Documentnummer:46954735

BESLUITVORMING BESPREKING INFORMEREN

SERVICEPUNT 71

Besluitvormingsformulier

Versie 04

Onderwerp	Informatiebeveiligingsbeleid Servicepunt71
Datum van indiening	23-11-2016
Naam en functie van opsteller	[redacted]
Mailadres opsteller	r.zoet@servicepunt71.nl
Naam verantwoordelijk (service)eenheidsmanager	MT Secretaris
Naam	secretaris Servicepunt71
Email	spt-secretaris@servicepunt71.nl
Vertrouwelijk?	Nee

Routing

Adviesoverleg Directeur (AOD)	Managementteam (MT SP71)	Werkoverleg Gez. Bedrijfsvoering (WGB)	Strategiegroep Gezamenlijke Bedrijfsvoering (SGB)
-Maak een keuze-	-Maak een keuze-	-Maak een keuze-	-Maak een keuze-

Bestuur	Ondernemingsraad (OR) check hier de WOR artikelen
Ter besluitvorming	-Maak een keuze-

Context	In 2013 is er een regionaal Statuut Informatiebeveiliging opgesteld, dat destijds is vastgesteld door het bestuur van Servicepunt71 (d.d. 26 sep 2013) en in de regio door de colleges van Leiden, Leiderdorp, Oegstgeest en Zoeterwoude. Het Statuut bevat algemene uitgangspunten over de wijze waarop we gezamenlijk onze informatie willen beveiligen. Door de invoering van nieuwe regelgeving, wijzigingen in de organisaties en de invoering van de Baseline Informatiebeveiliging Gemeenten (BIG) is het Statuut niet meer actueel. Het Statuut legde de basis voor informatiebeveiliging en was feitelijk een intentieverklaring, waarin werd uitgesproken conform de BIG en in onderlinge samenwerking de informatiebeveiliging in de regio op orde te brengen. In het voorliggend beleidsstuk is nu nader invulling gegeven aan deze intentie, waarbij de organisatie van informatiebeveiliging is beschreven, de ontwikkelrichting is bepaald en de kaders zijn aangegeven. Binnen de vijf organisaties is afgestemd om het beleid bestuurlijk vast te laten stellen in de colleges respectievelijk in het Bestuur van Servicepunt71.
Bespreekpunten / beslispunten	Het bestuur wordt verzocht: 1. Het informatiebeveiligingsbeleid Servicepunt71 vast te stellen
Impact / consequenties	Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke en Servicepunt71-informatie te beschermen en te waarborgen dat de 5 organisaties voldoen aan relevante wet en regelgeving. Via deze kaderstelling wordt verder uitvoering gegeven aan alle activiteiten die bijdragen aan deze doelstelling.

Consequenties

Financiële consequenties:	Nee	ICT consequenties:	Nee
Personele consequenties:	Nee	Inkoop consequenties	Nee
Juridische consequenties:	Nee		

Zorg ervoor dat de juridische, financiële en/of personele consequenties in de bijlage(n) beschreven staan!

Communicatie

Communicatieverantwoordelijke	Opsteller van het stuk	
Communicatieboodschap	Het bestaande informatiebeveiligingsbeleid van Servicepunt71 is aan herziening toe. De leden van de VNG hebben besloten dat de "Baseline Informatiebeveiliging Gemeenten" het basisnormenkader is voor gemeenten voor informatieveiligheid. Op basis van deze baseline is het Informatiebeveiligingsbeleid voor de gemeenten in onze regio en voor Servicepunt71 geharmoniseerd opgesteld. Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen dat de 5 organisaties voldoen aan relevante wet en regelgeving.	
Hoe wordt hierover gecommuniceerd?	Intranet	

Is er sprake van een uiterste bespreekdatum?
Nee

Documenten die bij de bespreking bekend moeten zijn

Bijbehorend bestand	2670695_161123_Informatiebeveiligingsbeleid_Servicepunt71.docx	Bijbehorend bestand 5	
Bijbehorend bestand 2	2670696_161124_Oplegnotitie_Informatiebeveiligingsbeleid.docx	Bijbehorend bestand 6	

Naam beoordelaar	[redacted]	en die is	akkoord met de door mij aangepaste voorstel

Memo

Aan: Bestuur
Van: [redacted]
CC:
Datum: 18 november 2016
Doorkiesnummer: 7269
Betreft: Beleid Informatiebeveiliging
Opmerkingen:

0 Vooraf

In 2013 is er een regionaal Statuut Informatiebeveiliging opgesteld, dat destijds is vastgesteld door het bestuur van Servicepunt71 (d.d. 26 sep 2013) en in de regio door de colleges van Leiden, Leiderdorp, Oegstgeest en Zoeterwoude. Het Statuut bevat algemene uitgangspunten over de wijze waarop we gezamenlijk onze informatie willen beveiligen. Door de invoering van nieuwe regelgeving, wijzigingen in de organisaties en de invoering van de Baseline Informatiebeveiliging Gemeenten (BIG) is het Statuut niet meer actueel. Het Statuut legde de basis voor informatiebeveiliging en was feitelijk een intentieverklaring, waarin werd uitgesproken conform de BIG en in onderlinge samenwerking de informatiebeveiliging in de regio op orde te brengen. In het voorliggend beleidsstuk is nu nader invulling gegeven aan deze intentie, waarbij de organisatie van informatiebeveiliging is beschreven, de ontwikkelrichting is bepaald en de kaders zijn aangegeven.
Binnen de vijf organisaties is afgestemd om het beleid bestuurlijk vast te laten stellen in de colleges respectievelijk in het Bestuur van Servicepunt71.

Dit beleidsstuk past qua stijl en omvang minder goed bij de nieuwe manier van werken binnen Servicepunt71 (korte en bondige stukken) maar er is gekozen voor aansluiting bij de regio. Het beleid is regionaal uniform, waarbij alleen het hoofdstuk van de interne organisatie door elke organisatie is aangepast. In deze oplegnotitie zijn de meest relevante punten m.b.t. het informatiebeveiligingsbeleid, de samenhang met andere thema's en de specifieke rol van Servicepunt71 opgenomen.

1 Definitie Informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen teneinde de betrouwbaarheid (Beschikbaarheid, Integriteit, Vertrouwelijkheid) van de informatievoorziening te waarborgen.
Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen en te voldoen aan relevante wet en regelgeving. Het beleid heeft de volgende uitgangspunten:

- Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeenten en de relevante landelijke en Europese wet- en regelgeving.
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

2 Samenhang gegevensbescherming

Informatieveiligheid raakt/overlapt gegevensbescherming (privacy). Bij gegevensbescherming staat wetgeving centraal, waarbij informatieveiligheid de uitvoer en beheersing van deze wetgeving mede mogelijk maakt. Gegevensbescherming kan alleen gerealiseerd worden door borging van informatieveiligheid.

3 Samenhang programma VRIS

De maatregelen die uit dit beleid voort vloeien (implementatie aanpak BIG) worden opgepakt regionale werkgroep waarin Servicepunt71 participeert. Deze werkgroep is een onderdeel van het programma VRIS (Versterken Regionale I-Samenwerking) en daarin wordt o.a. de huidige informatiebeveiliging en gegevensbescherming geoptimaliseerd. De werkgroep leden zorgen voor afstemming en samenhang tussen deze twee thema's en met het programma VRIS.

4 Rol en verantwoordelijkheid Servicepunt71

Het beleid dat voorligt is het geharmoniseerd beleid van de 5 organisaties. Iedere organisatie heeft daarin een eigen verantwoordelijkheid t.a.v. de invoering van de BIG, zo ook Servicepunt71. Toch zijn niet alle maatregelen op Servicepunt71 van toepassing, omdat die specifiek voor gemeenten zijn.
Daarnaast heeft Servicepunt71 nog een andere verantwoordelijkheid als dienstverlener aan de gemeenten. De rol van Servicepunt71 binnen informatiebeveiliging i.r.t. de gemeenten heeft betrekking op:

- SP71 als uitvoerder van de gemeentelijke processen
- Beheerder van de centrale informatiesystemen en gegevens van gemeenten
- Adviseur op gebied van tactische en operationele maatregelen
- Beheer en onderhoud van de beveiligingsmiddelen
- Centraal aanspreekpunt of coördinatie bij beveiligingsincidenten of datalekken waar het door Servicepunt71 beheerde centrale voorzieningen betreft, of als aangewezen uitvoerder door betreffende (regio) gemeente
- Toezien op, en indien nodig het bijstellen van uit te voeren wijzigingen op de omgeving voor wat betreft de beveiliging of het waarborgen van de privacy
- Centraal aanspreekpunt IBD namens regiogemeenten
- Opstellen ; bewaken ; en bijhouden van regionale basis infrastructuur architectuur en beveiligingsarchitectuur, en het handhaven hiervan
- Opstellen standaards voor de infrastructuur

5 Uitvoering

Servicepunt71 is een shared-uitvoeringsorganisatie van de gemeenten en dus ook van de maatregelen die zij nemen op dit gebied. De gemeenten bepalen samen met Servicepunt71 de strategie en welke tactische en operationele maatregelen nodig zijn. Om dat te kunnen hebben de 4 gemeenten een inventarisatie gedaan naar hun huidige situatie voor wat betreft de basis beveiligingsniveau. Dit wordt getoetst aan de BIG en daaruit volgt een GAP-analyse. Uit de analyse blijkt welke maatregelen er genomen moeten worden. Er is daarbij een onderscheid tussen lokale maatregelen en regionale. De lokale maatregelen dienen verder geanalyseerd te worden om te kijken welke er ook op Servicepunt71 van toepassing zijn. Dit zijn bijvoorbeeld organisatorische maatregelen, zoals de Meldplicht Datalekken en een eigen PDCA cyclus voor het op peil houden van de eigen processen en procedures. Servicepunt71 zal daarnaast ook een eigen analyse uitvoeren op activiteiten die geen relatie hebben met voorgaande gemeentelijke inventarisaties.
De regionale maatregelen monden uit in een uitvoeringsplan inclusief een termijnplanning. Hierin participeert Servicepunt71 als leverancier en informatie-eigenaar, waarbij er een opdracht van de vijf organisaties aan Servicepunt71 (als leverancier) volgt inclusief een kosteninschatting en dekkingsvoorstel. Na regionale goedkeuring (door SGB, als collectief opdrachtgever) van deze aanpak kan er worden overgegaan tot het projectmatig uitvoeren van de betreffende maatregelen door Servicepunt71 i.s.m. de gemeenten.

Informatiebeveiligingsbeleid Servicepunt71

Versie 0.2 Concept
18-11-2016

Versiebeheer

0.1	10-11-2016	Versie 0.1, op basis van Versie 0.4 van Informatiebeveiligingsbeleid Gemeente Oegstgeest
0.2	18-11-2016	Versie 0.2 aanpassingen na bespreking [redacted]

Inhoudsopgave

1 Inleiding

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging (IB). Deze uitgangspunten hebben een sterk normerend karakter, geven keuzes weer en zijn te beschouwen als het optimum beleid gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). In dit document is een aanzienlijk aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die gemeente breed voor alle processen en systemen moeten gaan gelden. Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning en control cyclus.

In 2013 is regionaal beleid ontwikkeld op het vlak van informatiebeveiliging. Dit document vervangt het Regionaal Statuut Informatiebeveiliging (d.d. 26 sep 2013) waarin de gemeenten Leiden, Leiderdorp, Zoeterwoude, Oegstgeest en Servicepunt71 gezamenlijke beleidsafspraken hebben gemaakt rondom informatiebeveiliging.

Dit document is in samenwerking tussen de gemeenten Leiden, Leiderdorp, Zoeterwoude, Oegstgeest en Servicepunt71 opgesteld. De uitgangspunten van dit document zijn voor elk van deze organisaties gelijk, voor wat betreft de organisatievormen heeft elk van deze organisaties het document 'op maat gesneden'. De gemeenten Leiderdorp, Zoeterwoude en Oegstgeest hebben in aanvulling op het bovengenoemde Statuut een addendum opgesteld; de Governance en Incidentenprocedure. De relevante punten uit dit addendum zijn als uitbreiding in dit beleid opgenomen en dus ook door Servicepunt71 overgenomen. Hiermee wijkt het beleid enigszins af van het door gemeente Leiden vastgestelde beleid.

Toegepast zijn de hoofdstukken uit de Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten. Deze kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden.

- Beveiligingsbeleid;
- Organisatie van informatiebeveiliging;
- Beheer van bedrijfsmiddelen;
- Beveiliging van personeel;
- Fysieke beveiliging en beveiliging van de omgeving;
- Beheer van communicatie- en bedieningsprocessen;
- Toegangsbeveiliging;
- Verwerving, ontwikkeling en onderhoud van informatiesystemen;
- Beheer van informatiebeveiligingsincidenten;
- Bedrijfscontinuïteitsbeheer;
- Naleving.

1.1 Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. 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;

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

integriteit / betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

1.2 Waarom informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden 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.

1.3 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 informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen.

1.4 Samenwerking

In 2013 is regionaal beleid ontwikkeld op het vlak van informatiebeveiliging. Dit Statuut Informatiebeveiliging is destijds vastgesteld door het bestuur van Servicepunt71 en in de regio door de colleges van Leiden, Leiderdorp, Zoeterwoude en Oegstgeest. Het Statuut bevat algemene uitgangspunten voor hoe we gezamenlijk onze informatie willen beveiligen. Door de invoering van nieuwe regelgeving, wijzigingen in de organisaties en de invoering van de Baseline Informatiebeveiliging Gemeenten (BIG) is het Statuut niet meer actueel. Ook de bescherming van vertrouwelijke – en persoons - gegevens kan niet worden geborgd zonder een adequate informatiebeveiliging. Via het programmaplan Versterken Regionale I-Samenwerking (VRIS) wordt o.a. de huidige informatiebeveiliging en gegevensbescherming geoptimaliseerd.

1.5 Verantwoordelijkheden

Het bestuur en management speelt een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid van is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

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

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor degelijk onderbouwde afweging en prioritering op basis van het 'pas toe of leg uit' principe.

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

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het College van B&W 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 én 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 organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

3. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.

4. De CISO (Chief Information Security Officer, in voormalig Statuut Coördinator Informatiebeveiliging) ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.

5. De gemeente 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 gemeente 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.

1.6 Werking

Dit IB-beleid treedt in werking na vaststelling door college van B&W/ Bestuur Servicepunt71. Hiermee komt het Statuut informatiebeveiliging (d.d. 26 sep 2013) van de gemeenten Leiden, Leiderdorp, Zoeterwoude en Oegstgeest & Servicepunt71 van 2013 te vervallen.

2 Uitgangspunten informatiebeveiliging

2.1 Samenhang

De nu volgende hoofdstukken corresponderen met de hoofdstukken 5 tot en met 15 uit de Tactische variant van de BIG. Ze geven een nadere invulling van het gemeentelijk informatiebeveiligingsbeleid. Informatieveiligheid raakt/overlapt gegevensbescherming (privacy), bij gegevensbescherming staat wetgeving centraal, waarbij informatieveiligheid de uitvoer en beheersing van deze wetgeving mede mogelijk maakt. Gegevensbescherming kan alleen gerealiseerd worden door borging van informatieveiligheid.

2.2 Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de 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. IB is het proces dat dit belang dient.

2.3 Visie

De komende jaren zetten de gemeenten Leiden, Leiderdorp, Zoeterwoude, Oegstgeest én Servicepunt71 zelf in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente 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. Daarbij is verantwoord en bewust gedrag van medewerkers essentieel voor informatieveiligheid.[2]

2.4 Doelstelling

Dit IB-beleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving. De gemeente 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 gemeente weet welke maatregelen genomen zijn 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.

2.5 Uitgangspunten

Het informatiebeveiligingsbeleid van de gemeente is in lijn met het algemene beleid van de gemeente 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 college van B&W/ Bestuur Servicepunt71. De Directie herijkt periodiek het IB-beleid.

2.6 Risicobenadering

De aanpak van informatiebeveiliging in de gemeente 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 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.

2.7 Doelgroepen

Het IB-beleid is bedoeld voor alle in- en externe medewerkers vanServicepunt71:

Doelgroep	Relevantie voor IB-beleid

[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 Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor de gemeente verricht.

[3] Daarbij geldt het pas toe of leg uit principe

Bestuur	Integrale verantwoordelijkheid
Directie	Kaderstelling en implementatie
Controller (Informatieveiligheid)	Verbijzonderde interne controle op naleving informatiebeveiligingsbeleid en realisatie van voorgenomen veiligheidsmaatregelen
(regionale) CIO	Kaderstelling en implementatie
CISO/Coördinator Informatiebeveiliging	Ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover
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
•	Dagelijkse coördinatie en werkzaamheden van IB
Privacy beheerder	Afstemming tussen privacy en IB
(regionale) Functionaris Gegevensbescherming	Afstemming tussen privacy en IB
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT-diensten (en -ontwikkelaars)	Technische beveiliging
Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners (inclusief Servicepunt71)	Compliance

2.8 Scope

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente 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 gemeentelijke IB-beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.[4]

2.9 IB-beleid en architectuur

IB is onderdeel van de informatiearchitectuur van Servicepunt71 en wordt (regionaal als onderdeel van programma VRIS) uitgewerkt in de IB-architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie).[5]

2.10 Bewustwording als randvoorwaarde

Veilig omgaan met gegevens is mensenwerk. Management en medewerkers dienen zich bewust te zijn van de risico's die samenhangen met de omgang met vertrouwelijke- en persoons gegevens en van de noodzaak van informatiebeveiliging. Bewustwording (communicatie) ten aanzien van informatiebeveiliging en gegevensbescherming is van groot belang voor een succesvolle implementatie van de BIG. Zowel regionaal als lokaal zal hier continu op worden ingezet.

[4] Bijvoorbeeld SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties.

[5] De processen van informatiebeveiliging zijn onderdeel van de GEMeentelijke Model Architectuur (GEMMA) om daarmee de basis voor informatieveiligheid te verankeren als integraal onderdeel van de bedrijfsvoering.

3 Organisatie van de informatiebeveiliging

3.1 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.

3.2 Doelstelling:

Beheren van de 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.

3.3 Verantwoordelijkheden

Het Bestuur is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de gemeente.[6]

- stelt kaders voor IB op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;

De Directie (in sturende rol) is verantwoordelijk voor kaderstelling en sturing. De directie:

- stuurt op concern risico's; het betreft hier risico's die impact hebben op de informatieveiligheid en niet binnen één specifiek team zijn te adresseren maar de gehele organisatie aangaan;
- 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 afdelingen binnen de organisatie (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.[7] De managers:

- stellen op basis van een expliciete risicoafweging betrouwbaarheidseisen voor door hen gebruikte informatiesystemen vast (classificatie);
- zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- rapporteren, via de CISO, over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

Team Bedrijfsvoering en de afdelingen ICT, HRM, etc., in uitvoerende rol zijn verantwoordelijk voor uitvoering;

- 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.

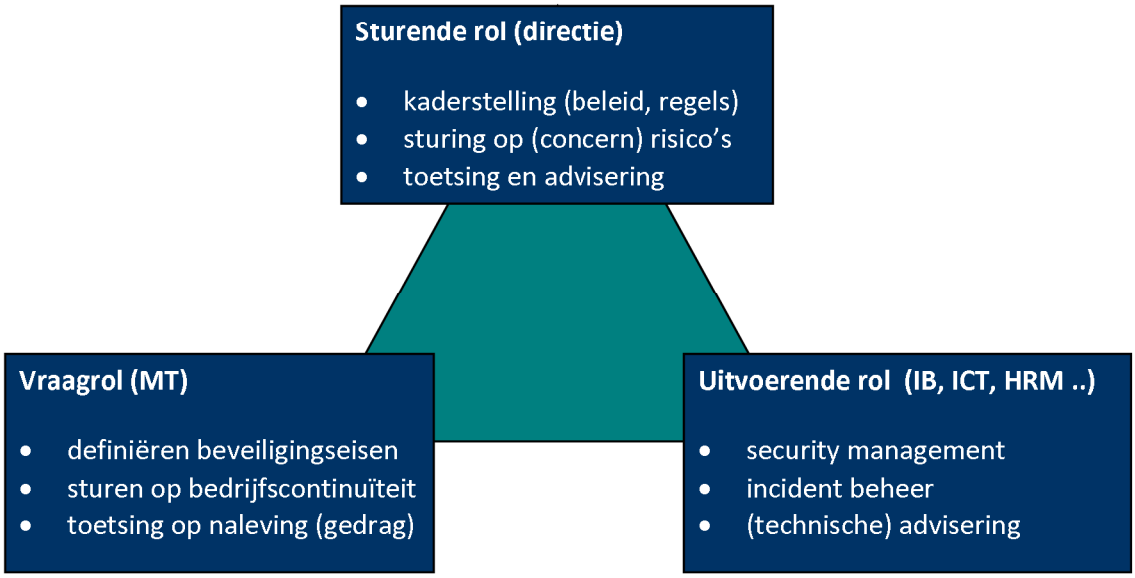
De controller informatieveiligheid heeft in ieder geval de volgende verantwoordelijkheden:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- De controle op de voortgang van het uitvoeren van de maatregelen uit het informatiebeveiligingsplan;
- De controle op de periodieke actualisatie van informatiebeveiligingsbeleid en op het Informatie-beveiligingsplan;
- Toetsen/bewaken van het niveau van informatiebeveiliging;
- Evalueren van beveiligingsincidenten.

---

[6] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten

[7] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten



Figuur 1: relaties

3.4 Taken en rollen

Het Bestuur stelt formeel het IB-beleid vast en kan de opdracht geven om dit te (laten) controleren. De directie adviseert het Bestuur formeel over vast te stellen beleid.

De CIO (Chief Information Officer)[8] geeft namens de directie 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 CISO. De CISO bevordert en adviseert gevraagd en ongevraagd over IB en rapporteert minimaal eenmaal per jaar organisatie breed aan de directie over de stand van zaken.

De coördinatie van informatiebeveiliging is idealiter belegd bij een strategische adviesfunctie binnen alle teams. Uitvoerende taken zijn zoveel mogelijk belegd bij i-security functionarissen. De teams rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de P&C cyclus.

Binnen Servicepunt71 is de CISO tegelijkertijd ook de coördinator informatiebeveiliging voor dagelijks beheer van de (technische) IB-aspecten. Informatiebeveiliging is onderdeel van de service management rapportage.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Sturen: **Directie dagelijkse uitvoering:** **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. Rapportage aan directie/ Bestuur
Vragen:	Formuleren van beveiligingseisen	Stimuleren van beveiligingsbewustzijn	Interne controle (IC), sturen op naleving van	Verbeteren bedrijfscontinuïteit.

[8] Alleen in Leiden is een CIO benoemd, in VRIS wordt gekeken naar de mogelijkheden voor het aanstellen van een regionale CIO. Zolang dit niet het geval is, deze rol belegd bij de gemeentesecretaris. Bij Servicepunt71 wordt dit voorlopig opgepakt door de directeur.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Alle teams	(classificatie) en opstellen clusterbeleid en beveiligingsplannen.	bij medewerkers, risico- en bedrijfscontinuïteit-management.	regels door medewerkers (gedrag), compliancy.	Rapportage aan CIO/CISO.
Uitvoeren: **Team Interne Bedrijfs-voering**	Beleidsvoorberei- ding, technische onderzoeken (marktverkenningen).	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies.	Scanning op kwetsbaarheden, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de CIO over aanpassingen aan de informatievoorziening.

Naast de bovengenoemde verantwoordelijkheden, taken en rollen zijn er nog een aantal taken en rollen die een relatie hebben met informatieveiligheid. Deze worden nader beschreven in bijlage 1.

3.5 Functioneel overleg

De CISO is voorzitter van het Overleg informatiebeveiliging dat 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- CISO;
- Coördinator Informatiebeveiliging Servicepunt71
- Controller Informatieveiligheid
- Beveiligingsbeheerders t.a.v.: BRP, Waardedocumenten, BAG, SUWI en DigiD;
- Beveiligingsbeheerders t.a.v.: FZ, ICT en DIV
- Privacy beheerder(s);
- Agendaleden: MT lid of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen Beveiligingsplan c.q. Plan van Aanpak (minimaal 2 keer per jaar bespreken);
- Veiligheidsincidenten;
- Planning en voorbereiding van Audits en controles;
- Evaluatie en actualisatie informatiebeveiliging en informatiebeveiligingsplan.

Daarnaast vindt afstemming plaats tussen de CISO en de functioneel applicatie- en gegevensbeheerder(s) en de procesverantwoordelijke(n) van (informatie)systemen.

De CISO's van de gemeenten Leiderdorp, Leiden, Zoeterwoude, Oegstgeest en de Coördinator Informatiebeveiliging van Servicepunt71 vormen gezamenlijk een regionaal informatiebeveiligingsoverleg. Het regionaal beveiligingsoverleg evalueert beleid, coördineert gezamenlijke beveiligingsissues, toetst het gekozen beveiligingsniveau en controleert op de uitvoering en naleving van het informatiebeveiligingsbeleid.

3.6 Rapportage en escalatielijn voor IB

(Decentrale) Security verantwoordelijke → CISO (→ (regionale) CIO) → directie

3.7 Externe partijen

IB-beleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt).[9] Ook voor externe partijen geldt hierbij pas toe of leg uit beginsel.

Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoopvoorwaarden (minimaal inkoopvoorwaarden ARBIT-2014), 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

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

contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren.[10]

Voor het tot stand brengen van datakoppelingen met externe partijen, geldt naast generiek IB-beleid ook een gemeentelijke aanvraag procedure via Servicepunt71. Het doel van de procedure is risicobeheersing.

Voor externe hosting van data en/of services gelden naast generiek IB-beleid de richtlijnen voor cloud computing.[11] De gemeente is minimaal gehouden aan:

- regels omtrent grensoverschrijdend dataverkeer;
- toezicht op naleving van regels door de externe partij(en);
- hoogste beveiligingseisen voor bijzondere categorieën gegevens;[12]
- melding bij Autoriteit Persoonsgegevens (voorheen CBP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

NB; Regionaal wordt (vanuit VRIS) een beleid uitgewerkt voor cloud computing.

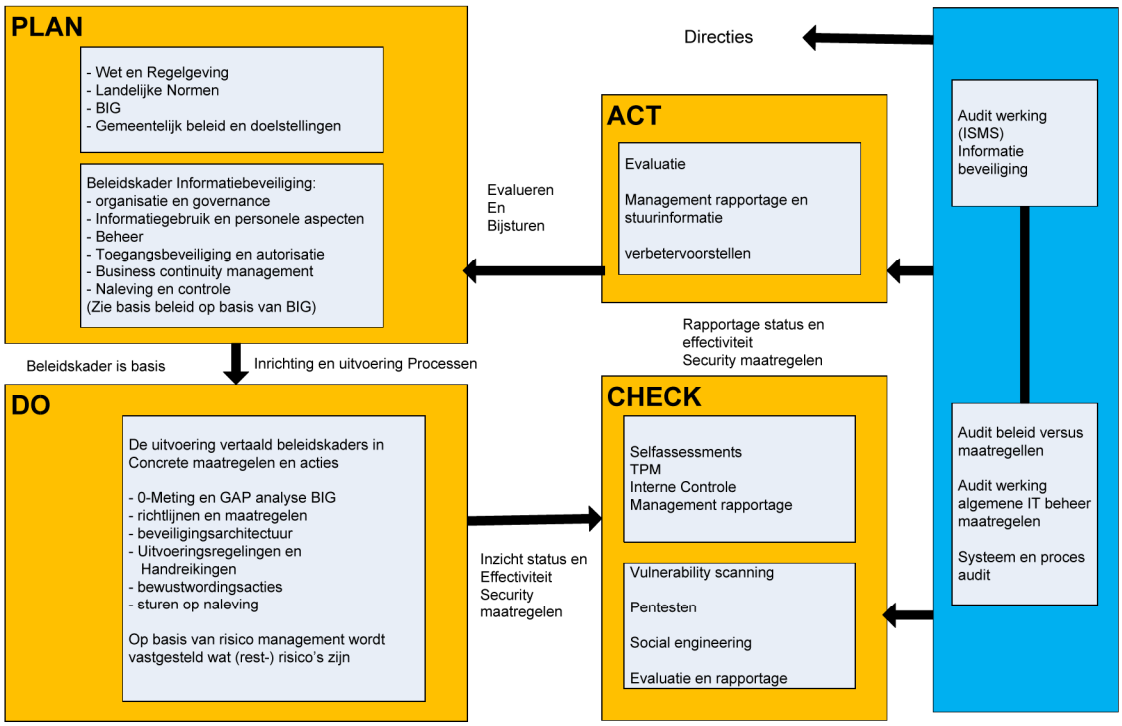
3.8 ICT crisisbeheersing en samenwerking

Voor interne crisisbeheersing dient een kernteam IB geïnstalleerd te zijn, bestaande uit CISO/ Coördinator Informatiebeveiliging, relevante experts en communicatie. De werkwijze is vastgelegd in het "Proces melden datalek – beveiligingsincident".

De gemeente en Servicepunt71 participeert in relevante regionale en landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde IB-platforms.

3.9 PDCA

Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[13] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.



Figuur 2: Information Security Management System

[10] Hiervoor kan gebruik worden gemaakt van een 'third party mededeling' (TPM) of een ISAE 3402-verklaring.
[11] Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[12] 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
[13] NEN/ISO 27001

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. Dit beleid wordt 1 keer per 4 jaar geactualiseerd of zoveel eerder als hier een directe aanleiding toe is. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het regionale Programmaplan VRIS en uitgewerkt in het informatiebeveiligingsplan (IB-beleid) van de gemeente. Team specifieke activiteiten worden gepland in de teamplannen.

- 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.

  - Interne controle: jaarlijks wordt de risico analyse geactualiseerd

  - Externe controle: betreft controle buiten het primaire proces door een auditor.[14] Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd. Bevindingen worden gerapporteerd aan de directie.

- 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.

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

4 Beheer van bedrijfsmiddelen

4.1 Verantwoordelijkheid voor bedrijfsmiddelen

4.1.1 Risico's:

Bedrijfsmiddelen[15] 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 geïdentificeerd zijn en 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.
- Regels vaststellen, documenteren en 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 gemeentelijke informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken gemeentelijke informatie voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van gemeentelijke 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 gemeentelijke 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 gemeentelijke 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 gemeente gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
    - aan de werkplek verbonden risico's;
    - het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

4.2 Classificatie van informatie

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

---

[15] software, hardware (computers, printers, USB sticks, harddisks, tablets, smartphones etc.) sleutels, toegangspasjes etc.

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 (wel tegen het aanpassen ervan!). De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

4.2.1 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.

4.2.2 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.

4.2.3 Beheersmaatregelen:

Informatie classificeren met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

Opstellen en uitdragen classificatiebeleid binnen de gemeente.

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** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente)*	**Niet zeker (Beschermd?)** informatie mag worden veranderd (niet door iedereen) *(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 intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** 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: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*
Hoog	**Geheim** informatie is alleen toegankelijk voor	**Absoluut** het bedrijfsproces staat geen	**Essentieel** informatie mag alleen in uitzonderlijke situaties

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
	direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	fouten toe *(bv: gemeentelijke informatie op de website)*	uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

4.2.4 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 "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 én daarnaast verdient een technische oplossing altijd de voorkeur boven gedragsverandering. Maar een technische beveiligingsmaatregel heeft echter geen werking zonder een of meer organisatorische maatregelen.

4.2.5 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.[16] Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

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

5 Beveiliging van personeel

5.1 Risico's

Het aannemen of inhuren van personeel en het laten verrichten van werkzaamheden door (externe) medewerkers verdient aandacht. Informatiebeveiliging is mensenwerk. Management en medewerkers dienen zich bewust te zijn van risico's die samenhangen met de omgang met vertrouwelijke gegevens en de noodzaak van informatiebeveiliging.

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.

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 HR-afdeling 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 herhaald 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 gemeente 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 geregeld in de CAR-UWO (rechten en plichten als ambtenaar). Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

5.4 Bewustwording

- De gemeente/ de directie/ de teams bevorderen algehele communicatie en bewustwording rondom informatieveiligheid.
- Het lijnmanagement bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen.
- 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 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.

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 gemeente 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 gemeente 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.

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.
- De gemeente 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 gemeente op straat komen te liggen. De gemeente 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.
- Het ontbreken van een regeling voor antivirus bescherming 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

- 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 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 gemeente 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 IB-beleid en algemeen gemeentelijk beleid;
- vooraf gemeld bij ICT t.b.v. toetsing op beheeraspecten;
    - voldoet aan geldende wet- en regelgeving.

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. 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.

7.3.3 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 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 continue 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 gemeente moet kunnen worden geïdentificeerd.
- 'Mobile code'17 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.
- Alle informatie, die wordt geplaatst op websites van de gemeente, 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.

7.4 Mobiele (privé-)apparatuur en thuiswerkplek

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente 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 gemeente 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 gemeentelijke informatie en integriteit van het gemeentelijke 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.

7.5 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.

---

[17] 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.

- 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.

7.6 Informatie-uitwisseling

- Voor het gebruik van gemeentelijke informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, geheimhoudingsverklaring, huisregels.
- Digitale documenten van de gemeente 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.

7.7 Controle[18]

- 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.[19] 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.

7.8 Beheer van de dienstverlening door een derde partij

7.8.1 Risico's

De gemeente 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 gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

7.8.2 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 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.

7.8.3 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.

---

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

[19] 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.

- Wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd.

7.8.4 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 medewerkers thuis leidt tot hogere beveiligingsrisico's.

7.9 Behandeling van media

7.9.1 Risico's

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

7.9.2 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.

7.9.3 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.

7.9.4 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 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, tablets, voor wanneer deze niet meer worden gebruikt.
- Encryptie op informatie met het classificatielabel vertrouwelijk en zeer geheim.

7.10 Uitwisseling van informatie

7.10.1 Risico's

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

7.10.2 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.

7.10.3 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.

7.10.4 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 gemeentelijke informatie dient te worden vastgesteld.[20] Logische toegang is gebaseerd op de classificatie van de informatie.

8.1 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).

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 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 dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts.
- De gemeente maakt ,waar mogelijk, gebruik van bestaande (landelijke) 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[21], deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen.
- 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).

8.5 Externe toegang

- De gemeente kan een externe partij toegang verlenen tot het gemeentelijke 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 gemeente, tenzij uitdrukkelijk overeengekomen.
- De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente 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 logisch gescheiden van het gemeentelijke bedrijfsnetwerk.
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Gemeentelijke informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen.[22]

---

[20] Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.

[21] Het wachtwoordbeleid is uitgewerkt in het wachtwoord beleids document van de gemeente.

[22] Separaat document

- 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) niet geschikt voor het delen van vertrouwelijke en geheime informatie.

8.7 Overige maatregelen

Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur.

Het netwerk van de gemeente is waar mogelijk 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 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[23]).
- 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 gemeentelijk 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.

8.9 Softwareontwikkeling en onderhoud

- Applicaties worden ontwikkeld en getest o.b.v. landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties.[24] Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10.[25]
- 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 medewerkers, die deze code onderhouden of installeren.
- 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.

8.10 Encryptie (versleuteling)

- De gemeente gebruikt encryptie conform PKI-overheid standaard.[26]
- Intern dataverkeer ('machine to machine') wordt conform classificatie beveiligd met certificaten.
- Beveiligingscertificaten worden centraal beheerd binnen de gemeente.

---

[23] Dit zijn Prince2 termen, zie hiervoor de projectmanagement methodiek Prince 2

[24] Nationaal Cyber Security Centrum, NCSC

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

[26] 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

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 CISO van de gemeente.
- Beveiligingsincidenten die worden gemeld bij de service desk van Servicepunt71, worden als zodanig geregistreerd en voorgelegd aan de Coördinator Informatiebeveiliging van Servicepunt71. Voor afhandeling geldt de reguliere rapportage en escalatielijn.
- Afhankelijk van de ernst van een incident is er een meldplicht bij de Autoriteit Persoonsgegevens.[27]
- Ernstige incidenten, waarbij een alarmfase (zie onder) in werking treedt, worden opgenomen in de rapportage van de CISO. Er wordt minimaal eenmaal per jaar gerapporteerd aan het management door de CISO.

9.4 Alarmfasen

Bij grote incidenten wordt gehandeld en opgeschaald conform de draaiboeken ICT- crisisbeheersing en of het proces melden datalek en beveiligingsincident.

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. Melding bij IBD indien nodig. Gemeentelijke communicatie is optioneel.
3	Concernbreed ICT-incident (en mogelijk andere gemeenten)	Impact op de gemeentelijke dienstverlening wordt echt ervaren.	Kernteam komt bij elkaar. Afhankelijk van het incident (impact) treedt de GRIP structuur in werking. Bestuur, CIO en directies worden geïnformeerd.	Melding aan CISO. Melding bij IBD (indien nodig). Gemeentelijke afdeling communicatie is vereist.
4	ICT-Incident is concern overstijgend	Impact op de gemeentelijke dienstverlening is	Mogelijk treedt de GRIP structuur in werking. Het kernteam is dan in beginsel adviserend en	Er is sprake van landelijke opschaling via de technische lijn (IBD → NCSC) of via de

[27] De WBP wordt hierop aangepast, er is tevens een EU verordening op handen (2016 en verder)

Alarm fase	Kenmerk	Impact	Opschaling	Bijzonderheden
	(landelijk)	manifest.	voert desgewenst coördinatie (binnen het ICT domein).	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 (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

10.2 Doelstelling

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

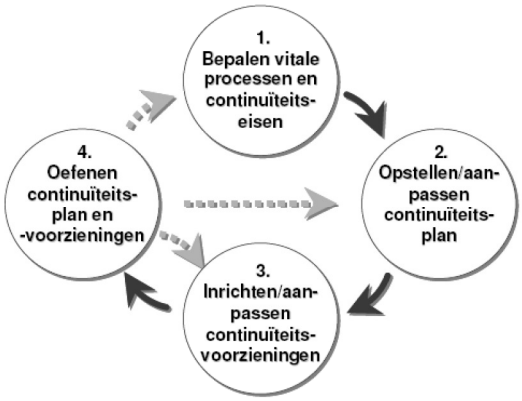
Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.

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

10.3 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

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 gemeentelijke 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 (regionaal) CIO) voor het toezicht op de uitvoering van het IB-beleid.
- ICT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het IB-beleid. 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, SUWI en GBA. Aanvullend op dit concern IB-beleid kunnen daarom specifieke normen gelden voor teams.[28]
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de (regionaal) CIO of CISO onderzocht door gemeentelijke auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). Jaarlijks worden ca. 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

Een overzicht van relevante wet en regelgeving is te vinden bij KING[29]. Zo is het gebruik van persoonsgegevens geregeld in de Wet Bescherming Persoonsgegevens[30].

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 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.

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

Bijlage 1 – Aanvullende rollen, taken en verantwoordelijkheden

De CISO heeft in ieder geval de volgende verantwoordelijkheden:

- Coördineert het formuleren van informatiebeveiligingsbeleid;
- Stelt het informatiebeveiligingsplan op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering van informatiebeveiligingsmaatregelen uit het informatiebeveiligingsplan;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatiebeveiliging;
- Ondersteunt de directie en de leidinggevenden met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatiebeveiliging;
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de Informatiebeveiligingsplannen;
- Bevorderen van het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Toetst of informatiebeveiliging een onderdeel uitmaakt van het informatieplannings-, systeemontwikkelings- en onderhoudsproces;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C cyclus. Hierbij bundelt de coördinator de deelbijdragen van de teammanagers.

Security officer SUWI, is belast met;

- het beheer van beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd;
- het bevorderen van en adviseren over de beveiliging van Suwinet;
- het houden van toezicht op het naleven van de maatregelen zoals beschreven in het Informatiebeveiligingsplan SUWI;
- het gevraagd en ongevraagd adviseren van medewerkers en management en het doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet;
- het beheren van het informatiebeveiligingsplan SUWI.

Beveiligingsbeheerder DigiD, is belast met;

- het beheer van beveiligingsprocedures en -maatregelen in het kader van DigiD, zodanig dat de beveiliging van DigiD overeenkomstig wettelijke eisen is geïmplementeerd;
- het bevorderen van en adviseren over de beveiliging van DigiD;
- het houden van toezicht op het naleven van de maatregelen geldend voor DigiD (o.a. normenkader DigiD audit);
- het gevraagd en ongevraagd adviseren van medewerkers en management en het doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van DigiD;
- het aanspreekpunt zijn voor de betrokken leverancier(s);
- het laten uitvoeren van de jaarlijkse DigiD audit;
- het opvolgen/implementeren van aanbevelingen vanuit de DigiD audit.

Rollen en functies binnen de gemeente brede informatieveiligheidsorganisatie volgens de Baseline Informatiebeveiliging Nederlandse Gemeenten;

Rol	Functie	Indien van toepassing: vervangende functie
FG regionaal		
CIO lokaal (belegd bij gemeentesecretaris)		
CIO regionaal (kwartiermaker)		
CISO		
Controller informatieveiligheid		
Beveiligingsbeheerder BRP		
Beveiligingsfunctionaris Reisdocumenten		
Beveiligingsfunctionaris Rijbewijzen		
Beveiligingsbeheerder BAG		
Beveiligingsbeheerder DigiD		
Beveiligingsbeheerder SUWI (Security Officer SUWI)		
Beveiligingsbeheerder Facilitaire Zaken		
Coördinator Informatiebeveiliging bij Servicepunt71		
Beveiligingsbeheerder DIV		
Privacy beheerder (Wet Bescherming Persoonsgegevens)		
Privacy beheerder BRP		
ACIB (Algemeen Contactpersoon Informatie Beveiligingsdienst)		
VCIB (Vertrouwd Contactpersoon Informatie Beveiligingsdienst)		

NB; op intranet is deze tabel te vinden waarbij er namen zijn ingevuld. Hiervoor is gekozen om te voorkomen dat er namen in dit beleid komen te staan.

Bijlage 2 - Relevante documenten en bronnen.

Intern

- VRIS Programmaplan

Extern

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging) (2007)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), KING, 2013
    - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
    - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- CBP richtsnoeren 'beveiliging van persoonsgegevens', http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
- GEMMA: http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/e-dienstverlening-verbeteren/gemma
- Gemma referentiecomponenten Informatiebeveiliging
- Algemene Inkoopvoorwaarden (ARBIT-2014)