Baseline Informatieveiligheid

Veiligheidsregio Twente

2021

VEILIGHEIDSREGIO TWENTE

Autorisatie
Versiegegevens

VERSIE:	DATUM:	OMSCHRIJVING:
[Versie]	[Datum]	[Samenvatting]

[Plaats], [Datum]
Versie [Versie]

OPSTELLERS:	BIJDRAGE IN DE WERKGROEP*:
Brouwer,Jeroen	[Opmerkingen]

Voorwoord en/of samenvatting

[Inhoud]

Inhoudsopgave

Inleiding

Goede informatievoorziening is voor Veiligheidsregio Twente van cruciaal belang voor het goed kunnen uitvoeren van de taken die zijn vastgelegd in de Wet veiligheidsregio's. De Vakgroep Informatieveiligheid heeft de Baseline Informatiebeveiliging Gemeenten (BIG) vastgesteld als inhoudelijk normenkader voor informatieveiligheid in de Veiligheidsregio's. Hiervoor zijn twee redenen:

1. De BIG is gebaseerd op de internationale standaarden voor informatieveiligheid ISO 27001/27002;
2. Het opstellen en onderhouden van een Baseline Informatieveiligheid voor Veiligheidsregio's levert een te weinig specifiek product op om de inspanning daartoe te rechtvaardigen.

Een Veiligheidsregio blijft niettemin zelf volledig verantwoordelijk voor het vaststellen, uitvoeren, beoordelen en bijstellen van haar informatieveiligheidsbeleid. Dit document beschrijft het Informatieveiligheidsbeleid van Veiligheidsregio Twente. Het Informatieveiligheidsbeleid draagt bij aan een adequate hulpverlening en betrouwbare informatievoorziening en geeft uitvoeringsmogelijkheden aan wettelijke verplichtingen ten aanzien van bescherming van gegevens en rechten van personen.

Informatie wordt in alle geledingen van de Veiligheidsregio verwerkt en daarmee is informatie-veiligheid een thema dat integraal moet worden geadresseerd. In dit document wordt de integrale informatieveiligheid uitgewerkt in een aantal deelbeleidsthema's:

Visie & Missie
Beleidskaders Informatieveiligheid
H1 Uitgangspunten Informatieveiligheid;
Organisatie
H2 Organisatie van informatieveiligheid;
Maatregelen
H3 Beheer van bedrijfsmiddelen;
H4 Beveiliging van personeel;
H5 Fysieke beveiliging en beveiliging van de omgeving;
H6 Beheer van communicatie- en bedieningsprocessen;
H7 Toegangsbeveiliging;
H8 Verwerving, ontwikkeling en onderhoud van informatiesystemen;
Incidenten
H9 Beheer van informatiebeveiligingsincidenten;
H10 Bedrijfscontinuïteitsbeheer;
Toezicht
H11 Naleving.

Informatieveiligheid

Informatieveiligheid is de integrale benadering van structurele organisatorische en technische maatregelen, processen en procedures die gericht zijn op de bescherming van informatie. Onder bescherming van informatie wordt verstaan: het waarborgen van

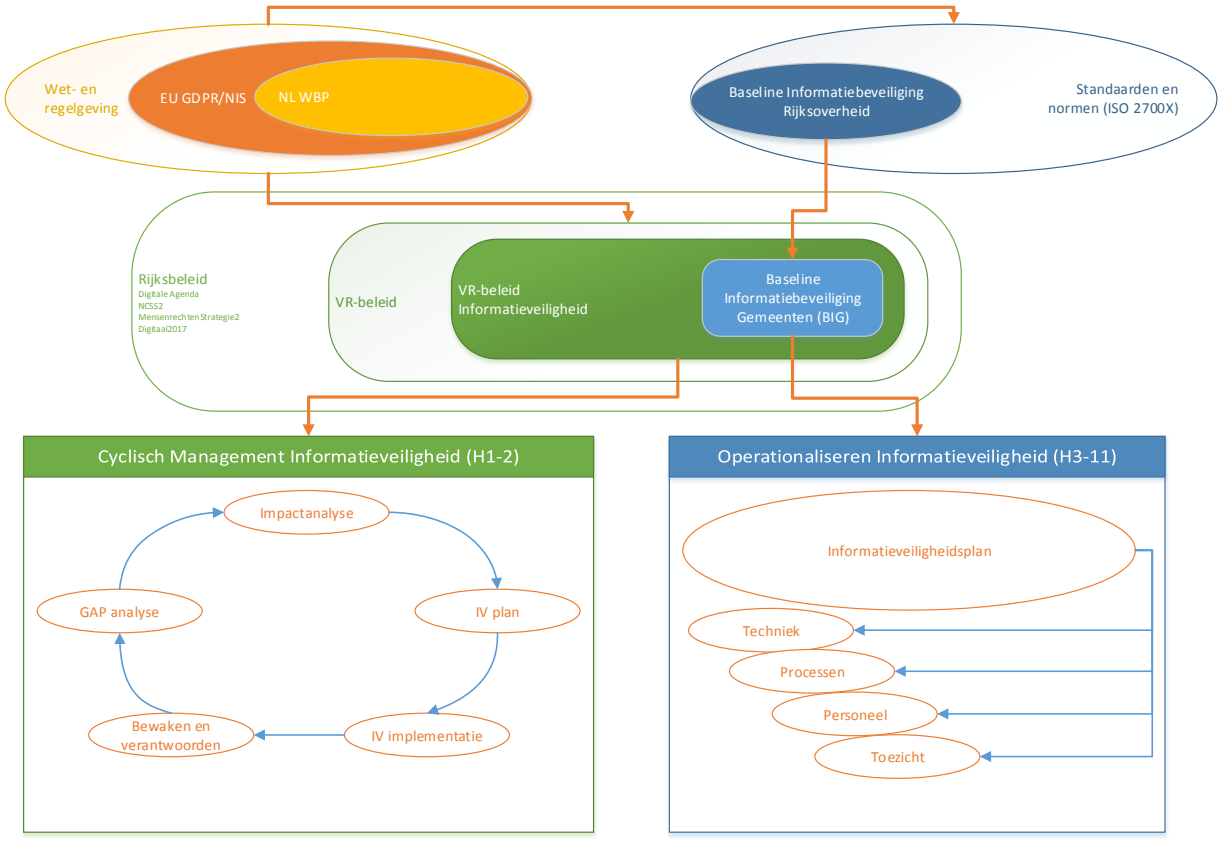
- *beschikbaarheid:* systemen en informatie zijn beschikbaar op de momenten dat zij voor gebruikers beschikbaar moeten zijn;
- *integriteit:* de informatie is correct, volledig, betrouwbaar en controleerbaar;
- *vertrouwelijkheid*: de informatie is niet beschikbaar voor onbevoegden.

Reikwijdte en afbakening informatiebeveiliging

Informatieveiligheid is meer dan goed gebruik van 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 mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligings-maatregelen zijn: clean desk policy, handreikingen voor het gebruik van mobiele devices en werkinstructies voor telewerken.

Samenhang

In onderstaand schema is weergegeven hoe wet- en regelgeving en standaarden van invloed zijn op (overheids)beleid, en hoe daarop het thema Informatieveiligheid in de Veiligheidsregio's wordt uitgewerkt.



Opbouw document

Het document is opgebouwd uit het integrale deel Baseline Informatieveiligheid, nader aangevuld met uitvoeringsregelingen/handreikingen voor specifieke operationele thema's, allen gebaseerd zijn op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Beleidskaders Informatieveiligheid

Het bestuur van Veiligheidsregio Twente heeft zijn visie voor beleidskaders op het gebied van informatieveiligheid geformuleerd:

Veiligheidsregio Twente gaat zorgvuldig, veilig en professioneel om met alle gegevens in de organisatie.

De Veiligheidsdirectie heeft daartoe dit informatieveiligheidsbeleid opgesteld, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Het gehele bestuur geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatieveiligheidsbeleid van en voor de hele organisatie. Dit beleid is van toepassing op de gehele Veiligheidsregio Twente, alle processen, organisatieonderdelen, objecten, informatiesystemen, gegevens(verzamelingen) en externe partijen die voor of namens Veiligheidsregio Twente gegevens verwerken. Dit informatieveiligheidsbeleid is in lijn met het algemene beleid van Veiligheidsregio Twente en relevante landelijke en Europese wet- en regelgeving. Dit beleid bevat een bijlage met nadere aanwijzingen.

De Veiligheidsregio is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van dit beleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: Wvr, Wbp, AVG en archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het Veiligheidsberaad heeft de BIG van toepassing verklaard voor Veiligheidsregio's, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.
- Er is een Vakgroep Informatieveiligheid die Veiligheidsregio's ondersteunt bij de implementatie van de BIG en bijbehorende technische en organisatorische maatregelen met: standaardproducten, gevraagd en ongevraagd advies en toezicht (collegiale audits).

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007), de BIG en de Algemene Verordening Gegevensbescherming:

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor Veiligheidsregio Twente. De verantwoordelijkheid voor informatieveiligheid ligt bij het (lijn)management, met **de Voorzitter van de Veiligheidsregio als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. De **Functionaris Gegevensbescherming** houdt onafhankelijk toezicht op de kaders en de uitvoering van informatieveiligheid en het melden van incidenten (waaronder meldplichtige datalekken).
3. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatieveiligheidsbeleid 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.
4. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.

5. De **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.
6. De **security officer** ondersteunt in de uitvoering, kwaliteitsbewaking, beoordeling en verbetering van informatieveiligheid,
7. De veiligheidsregio stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid, en heeft protocollen en rollen vastgesteld voor het beheersen van beveiligingsincidenten.
8. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**.
9. Alle medewerkers van Veiligheidsregio Twente worden **bewust gemaakt en getraind** in het gebruik van procedures om gegevens, eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
10. 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 Informatieveiligheidsbeleid treedt in werking na vaststelling door het Algemeen Bestuur van Veiligheidsregio Twente en vervangt daarmee alle versies van oudere datum.

Aldus vastgesteld door het Algemeen Bestuur van Veiligheidsregio Twente op *[datum],*

[Naam. Functie] [Naam. Functie]

1 Uitgangspunten informatiebeveiliging Veiligheidsregio Twente

Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van Veiligheidsregio Twente. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de hulpverlening en de algemene bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

Missie

Veiligheidsregio Twente zet in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatie-voorziening is noodzakelijk voor het goed functioneren van de Veiligheidsregio en vormt de basis voor het beschermen van rechten van burgers en bedrijven.[1] Dit vereist een integrale aanpak, goed opdrachtgeverschap en actueel risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie die de Veiligheidsregio in bezit of in gebruik heeft, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijnings-vormen, 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 betrouwbare en tijdige informatie (gezondheidszorg, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van *alle* medewerkers is essentieel voor informatieveiligheid.[2]

Doelstelling

Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische en organisatorische maatregelen om informatie die de Veiligheidsregio in bezit of in gebruik heeft te beschermen en te waarborgen, dat de Veiligheidsregio voldoet aan relevante wet en regelgeving. Veiligheidsregio Twente streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de veiligheidsregio weet welke maatregelen voor welke gegevens genomen moeten worden, en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

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

Uitgangspunten

- Het informatiebeveiligingsbeleid van Veiligheidsregio Twente is in lijn met het algemene beleid van de Veiligheidsregio en de relevante landelijke en Europese wet- en regelgeving.[3]
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- Het IB-beleid wordt vastgesteld door het Algemeen Bestuur van de Veiligheidsregio, de CISO herijkt periodiek het IB- beleid.

Risicobenadering

- De aanpak van informatiebeveiliging (IB-beleid) in Veiligheidsregio Twente is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG/KING (GAP-analyse). Indien een systeem of gegevensobject 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 (wettelijke) 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**. Toezicht en advies op dit proces is belegd bij de FG/PO.

Doelgroepen

- Het Informatieveiligheidsbeleid van Veiligheidsregio Twente is van toepassing op al haar interne en externe medewerkers en alle derden die voor, namens of in opdracht van Veiligheidsregio Twente gegevens verwerken of laten verwerken.

Doelgroep	Relevantie voor IB-beleid
Algemeen Bestuur Veiligheidsregio	Integrale verantwoordelijkheid
FG/CISO/PO	Kaderstelling, toezicht, implementatie en incidentmanagement
Lijnmanagement (proceseigenaren)	Sturing op informatieveiligheid en controle op naleving
Medewerkers	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen van 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

Scope

- De scope van dit beleid omvat alle gegevens die de Veiligheidsregio in bezit of in gebruik heeft of aan derden verstrekt, de informatiesystemen die de veiligheidsregio gebruikt of laat gebruiken, de verwerking van de gegevens door medewerkers, en/of anderen in opdracht van de Veiligheidsregio in de meest brede zin van het woord.

[3] Daarbij geldt het 'comply or explain' principe (pas toe of leg uit)

- Dit Veiligheidsregio IB-beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.[4]

IB-beleid en architectuur

- IB is onderdeel van de Veiligheidsregio Twente informatiearchitectuur en uitgewerkt in de IB-architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie).[5]

Werking

- Dit IB-beleid treedt in werking na vaststelling door het Algemeen Bestuur van de Veiligheidsregio. Hiermee komen voorgaande versies van het IB-beleid van Veiligheidsregio Twente te vervallen.

[4] Bijvoorbeeld AVG (Algemene Verordening Gegevensbescherming), Archiefwet en Basisregistraties.
[5] De processen van informatiebeveiliging worden onderdeel van de volgende GEMMA versie om daarmee de basis voor informatieveiligheid te verankeren als integraal onderdeel van de bedrijfsvoering.

2 Organisatie van de informatiebeveiliging

2.1 Interne organisatie

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 die op grond van wet- en regelgeving en behoorlijk bestuur zijn vereist.

Doelstelling:

Beheren 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 van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

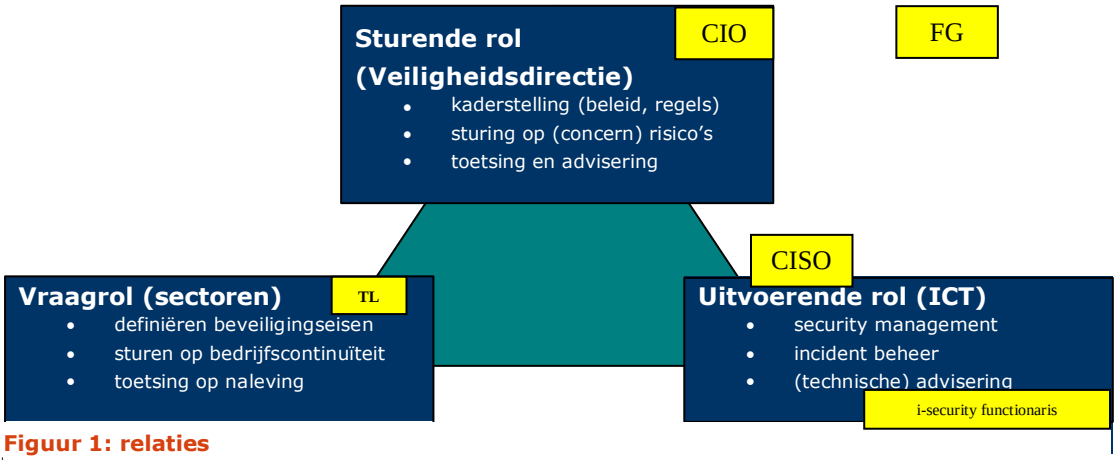
Verantwoordelijkheden

- Het Algemeen Bestuur van de Veiligheidsregio is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van Veiligheidsregio Twente.[6]
  - stelt kaders voor informatiebeveiliging (IB) op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;
- De Veiligheidsdirectie (in sturende rol) is verantwoordelijk voor kaderstelling en sturing.[7]
  - stuurt 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.
- De kolommen binnen de Veiligheidsregio (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.[8]
  De kolomdirectie:
  - 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 Veiligheidsregio in de managementrapportages.
- De Interne Service Organisatie of gelijkwaardig (ICT, HR, bedrijfsvoering, etc., in uitvoerende rol) is verantwoordelijk voor uitvoering.[9]

[6] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
[7] Met betrekking tot de i-functie geeft de CIO op dagelijkse basis namens de directie invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.
[8] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten

De interne service organisatie:

- 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

2.2 Taken en rollen

- De Algemeen Bestuur stelt formeel het IB-beleid vast. De uitvoering van het beleid moet periodiek gecontroleerd worden. De Veiligheidsdirectie adviseert het Algemeen Bestuur formeel over vast te stellen beleid.
- De CIO (Chief Information Officer), portefeuillehouder of vergelijkbare rol geeft namens de Veiligheidsdirectie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie 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, coördineert de integrale uitvoering en rapporteert periodiek concernbreed aan de directie over de stand van zaken.
- Wettelijk verplicht intern toezicht op - en coördinatie van - informatiebeveiliging is belegd bij de strategisch gepositioneerde Functionaris Gegevensbescherming. Uitvoerende taken zijn zoveel mogelijk belegd bij (decentrale) i-security functionarissen. De afdelingen rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de P&C cyclus.
- De interne service organisatie (met name ICT) heeft een security functionaris[10] aangesteld voor dagelijks beheer van technische IB-aspecten. De security functionaris rapporteert aan de CISO. Informatiebeveiliging is onderdeel van de service management rapportage.

[9] Let op, de interne service organisatie is tegelijk ook klant, het gaat hier echter om de uitvoerende rol.

[10] Voor de taakverdeling tussen de security functionaris en FG: zie Positionering van de FG (KING/VNG)

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Sturen: Directie dagelijkse uitvoering: CIO/CISO	Ontwikkelen van visie en kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, toewijzen verantwoordelijk-heden, advisering, PIA's, procedures, crisisbeheersing en incident respons, deelname ISAO's.	Controle, audit, pentesten.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie
Vragen: 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: Service organisatie/ i-security functionaris/ security officer	Beleidsvoorbereiding, technische onderzoeken (marktverkenningen).	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies, faciliteren rechten van betrokkenen (inzage en correctie, data-portabiliteit)	Vulnerability scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de CIO/CISO over aanpassingen aan de informatievoorziening.
Control: Functionaris Gegevens-bescherming	Informatie en advies aan Bestuur inzake wettelijke verplichtingen, toetsen beleid aan wet- en regelgeving en sturingsinformatie uit audits en rapportages.	Toezien op - naleven wet- en regelgeving en beleid - toewijzing van verantwoordelijk-heden - bewustmaking en opleiding personeel - audits; Regierol bij incident respons, adviesrol bij PIA's, contactpunt voor autoriteit gegevensbescherming.	Auditkaders, integraal aggregeren rapportages en audits tot sturingsinformatie.	Sturingsinformatie uitwerken in verbeter- en beleidsvoorstellen. Rapportage aan Bestuur Veiligheidsregio

2.3 Functioneel overleg

De CISO stelt een organisatie voor van security gerelateerde (PO/SO) functionarissen binnen de Veiligheidsregio en de CISO organiseert tenminste eenmaal per kwartaal een (security) overleg met dit gremium. De CISO is voorzitter. Het overleg heeft binnen de Veiligheidsregio een adviesfunctie richting de CIO of gelijkwaardig en richt zich met name op beleid en adviseert over tactisch/strategische 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.

2.4 Rapportage en formele escalatielijn voor IB

(Decentrale) Security Functionaris → CISO → CIO → Bestuur

2.4.1. Externe partijen

- IB-beleid, landelijke normen en wet- en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de Veiligheidsregio samenwerkt (en informatie mee uitwisselt).[11] Ook voor externe partijen geldt hierbij het 'comply or explain' beginsel (pas toe of leg uit).
- 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 IB-beleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de Veiligheidsregio bevoegd is om de toepassing van beveiligingsmaatregelen te (laten) controleren.[12]
- Voor het tot stand brengen van datakoppelingen met externe partijen, geldt naast generiek IB-beleid een ITIL procedure 'Inrichten datakoppeling'. Het doel van de procedure is risicobeheersing en uniformiteit.
- Voor externe hosting van data en/of services gelden naast generiek IB-beleid de richtlijnen voor cloud computing.[13] De Veiligheidsregio is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door de externe partij(en);
  - passende beveiligingseisen voor bijzondere categorieën gegevens;[14]
  - melding bij Autoriteit Persoonsgegevens (AP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

2.4.2. ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing dient een kernteam IB geïnstalleerd te zijn, bestaande uit CISO of functionaris informatiebeveiliging, security functionaris ICT Service organisatie, relevante experts en de Veiligheidsregio communicatie afdeling. De werkwijze dient te zijn vastgelegd.
- Veiligheidsregio Twente participeert in relevante landelijke platforms (Vakgroep Informatieveiligheid) en onderhoudt contacten met andere sectoraal/regionaal georganiseerde IB-platforms (ISAO's/ISAC's/NCSC).

2.4.3. PDCA

- Informatiebeveiliging is een continu verbeterproces.[15] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.
- Toelichting figuur 2:
  - Plan: De cyclus start met IB-beleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis. De planning op hoofdlijnen is onderdeel van het integrale jaarplan en is uitgewerkt in het informatiebeveiligingsplan (IB-beleid) van de Veiligheidsregio. Afdelingsspecifieke activiteiten worden gepland in het afdelings-IB plan of het afdelings- informatieplan (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.[16] Bevindingen worden gerapporteerd aan de FG, CIO en de directies.
  - Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. 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 directie. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

[11] Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Nederlandse Gemeenten.

[12] Hiervoor kan gebruik worden gemaakt van een gestandaardiseerde bewerkersovereenkomst van de IBD.

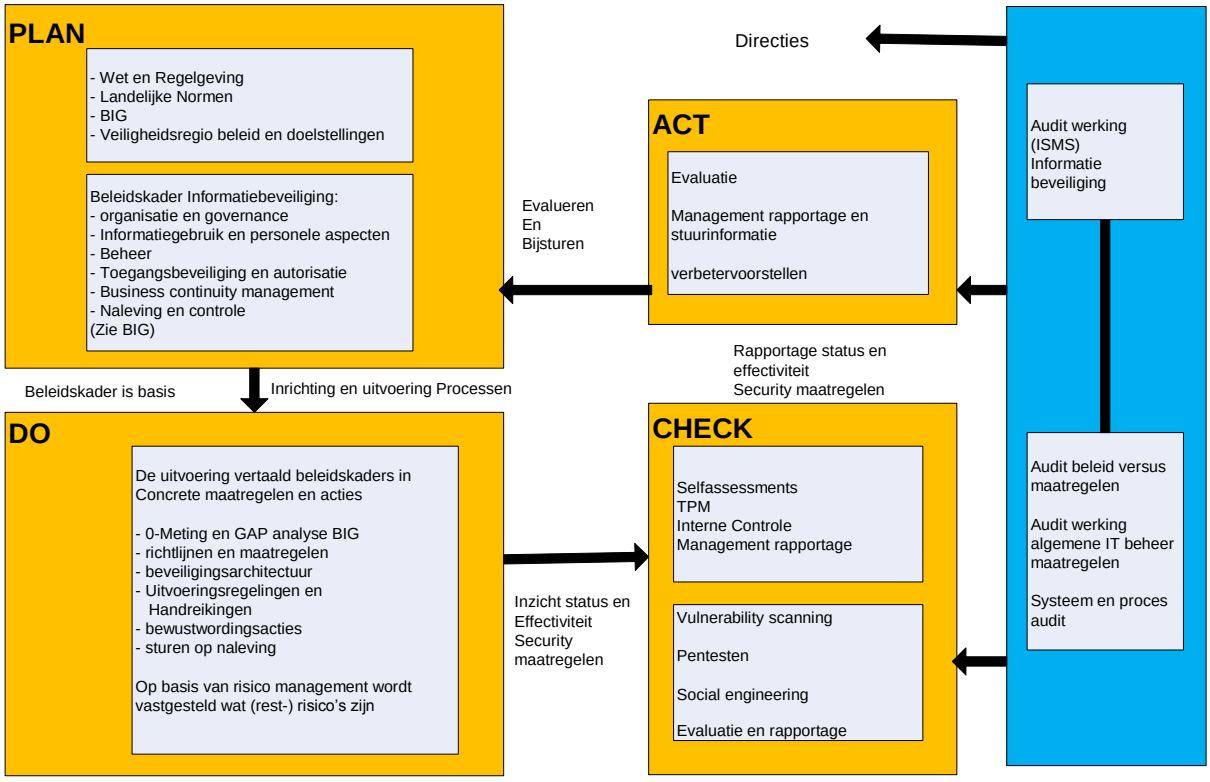
[13] Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html

[14] 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

[15] NEN/ISO 27001

[16] Van onder meer de accountant, rijksoverheid (voor bijv. basisregistraties) en Veiligheidsregio auditors (intern).

Figuur 2: Information Security Management System



Information Security Management System

3 Beheer van bedrijfsmiddelen

3.1 Verantwoordelijkheid voor bedrijfsmiddelen

Risico's:

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals verlies, diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgesteld:
  - wie de gebruiker/eigenaar van het bedrijfsmiddel is;
  - tot welke informatie het betreffende bedrijfsmiddel toegang geeft;
  - of de mate van beveiliging van het bedrijfsmiddel adequaat is.

- Onvoldoende betrokkenheid van eindgebruikers bij informatiebeveiliging waardoor beveiligingsprocedures niet worden uitgevoerd en incidenten niet (tijdig) worden gemeld.

Doelstellingen

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

Voor alle bedrijfsmiddelen is vastgesteld wie de eigenaar/eindgebruiker is, welke informatie het bedrijfsmiddel ontsluit, alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

Beheersmaatregelen

- Alle bedrijfsmiddelen moeten geïdentificeerd zijn er moet een inventaris van worden bijgehouden.
- Alle informatie en bedrijfsmiddelen, die verband houden met ICT-voorzieningen aan een 'eigenaar' (een deel van de organisatie) toewijzen en classificeren.
- 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 bedrijfsinformatie de nodige zorgvuldigheid te betrachten (conform instructie) en de integriteit en goede naam van de Veiligheidsregio te waarborgen.
- Medewerkers gebruiken bedrijfsinformatie alleen voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van bedrijfsinformatie 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.
  - Privémiddelen mogen worden gebruikt voor telewerken mits deze adequaat beveiligd zijn.
  - De inlogomgeving die daartoe wordt aangeroepen toetst de beveiliging en vereist installatie van aanvullende beveiligingssoftware.
  - De medewerker meldt vermoedelijk misbruik of een andere inbreuk op de veiligheid van zijn/haar account of de gegevens waartoe het account toegang geeft onmiddellijk conform instructie.

  - 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 informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
  - het geheime karakter van dienst eigen inloggegevens;
  - de beveiligingsclassificatie van de informatie (zie hieronder);
  - de door de Veiligheidsregio gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
  - aan de werkplek verbonden risico's;

3.2 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt.[17] 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.

Risico's:

- Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de primaire processen.
- 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.

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.

Beheersmaatregelen:

- Informatie classificeren met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Opstellen en uitdragen classificatiebeleid binnen de Veiligheidsregio.
- Er dienen geschikte samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de classificering en verwerking van informatie overeenkomstig het classificatiesysteem dat is vastgesteld.

[17] Dit is in detail beschreven in de Handreiking dataclassificatie IBD/KING 2016

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de Veiligheidsregio)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het Veiligheidsnet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoerings-informatie en primaire procesinformatie zoals vergunningen)*	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*
Hoog	**Geheim** informatie is alleen toegankelijk voor specifieke functionaris *(bv: aanvalsplannen en incidentinformatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: GMS, KVT)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: P2000)*

Uitgangspunten

- De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.
- Het object van classificatie is informatie. We classificeren 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 passend 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 én daarnaast verdient een technische oplossing altijd de voorkeur boven gedragsverandering.
- Dataclassificatie wordt uitgevoerd conform de IBD handreiking 'Dataclassificatie'.

Toelichting

De te nemen maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Dit is vaak situatie afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het mitigeren van de risico's disproportioneel hoog zijn.[18] Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

[18] Dit is uitgebreid beschreven in: 'Beveiliging van persoonsgegevens', CBP richtsnoeren, 2013.

4 Beveiliging van personeel

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.

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.

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 HR-afdeling houdt toezicht op dit proces.
- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd tenzij schriftelijk anders bepaald. 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 herhaald tijdens het dienstverband.
- Het lijnmanagement bepaalt welke rol(len) de medewerker moet vervullen en welke rol-gebaseerde 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 Veiligheidsregio gelden voor informatiebeveiliging. Deze training dient regelmatig te worden herhaald en geregistreerd om het beveiligingsbewustzijn aantoonbaar op peil te houden.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in de Arbeidsvoorwaardenregeling Veiligheidsregio Twente (AVT).
- Regels die volgen uit dit beleid en andere regelingen gelden ook voor externen, die in opdracht van de Veiligheidsregio werkzaamheden uitvoeren.

Bewustwording

- De Veiligheidsregio/ de directie/ de afdeling bevordert 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 en trainingen wordt periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

5 Fysieke beveiliging en beveiliging van de omgeving

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 m.b.t. 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.

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.

Beheersmaatregelen

- Alle objecten (gebouwen) van de Veiligheidsregio 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 houden gebouwbeheerders 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 Veiligheidsregio wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is beperkt door de Wet Bescherming Persoonsgegevens en nadere regels.
- 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.

6 Beveiliging van apparatuur en procedures

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.
- De Veiligheidsregio gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de Veiligheidsregio op straat komen te liggen. De Veiligheidsregio blijft 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 en ongepatchte beveiligingsissue's.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

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.

6.1 Beheersmaatregelen

Organisatorische aspecten

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien noodzakelijk 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 Veiligheidsregio eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede contractuele afspraken (bewerkersovereenkomst) en controle hierop.
- Externe hosting van data en/of services is getoetst aan geldend beleid en tevens:
  - goedgekeurd door verantwoordelijk lijnmanager;
  - vooraf gemeld bij ICT t.b.v. toetsing op beheeraspecten.

Systeemplanning en –acceptatie

- Nieuwe systemen, upgrades en nieuwe versies worden conform ITIL methodiek 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 vastgelegd.
- 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. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk.
- 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.

Technische aspecten

- Alle gegevens anders dan classificatie 'geen' worden versleuteld conform beveiligingseisen in de Gemeentelijke IB-architectuur
  - Classificatieniveau 'laag': transportbeveiliging buiten het interne netwerk;
  - Classificatieniveau 'midden': transportbeveiliging;
  - Classificatieniveau 'hoog': transport en berichtbeveiliging.
- Versleuteling vindt plaats conform 'best practices' (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
- Gegevens op papier worden beschermd door een deugdelijke opslag of vernietiging 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 Veiligheidsregio moet kunnen worden geïdentificeerd.
- 'Mobile code'[19] 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 uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt
- 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.

[19] 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.

- Alle informatie, die wordt geplaatst op websites van de Veiligheidsregio, 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 minimum niveau (service levels) komt.

Mobiele (privé-)apparatuur en thuiswerkplek

- Beveiligingsmaatregelen hebben betrekking op zowel door de Veiligheidsregio verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het Veiligheidsregio netwerk is de Veiligheidsregio bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
- Op verzoek van de Veiligheidsregio 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 Veiligheidsregio informatie en integriteit van het Veiligheidsregio netwerk.
- In geval van dringende redenen (beveiligingsincidenten) kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden. Voor beveiligingsincidenten wordt een regeling ontwikkeld in H8.

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 Veiligheidsregio informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, geheimhoudingsverklaring, huisregels en werkinstructies.
- Digitale documenten van de Veiligheidsregio waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld.
- Er is een (spam) filter geactiveerd voor inkomende e-mail berichten.

Controle[20]

- Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiliging-sincidenten, 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.[21] 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 door een gebruiker of systeembeheerder. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.

6.2 Beheer van de dienstverlening door een derde partij

Risico's

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

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 in 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.

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.

[20] Controle is nader toegelicht in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
[21] 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.

- 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.

Uitgangspunten

- In de basis-SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging.
- De in de bewerkersovereenkomst opgenomen beveiligingsmaatregelen zijn het resultaat van een analyse van de risico's, rekening houdend met de classificatie van de data die wordt verwerkt.
- 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.

6.3 Behandeling van opslagmedia

Risico's

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

Doelstelling

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

Opslagmedia worden beheerst en fysiek beschermd.

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

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.

Uitgangspunten

- Er zijn procedures voor het beheer van (beveiliging 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 licentie plichtige 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.

6.4 Uitwisseling van informatie

Risico's

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

Beheersmaatregelen

- Vaststellen formeel beleid, formele procedures en formele beheersmaatregelen om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen, afgestemd op de classificatie van de betreffende informatie.
- 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.

Doelstelling

Handhaven van beveiliging van informatie en programmatuur, die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

Een formeel uitwisselingsbeleid m.b.t. 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.

Uitgangspunten

- Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
- Voor gegevensverwerking door en/of voor ketenpartneren worden aan de hand van erkende standaarden en normen randvoorwaarden voor de verwerking schriftelijk vastgelegd in o.a. verwerkersovereenkomsten.
- 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.

7 Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot Veiligheidsregio informatie dient te worden vastgesteld.[22] Logische toegang is gebaseerd op de classificatie van de informatie.

Risico's:

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) 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 (m.n. waar ook niet ICT-teams toegang hebben).

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.

Uitgangspunten

- De eigenaar van de data is bevoegd toegang te verlenen.
- Er worden in de regel geen 'algemene' identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien niet (wettelijke) vereist, kan (voor informatie met de laagste dataclassificatie) worden gewerkt met functionele accounts.
- De Veiligheidsregio maakt ,waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals DigiD en eHerkenning) en best practices op dit gebied (zoals 2 factor authenticatie).

7.1 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.[23]
- 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 'multi-factor' authenticatie (bijv. naam/wachtwoord + token).
- Nadere uitvoeringsregels zijn vastgesteld in het IBD wachtwoordbeleid (product operationele BIG).

[22] Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.
[23] Het wachtwoordbeleid is uitgewerkt in het wachtwoord beleids document van de Veiligheidsregio.

7.2 Externe toegang

- De Veiligheidsregio kan een externe partij toegang verlenen tot het Veiligheidsregio 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 Veiligheidsregio, tenzij uitdrukkelijk vastgelegd in een verwerkersovereenkomst.
- De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers conform afspraken in de verwerkersovereenkomst. De Veiligheidsregio heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.

7.3 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 (VRT_WiFi_Gast). Deze zijn logisch gescheiden van het Veiligheidsregio bedrijfsnetwerk.
- Mobiele bedrijfsapplicaties worden via Mobile Device Management aangeboden zodat er geen Veiligheidsregio informatie wordt opgeslagen op het mobiele apparaat ('zero footprint') buiten. Veiligheidsregio informatie, anders dan openbare informatie, dient te worden versleuteld bij transport en opslag conform classificatie eisen.[24]
- Voorzieningen als webmail, als ook sociale netwerk en clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, het ontbreken van versleuteling), en het ontbreken van wettelijk vereist toezicht, niet toegestaan voor het delen van informatie met een andere dataclassificatie dan "openbaar".

7.4 Overige maatregelen

- Het fysieke (bekabelde) en draadloze (WiFi) netwerk zijn niet toegankelijk voor onbeheerde apparatuur.
- Het netwerk van de Veiligheidsregio is waar mogelijk gesegmenteerd (afdelingen, gebruikers en systemen zijn logisch gescheiden). Tussen segmenten met verschillende beschermings-niveaus worden access control lists (ACL's) geïmplementeerd.

[24] Separaat document, zie IBD handreiking dataclassificatie

8 Beheer van informatiesystemen

Risico's:

- Onvoldoende aandacht voor informatieveiligheid tijdens de designfase van een informatiesysteem.
- Ontbreken van een Privacy Impact Assessment voor het informatiesysteem.
- Verzwakking van beveiliging door interne (phishing, malicious insider) of externe handelingen (hack, spionage) van gebruikers.
- Verzwakking van beveiliging door onvoldoende onderhoud (updates, patches).

Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van het ontwerp en de lifecycle van informatiesystemen.

8.1 Ontwerpfase van procesinformatie

- Toetsing op IB-beleid is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de project start en eind architectuur (PSA en PEA[25]).
- Projecten met een hoog risicoprofiel vallen onder toezicht van de CISO/FG. Toetsing op architectuur en informatieveveiliging is hier onderdeel van.
- Projectmandaten worden ten behoeve van behandeling in DVO/Veiligheidsregio 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, rekening houdend met de meest recente lijst "verplichte open standaarden".

8.2 Softwareontwikkeling en onderhoud

- Applicaties worden ontwikkeld en getest o.b.v. landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties.[26] Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10.[27]
- Web applicaties worden voor de in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
- 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 beheerders.
- Technische kwetsbaarheden worden regulier met een minimum van 4 keer per jaar gerepareerd door 'patchen' van software, of 'ad hoc' bij acute dreiging. Welke software wordt geüpdatet wordt mede bepaald door de risico's.
- Voor applicaties met een verhoogd risicoprofiel worden voorzieningen getroffen om inbreuken op de beveiliging te detecteren.

[25] Dit zijn Prince2 termen, zie hiervoor de projectmanagement methodiek Prince2

[26] Nationaal Cyber Security Centrum, NCSC

[27] https://www.owasp.org/index.php/Main_Page

8.3 Encryptie (versleuteling)

- De Veiligheidsregio gebruikt encryptie conform PKI-overheid standaard.[28]
- Intern dataverkeer ('machine to machine') wordt conform classificatie beveiligd met certificaten.
- Beveiligingscertificaten worden centraal beheerd binnen de Veiligheidsregio.

[28] Public Key Infrastructure voor de overheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.

9 Beveiligingsincidenten

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.
- Niet (tijdig) voldoen aan de wettelijke meldplicht die voor bepaalde incidenten geldt.

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 of instantie.

9.1 Melding en registratie

- De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de functionaris informatiebeveiliging van de Veiligheidsregio.
- Beveiligingsincidenten worden geregistreerd en voorgelegd aan de functionaris informatiebeveiliging.
- Van elk beveiligingsincident wordt de wettelijke meldplicht beoordeeld en opgevolgd.[29]
- Beveiligingsincidenten worden afgehandeld en opgeschaald conform het protocol dataincidenten.

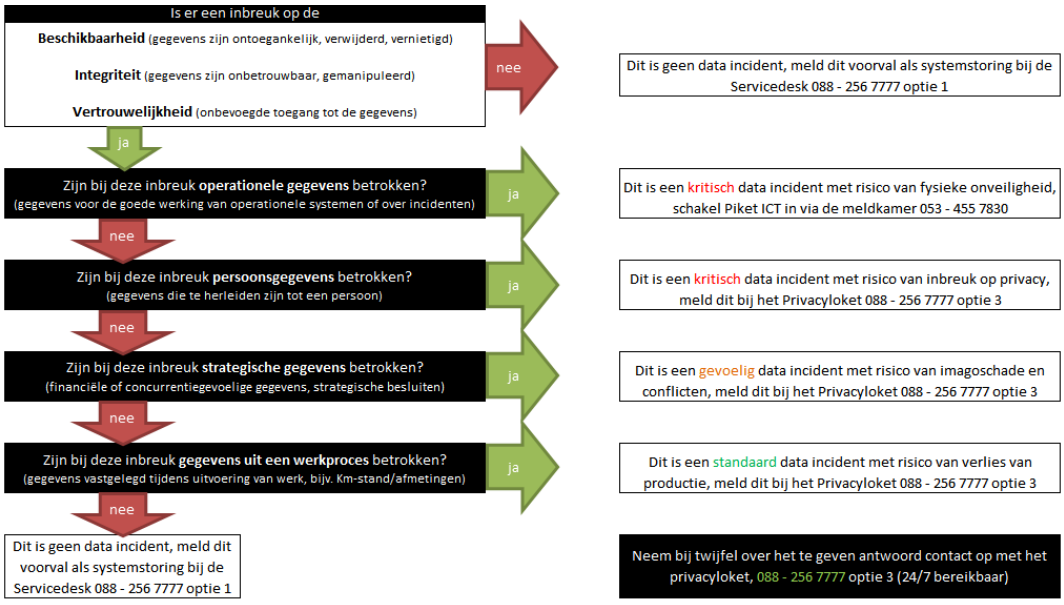
[29] De meldplicht geldt al onder de WBP, deze worden in de AVG en NIST (2018) aangescherpt

9.2 Opschaling en afhandeling

- Beveiligingsincidenten worden afgehandeld en opgeschaald conform hun risicoclassificatie.

aard gegevens	potentieel risico	omvang inbreuk relevant	risico classificering
Operationele gegevens	fysieke onveiligheid, inbreuk privacy, imagoschade, boete	nee	kritisch
Persoonsgegevens	inbreuk privacy, imagoschade, boete	nee	kritisch
Strategische gegevens (concurrentiegevoelig, financieel)	imagoschade, conflicten	nee	gevoelig
Gegevens uit werkproces	verlies van productie	ja	standaard

- Middels een stroomschema wordt afhandeling en opschaling bepaald.



10 Bedrijfscontinuïteit

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.
- Uitval of onbeschikbaarheid van medewerkers (ziekte, sterven, ontslag, repressieve inzet) en systemen (uitval elektriciteit of infrastructuur) kan een reële bedreiging zijn.

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.

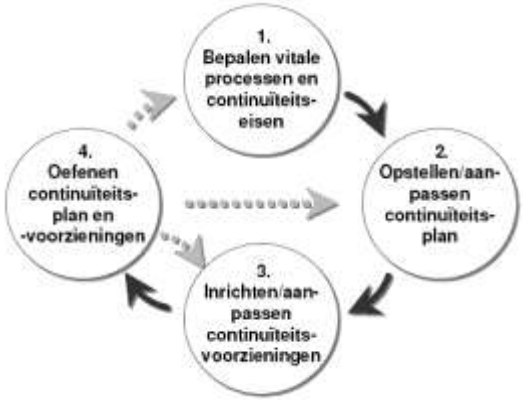
Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.

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

- Elk Veiligheidsregio afdeling 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.

Beleidsuitgangspunt

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen.
Continuïteitsplannen moeten regelmatig worden getest en actueel worden gehouden.



Figuur 3:• BCM Cyclus

11 Naleving en Toezicht

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 Veiligheidsregio processen waarin wordt gewerkt met 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 voorzitter van de Veiligheidsregio voor het toezicht op de uitvoering van het IB- beleid.
- Toezicht op de uitvoering en naleving van de Wbp/AVG in alle processen (ook de uitbestede) binnen de Veiligheidregio wordt uitgevoerd door de Functionaris Gegevensbescherming.
- Leveranciers, derden en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het IB-beleid. Bij uitbestede (beheer)processen wordt gebruik gemaakt van SLA's, verwerkersoverenkomsten en ISO normering 27001.
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI en GBA. Aanvullend op dit concern IB-beleid kunnen daarom specifieke normen gelden voor clusters.[30]
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de CIO onderzocht door Veiligheidsregio auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C cyclus wordt gerapporteerd over informatieveiligheid.
- Er wordt een beveiligingsregister aangelegd en onderhouden. Dit register bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de wettelijke-/specifieke beveiligingseisen is voldaan.

11.2 (Wettelijke) kaders

- Een overzicht van relevante wet en regelgeving is te vinden bij KING.[31] Zo is het gebruik van persoonsgegevens geregeld in de Wet Bescherming Persoonsgegevens.[32]
- Voor elk type registratie wordt 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

[30] Binnen de sector Veiligheidsregio wordt gestreefd naar een uniform audit-kader om de verantwoordingslast zo veel mogelijk te beperken.
[31] Een concept overzicht van wetten, regelingen en andere kaders is beschikbaar op de website van KING.
[32] Zie ook: CBP richtsnoeren

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 1: Relevante documenten en bronnen

Intern

- VRT Memo bescherming persoonsgegevens dd 09-12-2015
- BVO VRT Plan van Aanpak Informatieveiligheid 03-11-2016

Extern

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging) (2007)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), KING, 2013: https://www.ibdgemeenten.nl/producten/
- CBP richtsnoeren 'beveiliging van persoonsgegevens', 2013: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
- GEMMA: http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/e-dienstverlening-verbeteren/gemma
- Voorbeeld informatiebeveiligingsbeleid Gemeenten (KING/VNG): https://www.ibdgemeenten.nl/downloads/voorbeeld-informatiebeveiligingsbeleid-gemeenten/
- Rol en taken van de FG (KING/VNG): https://www.kinggemeenten.nl/sites/king/files/20170221%20Handreiking%20Rol%20en%20Taken%20van%20FG_v1.00.pdf
- Positionering van de FG (KING/VNG: https://www.kinggemeenten.nl/sites/king/files/Handreiking%20Positionering%20FG.pdf
- Handreiking dataclassificatie (KING/VNG: https://www.ibdgemeenten.nl/wp-content/uploads/2016/08/20160803-Handreiking-dataclassificatie-1.6.1.pdf.pagespeed.ce.syEAJBQM8L.pdf