen en/of licentieplichtige programmatuur op is geïnstalleerd.
- Er zijn richtlijnen voor het opbergen van papieren en computermedia. In ieder geval voor gevoelige of kritieke bedrijfsinformatie.
- Innamebeleid voor mobiele apparatuur , zoals laptops, pda's, iPads, voor wanneer deze niet meer worden gebruikt.
- Encryptie op informatie met het classificatielabel vertrouwelijk en zeer geheim.

## 7.7 Uitwisseling van informatie

### 7.7.1 Risico's

- Verlies of diefstal van laptops, USB-sticks, iPads e.d., waarbij bovendien informatie in verkeerde handen komt.

### 7.7.2 Beheersmaatregelen

- Vaststellen formeel beleid, formele procedures en formele beheersmaatregelen om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- Vaststellen overeenkomsten voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
- Beschermingsmaatregelen voor media die informatie bevatten tegen onbevoegde toegang, misbruik of het corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
- Bescherming van informatie, die een rol speelt bij elektronische berichtuitwisseling.

### 7.7.3 Doelstelling

*Handhaven van beveiliging van informatie en programmatuur, die wordt uitgewisseld binnen*

*een organisatie en met enige externe entiteit.*

*Een formeel uitwisselingsbeleid met betrekking tot de uitwisseling van informatie en programmatuur tussen organisaties, dat in lijn is met de uitwisselingsovereenkomsten en relevante wetgeving.*

*Vastgestelde procedures en normen ter bescherming van informatie en fysieke media, die informatie bevatten die wordt getransporteerd.*

### 7.7.4 Uitgangspunten

- Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
- Een basisraamwerk met randvoorwaarden voor gegevensuitwisseling met ketenpartners.
- Gevoelige informatie (classificatie vertrouwelijk en zeer geheim) wordt nooit bekend gemaakt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
- Bewustzijn en sociale controle om het risico op het lekken van informatie via telefoon e.d. te laten afnemen.

## 8. Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot organisatie-informatie dient te worden vastgesteld.[24] Logische toegang is gebaseerd op de classificatie van de informatie.

### 8.1 Risico's:

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de BIR en/of een aanvullende risicoanalyse is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (met name waar ook niet ICT-teams toegang hebben).

### 8.2 Doelstelling

*Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.*

*Beleid ten aanzien van informatieverspreiding en autorisatie is van toepassing.*

### 8.3 Uitgangspunten

- De eigenaar van de data is bevoegd toegang te verlenen.
- Er wordt geen toegang verleend (account uitgegeven), waarvan de rechten aan meer dan één natuurlijk persoon zijn toegewezen. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd.
- De organisatie maakt gebruik van bestaande (landelijke) generieke voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals: DigiD en eHerkenning).

### 8.4 Authenticatie en autorisatie

- Wachtwoorden worden voor een beperkte periode toegekend (3 tot maximaal 6 maanden). Wachtwoorden dienen aan eisen te voldoen, deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen.[25]
- De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.
- Authenticatiemiddelen, zoals wachtwoorden, worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (door middel van encryptie).
- Autorisatie is rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.
- Toegang tot informatie met classificaties 'midden' of 'hoog' vereist 'multifactor' authenticatie (bijv. naam/wachtwoord + token).

[24] Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.
[25] Het wachtwoordbeleid is uitgewerkt in het wachtwoord beleidsdocument.

### 8.5 Externe toegang

- De organisatie kan een externe partij toegang verlenen tot het eigen netwerk. Hiervoor dient een procedure gemaakt en gevolgd te worden. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de organisatie, tenzij uitdrukkelijk overeengekomen.
- De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De organisatie heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.

### 8.6 Mobiel en thuiswerken

- Voor werken op afstand is een thuiswerkomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
- Onbeheerde apparatuur (privé-apparaten of de ‘open laptop’) kan gebruik maken van draadloze toegangspunten (WiFi). Deze zijn ten minste logisch gescheiden van het bedrijfsnetwerk van de organisatie.
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen organisatie-informatie wordt opgeslagen op het mobiele apparaat (‘zero footprint’). Informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen.[26]
- Voorzieningen als webmail, als ook sociale netwerk en clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, en het ontbreken van versleuteling) niet geschikt voor het delen van vertrouwelijke en geheime informatie en worden hiervoor niet gebruikt.

### 8.7 Overige maatregelen

- Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur.
- Het netwerk van de organisatie is waar nodig gesegmenteerd (afdelingen, gebruikers en systemen zijn logisch gescheiden). Tussen segmenten met verschillende beschermingsniveaus worden access control lists (ACL’s) geïmplementeerd.

### 8.8 Beveiliging van informatiesystemen (software)

#### 8.8.1 Doelstelling

| |
|---|
| *Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.* |

#### 8.8.2 Organisatorische aspecten

- Toetsing op informatiebeveiligingsbeleid is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de project start en eind architectuur (PSA en PEA[27]).

[26] Separaat document.
[27] Dit zijn Prince2 termen, zie hiervoor de projectmanagement methodiek Prince2.

- Projecten met een hoog risicoprofiel vallen onder toezicht van ICT. Toetsing op architectuur en informatiebeveiliging is hier onderdeel van.
- Projectmandaten worden ten behoeve van behandeling in overleg (onder meer) voorzien van een advies op informatiebeveiliging.
- In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingseisen opgenomen.

### 8.8.3 Softwareontwikkeling en onderhoud

- Applicaties worden ontwikkeld en getest op basis van landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties.[28]
- (Web)applicaties worden ontwikkeld en tenminste getest op basis van bekende kwetsbaarheden. Hiervoor wordt minimaal gebruik gemaakt van de richtlijnen, zoals vastgelegd in de OWASP top 10[29] of door CIP[30].
- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
- Alleen gegevens die noodzakelijk zijn voor de gebruiker worden uitgevoerd (doelbinding), rekening houdend met beveiligingseisen (classificatie).
- Toegang tot de broncode is beperkt tot de medewerkers, die deze code onderhouden of installeren.
- Beveiligingsupdates en beveiligingspatches worden zo spoedig mogelijk en na positief te zijn getest doorgevoerd.

### 8.8.4 Encryptie (versleuteling)

- De organisatie gebruikt encryptie conform PKI-overheid standaard.
- Intern dataverkeer (‘machine to machine’) wordt conform classificatie beveiligd met certificaten.
- Beveiligingscertificaten worden centraal beheerd binnen de organisatie.

[28] Nationaal Cyber Security Centrum (NCSC)
[29] https://www.owasp.org/index.php/Main_Page en CIP
[30] Volgens de methode en normen “Grip op SSD” van CIP

# 9. Beveiligingsincidenten

## 9.1 Risico's

- Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

## 9.2 Doelstelling

*Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.*

*Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.*

*Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.*

## 9.3 Melding en registratie

- De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de functionaris informatiebeveiliging van de organisatie.
- Beveiligingsincidenten die worden gemeld bij de service desk, worden als zodanig geregistreerd en voorgelegd aan de security functionaris binnen ICT. Voor afhandeling geldt de reguliere rapportage en escalatielijn.
- Afhankelijk van de ernst van een incident vindt direct een escalatie plaats en kan het verplicht zijn het incident te melden bij het College Bescherming Persoonsgegevens.[31]
- Ernstige incidenten, waarbij een alarmfase (zie onder) in werking treedt, worden opgenomen in de kwartaalrapportage van de CISO.

## 9.4 Alarmfasen

- Bij grote incidenten wordt gehandeld en opgeschaald conform de draaiboeken ICT-crisisbeheersing.

[31] De Wbp wordt hierop aangepast, er is tevens een EU verordening op handen (2014 en verder).

| Alarm fase | Kenmerk | Impact | Opschaling | Bijzonderheden |
|---|---|---|---|---|
| 1 | Lokaal ICT-incident bij één afdeling. | Oplosbaar probleem: bronbestrijding. | In beginsel niet. Probleem wordt opgelost door ICT. | Melding aan CISO |
| 2 | ICT-Incident bij meerdere afdelingen. | Nog steeds een geïsoleerd probleem: bron - + effectbestrijding. | In beginsel niet. Probleem wordt opgelost door ICT. | Melding aan CISO.<br>Melding bij CERT indien nodig. Communicatie is optioneel. |
| 3 | Concernbreed ICT-incident (en mogelijk andere organisaties) | Impact op de dienstverlening wordt echt ervaren. | Kernteam komt bij elkaar. Bestuur, CIO en directies worden geïnformeerd. | Melding aan CISO. Afdeling communicatie is vereist. |
| 4 | ICT-Incident is concern overstijgend (landelijk) | Impact op de dienstverlening is manifest. | Het kernteam is dan in beginsel adviserend en voert desgewenst coördinatie (binnen het ICT domein). | Er is sprake van landelijke opschaling via de technische lijn (NCSC) of via de maatschappelijke lijn (NCC). |

# 10. Bedrijfscontinuïteit

## 10.1 Risico's

- Wanneer er niet of nauwelijks invulling gegeven wordt aan de continuïteitsplanning is er naast een vals gevoel van veiligheid, ook grote kans op ad hoc maatregelen als een calamiteit zich voordoet.
- Het uitvallen van medewerkers (ontslag, ziekte, overlijden) kan een reële bedreiging zijn.

## 10.2 Doelstelling

*Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.*

*Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.*

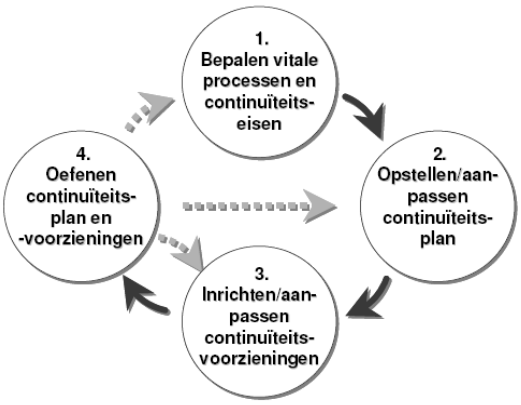
*Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.*

- Elk organisatieonderdeel voert een business impactanalyse uit. Afhankelijk van de bevindingen worden per afdeling vervolgacties gepland.
- Elke afdeling heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - Risico's;
  - Identificatie van essentiële procedures voor bedrijfscontinuïteit;
  - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
  - 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.
- Er worden minimaal jaarlijks oefeningen of testen gehouden om de BCM-plannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

## 10.3 Beleidsuitgangspunt

Er zijn voor processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen.

Continuïteitsplannen worden regelmatig getest en worden actueel gehouden.




**Figuur 3:• BCM Cyclus**

## 11. Naleving

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

### 11.1 Organisatorische aspecten

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en effectiviteit van de geïmplementeerde maatregelen;
  - de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.
- De CISO zorgt namens de bestuurlijk verantwoordelijke voor het toezicht op de uitvoering van het informatiebeveiligingsbeleid.
- ICT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatiebeveiligingsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD en GBA. Aanvullend op dit concern informatiebeveiligingsbeleid kunnen daarom specifieke normen gelden voor clusters.
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de CIO onderzocht door interne of externe auditors en door onafhankelijke externen (bijvoorbeeld door middel van ‘penetratietesten’). Jaarlijks worden ongeveer 3 audits/onderzoeken gepland. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C-cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het ‘in control’ statement.
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

### 11.2 (Wettelijke) kaders

- Voor de uitvoering en daarmee voor de naleving wordt uitgegaan van de relevante wet- en regelgeving die geldt op het gebied van informatiebeveiliging voor <organisatie>, zoals de Wbp, BIR en VIR.
- Voor elk type registratie is de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.

- Bij het (laten) vervaardigen en installeren van programmatuur, wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

## Bijlage: Relevante documenten en bronnen

Voor het informatiebeveiligingsbeleid zijn de volgende documenten relevant:

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging) (2007)
- Baseline Informatiebeveiliging Rijksdienst (BIR)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR)
- CBP richtsnoeren 'beveiliging van persoonsgegevens', 2013: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx