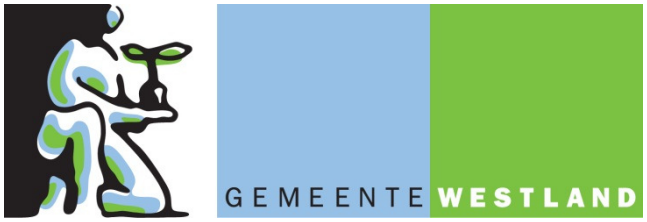
Gemeentebreed Informatiebeveiligingsbeleid

Versie	: 1.1 definitief
Auteurs	: Marvin Suijker, Sandra Paulusma, Nico Olsthoorn, Eelco Teesink, Sander van Gulik, Natascha Banziger, Ingrid Slaman, Gerard Witkamp, Carla Wezenaar, Karel Alleblas, Albert van Harling, Michel Jansen Vreeling, Roland van de Bosch,
Datum	: 1 augustus 2014
Corsa	: 14-0428020



I Voorwoord

I.I Totstandkoming

In dit document wordt het gemeentebreed informatiebeveiligingsbeleid beschreven van de gemeente Westland.

Het informatiebeveiligingsbeleid is gebaseerd op de internationale standaarden voor informatiebeveiliging: NEN/ISO 27001 en NEN/ISO 27002. Op basis van deze standaard is onlangs de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING 2013) opgeleverd. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de veiligheid van informatie binnen gemeentelijke organisaties. De uitgangspunten uit deze baseline zijn integraal opgenomen in dit gemeentebrede informatiebeveiligingsbeleid. Evenals de richtlijnen van het DigID veiligheidsassessment (DigiD audit). Hierdoor is een actueel en volledig naar de laatste inzichten opgesteld beleidsplan voor de gemeente Westland ontstaan.

Het beleid is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en management die in het kader van werkzaamheden of een project moeten weten aan welke kwaliteitsaspecten aandacht moet worden besteed. De intentie is niet dat alle medewerkers exact weten wat er in het gemeentebreed informatiebeveiligingsbeleid staat, maar men moet wel weten dat het beleid er is, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn.

De basis van dit informatiebeveiligingsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING 2013). De specifieke invulling voor de gemeente Westland heeft plaatsgevonden door middel van interviews met medewerkers en management uit verschillende delen van de organisatie en een aantal workshop met een brede afvaardiging uit de organisatie. Tijdens deze bijeenkomsten zijn de specifieke gemeentelijke inzichten en accenten opgehaald.

I.II Leeswijzer en ambitieniveau

Dit document bevat een groot aantal beleidsuitgangspunten op het gebied van de veiligheid van gemeentelijke informatieprocessen. Deze brede set van uitgangspunten staat echter los van het ambitieniveau van de gemeente om direct aan al deze beleidsuitgangspunten praktische invulling te geven.
Een deel van de benoemde aandachtgebieden wordt tijdens de fase van risicoanalyse geïnventariseerd en op dat moment van een prioriteit voorzien. De gemeente maakt tijdens dit proces zelf keuzes over de prioritering en fasering van de implementatie van de onderdelen van het beleidsplan.
Een ander deel van de beleidsuitgangspunten heeft betrekking op aandachtgebieden die pas actueel worden indien de gemeente voor een dergelijke keuze of vraagstuk staat, bijvoorbeeld de inzet van Cloudtechnologie, Bring Your Own Device (BYOD), gezamenlijk uitbesteden van software ontwikkeling of de aanschaf van een nieuw informatiesysteem. In dat specifieke geval hanteert de gemeente de beleidsuitgangspunten in dit document om de veiligheid van informatie bij deze keuze te vergroten.

Het ambitieniveau dat wel met dit document wordt bepaald wordt gevormd door de meetlat die de gemeente hanteert bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen. Deze meetlat is specifiek opgesteld voor de Nederlandse gemeenten en is in dit document naar de specifieke situatie van de gemeente Westland vertaald.

1. Waarom informatiebeveiliging?

1.1 Inleiding

De gemeente Westland is een informatie-intensieve organisatie met een sterke focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeente moeten kunnen beschikken over betrouwbare informatie om de klanten optimaal te kunnen helpen en adviseren. Daarnaast moeten burgers en bedrijven er op kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

Informatisering speelt een steeds prominentere rol in de gemeentelijke organisatie. Deze rol wordt in het kader van het stelsel van basisregistraties en de toenemende complexiteit van het digitale dienstverleningskanaal steeds belangrijker. Ook de gemeente Westland richt zich op het koppelen van systemen waardoor grote gegevensverzamelingen ontstaan die vervolgens weer specifieke informatie opleveren voor interne en externe afnemers.

Daarnaast is de gemeente steeds afhankelijker van goed werkende informatievoorzieningen en -systemen. Dit betekent dat de gemeente Westland alert is op mogelijke verstoringen van of bedreigingen gericht op informatiesystemen, mede omdat veel informatiesystemen niet zijn ontworpen met het oog op veiligheid. De veiligheid die met de technische middelen kan worden bereikt is begrensd en wordt al vanouds ondersteund met passende beheerprocessen en procedures. Daarnaast speelt echter de menselijke factor (het menselijk gedrag) een steeds grotere rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk. Deze factor speelt, door de steeds complexer wordende informatieprocessen, veelal zelfs een doorslaggevende rol.

Informatie kan in verschillende vormen bestaan. Het kan zijn geschreven, gesproken, gedrukt of digitaal zijn opgeslagen. Het wordt per post of via digitale media verzonden. Al deze verschijningsvormen van informatie vragen voor een deel eenzelfde generieke aanpak, maar kennen ook verschillen. Dit document besteedt hier aandacht aan.

De veiligheid van informatie speelt binnen een groot aantal gebieden van de gemeente een rol. Om te voorkomen dat binnen elk van die gebieden (bijvoorbeeld rondom de SUWI, DigiD, BRP of BAG) separaat beleid ontwikkeld en geïmplementeerd moet worden, is de keuze gemaakt dit gemeentebrede informatiebeveiligingsbeleid op te stellen. Hierbij worden organisatiebrede, overkoepelende onderwerpen geïntegreerd en in algemeen beleid en algemene procedures vastgelegd. Specifieke zaken worden per werkgebied in aparte onderdelen opgenomen.

In het gemeentebrede informatiebeveiligingsbeleid wordt op strategisch/ tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatiebeveiliging van de gemeente Westland. Dit document zal samen met de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie moeten opleveren waardoor de kwaliteitskenmerken van informatie, te weten: de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatie binnen de organisatie zijn gewaarborgd.

1.2 De informatiebeveiligingspiramide

Ook de centrale overheid heeft veel aandacht voor de veiligheid van informatie binnen de verschillende overheidslagen. Naast het ontwikkelen van nieuwe wet en regelgeving op dit gebied uit zich deze aandacht ook in bewustwordingscampagnes en ondersteuning van gemeentelijke overheden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen. De ontwikkeling door KING/VNG van de de Baseline Informatiebeveiliging Nederlandse Gemeenten (2013) vormt hiervan een voorbeeld. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die is gebaseerd zijn op de internationale standaarden voor informatiebeveiliging NEN/ISO 27001 en 27002, bieden een meetlat voor gemeenten om hun Informatiebeveiliging op orde te brengen en te houden.

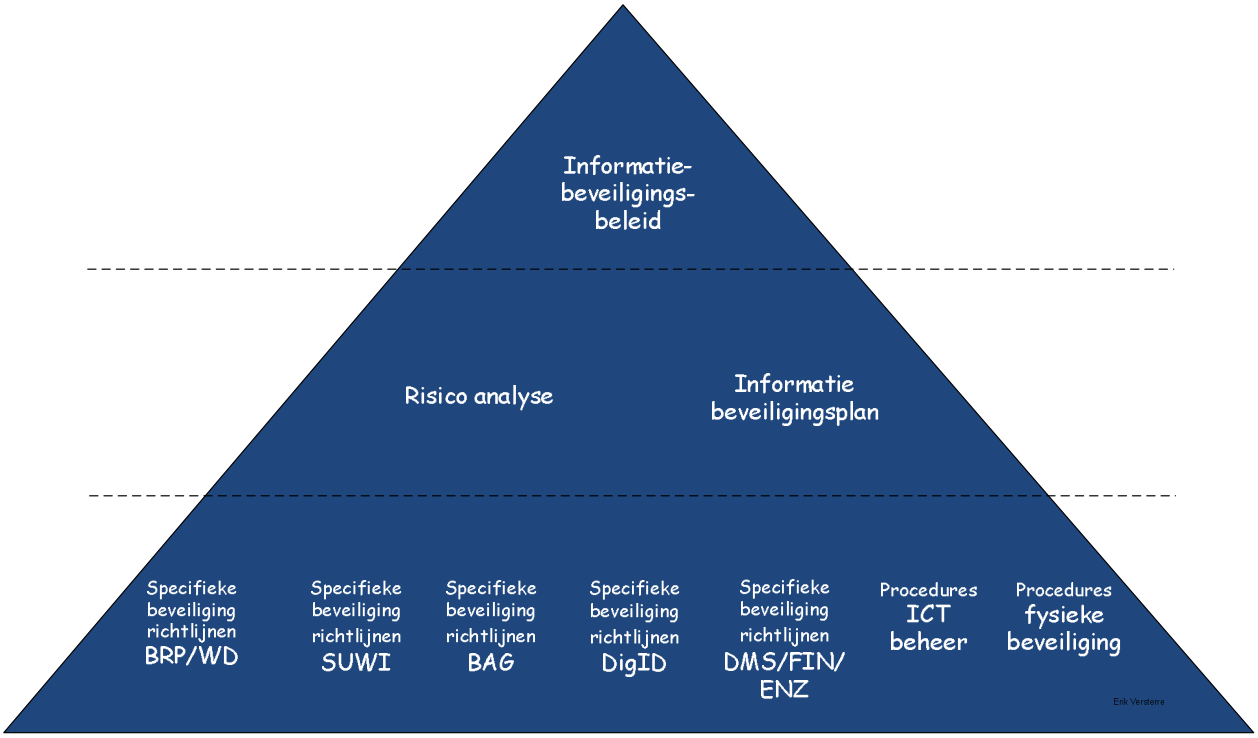
Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (2013) en aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC). Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking worden gesteld, zoals de Wet Gemeentelijke Basisadministratie Persoonsgegevens (Wet BRP), Wet Bescherming Persoonsgegevens (WBP), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit), Wet Openbaarheid Bestuur (Wob) enzovoort.
Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo (aanvullingen op) wettelijke kaders met betrekking tot overige authentieke registraties, zoals de Wet Basisregistratie Adressen en Gebouwen (BAG), Wet Kenbaarheid Publiekrechtelijke Beperkingen (Wkpb), de nieuwe Wet Ruimtelijke Ordening (Wro) en de Archiefwet. Deze stroomlijning van de informatievoorziening vereist in steeds ruimere mate aansluiting op zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van de informatieprocessen bieden een helder motief voor overheden om hun aandacht nog meer te richten op de veiligheid voor overheidsinformatie.

Teneinde de scope van dit document te verduidelijken, is in het onderstaande voorbeeldfiguur aangegeven welke niveaus van informatiebeveiliging vallen te onderkennen.

Bovenaan de piramide treffen we het informatiebeveiligingsbeleid aan. Dit is een organisatie breed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar. Het informatiebeveiligingsbeleid is zodanig opgezet dat praktijksituaties eenvoudig kunnen worden opgezet of hieraan worden getoetst.

De tweede laag van de piramide is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een risico-inventarisatie en evaluatie (RI&E). Tijdens deze RI&E worden de uitgangspunten in het gemeentebrede informatiebeveiligingsbeleid getoetst met de praktijksituatie. Hier worden niet alleen de ‘harde aspecten’ onderzocht. Dat wil zeggen de techniek, de regels en de procedures. Maar worden ook de ‘zachte aspecten’ meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie. De risico-inventarisatie en vervolgens de risicoafweging geeft weer welke onderwerpen onderdelen zijn en op welke onderdelen nog aanvullende maatregelen nodig zijn.
De uitkomst van de analyse wordt vervolgens gebruikt als input voor het Informatiebeveiligingsplan. Dit document kan gezien worden als een Plan van Aanpak voor de verdere implementatie van informatieveiligheid binnen de organisatie.

Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals het BRP, de BAG of het financiële pakket, maar kan ook gericht zijn op de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.



1.3 Toelichting op ISO 27001 en ISO 27002 (code voor informatiebeveiliging)

Het gemeentebreed informatiebeveiligingsbeleid is volledig gebaseerd op de internationale standaard voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002. De eerste standaard (27001) biedt een richtlijn voor de implementatie en borging van Informatiebeveiliging binnen de organisatie. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde ‘best practices’ voor een praktische en concrete aanpak van informatiebeveiliging binnen de organisatie. De Baseline Informatiebeveiliging Nederlandse Gemeenten (2013) is afgeleid van deze beide internationale informatiebeveiligingsnormen, waarbij in de Baseline Informatiebeveiliging Nederlandse Gemeenten de methodiek en de terminologie specifiek is aangepast voor de situatie in gemeenten.

1.4 Algemene oriëntatie en positionering

Informatiebeveiliging maakt onlosmakelijk deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar directe en indirecte omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Raakvlakken:
- Algemeen beveiligingsbeleid (bijv. deuren, kluizen, toegangscontrole);
- Personeelsbeleid (bijv. screening, opleiding en functietypering);
- Organisatiebeleid (bijv. functiescheiding);
- Informatiseringsbeleid (bijv. standaardisatie, Internet en Cloud functionaliteit);
- Privacybeleid (bijv. correct gebruik van persoonsgegevens);
- Juridisch beleid (bijv. afbreukrisico's bij privacyschendingen, clausulering in overeenkomsten met derden, Third Party Mededelingen);
- Dienstverleningsconcept (bijv. website, het Nieuwe Werken, DigiD).

Het doel van informatiebeveiliging is het behoud van:
- Beschikbaarheid / continuïteit (voorkomen van uitval van systemen);
- Integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig);
- Vertrouwelijkheid / exclusiviteit (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn);
- Controleerbaarheid.

1.5 Verantwoordelijkheid en bevoegdheid informatiebeveiligingsbeleid

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van informatiebeveiliging binnen de gemeente[1]. De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris. Zie hoofdstuk 3 voor de organisatie- en proceslijnen met betrekking tot de griffie.

De vaststelling en implementatie van de informatiebeveiligingsstructuur[2] en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Westland. Het college mandateert de uitvoering van het informatiebeveiligingsbeleid aan de gemeentesecretaris en het managementteam. De gemeentesecretaris en het managementteam zijn daarmee volledig bevoegd voor het nemen van operationele maatregelen. De organisatie- en proceslijnen met betrekking tot de griffie zijn in hoofdstuk 3 weergegeven.

Het afdelingsmanagement is verantwoordelijk voor de informatiesystemen waarvan zij eigenaar is. Zij dient deze systemen te classificeren naar risicogevoeligheid en te organiseren zodat er adequate maatregelen kunnen worden getroffen om deze risico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

1.6 Werkingsgebied informatiebeveiligingsbeleid

Dit informatiebeveiligingsbeleid heeft betrekking op alle gemeentelijke informatieprocessen, zowel binnen de ambtelijke organisatie als binnen de bestuurlijke organisatie. De gemeente Westland stelt zich ten doel om de normen zoals beschreven in dit informatiebeveiligingsbeleid voor alle gemeentelijke informatieprocessen te laten gelden. Daarnaast zal de gemeente (indien van toepassing) de kwaliteitsnormen met betrekking tot veiligheid opleggen aan derden, ketenpartners en samenwerkingspartners met wie informatieprocessen worden gedeeld of informatie wordt uitgewisseld.

1.7 Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatiebeveiliging valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):

- Grondwet;
- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Wet Bescherming Persoonsgegevens (WBP);
- Archiefwet / Archiefregeling;
- Databankenwet;
- Wet Elektronisch Bestuurlijk Verkeer;

[1] In hoofdstuk 3 worden de verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging uitgebreider beschreven.

[2] Onder het begrip informatiebeveiligingsstructuur wordt in dit verband de complete beheercyclus van het informatiebeveiligingsproces verstaan (beleidsvorming, implementatie, verantwoording, controle en bijstelling). Informatiebeveiliging wordt gedefinieerd als een verzamelbegrip voor de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

- Wet elektronische handtekeningen;
- Wet algemene bepalingen burgerservicenummer;
- Paspoortwet;
- Archiefwet;
- Wet BasisRegistratie Personen (BRP);
- Wet Openbaarheid Bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Nieuwe Wet Ruimtelijke Ordeningen (nWRO).

Op grond van bovenstaande wet- en regelgeving worden eisen gesteld aan het niveau van informatiebeveiliging, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

1.8 Opbouw hoofdstukken

In de navolgende hoofdstukken worden de informatiebeveiligingsnormen beschreven. Elk hoofdstuk begint met de doelstelling en het beoogde resultaat en beschrijft vervolgens de basisnormen.
De indeling van het informatiebeveiligingsbeleid is gebaseerd op de Baseline informatiebeveiliging Nederlandse Gemeenten. Als referentie zijn de hoofdstuknummers uit de internationale ISO 27002 standaard (Code voor Informatiebeveiliging) achter ieder hoofdstuk vermeld.

Hoofdstuk 1: Inleiding
Hoofdstuk 2: Informatiebeveiligingsbeleid en - plan (CvIB hoofdstuk 1)
Hoofdstuk 3: Organisatie van de informatiebeveiliging (CvIB hoofdstuk 2)
Hoofdstuk 4: Classificatie en beheer van informatie en bedrijfsmiddelen (CvIB hoofdstuk 3)
Hoofdstuk 5: Beveiliging van personeel (CvIB hoofdstuk 4)
Hoofdstuk 6: Fysieke beveiliging (CvIB hoofdstuk 5)
Hoofdstuk 7: Beheer van communicatie- en bedieningsprocessen (CvIB hoofdstuk 6)
Hoofdstuk 8: Logische toegangsbeveiliging (CvIB hoofdstuk 7)
Hoofdstuk 9: Verwerving, ontwikkeling en onderhoud van informatiesystemen (CvIB hoofdstuk 8)
Hoofdstuk 10: Beheer van informatiebeveiligingsincidenten (CvIB hoofdstuk 9)
Hoofdstuk 11: Bedrijfscontinuïteitsbeheer (CvIB hoofdstuk 10)
Hoofdstuk 12: Naleving (CvIB hoofdstuk 11)

2. Informatiebeveiligingsbeleid

Doelstelling:
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid.

Resultaat:
Strategisch beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatiebeveiliging alsmede het vereiste beveiligingsniveau zijn vastgelegd.

2.1 Beleidsdocument voor informatiebeveiliging

Het College van B&W heeft de bevoegdheid om dit gemeentebrede beleidsdocument voor informatiebeveiliging vast te stellen en vervolgens opdracht te geven aan de organisatie om het beleid uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen. Zie hoofdstuk 3 voor de organisatie- en proceslijnen met betrekking tot de griffie.

In dit document zijn de volgende aspecten aanwezig:

- De doelstellingen van informatiebeveiliging voor de gemeente;
- De beveiligingseisen en –prioriteiten;
- De organisatie van de informatiebeveiligingsfunctie (zie hoofdstuk 3);
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging voor het hoogste management, het lijn- of procesmanagement;
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie 1.2) en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (1.6);
- Een verwijzing naar een specifiek informatiebeveiligingsplan (zie 2.2) en procedures, gedragsregels en overige relevante documentatie;
- Het benoemen van de raakvlakken met andere relevante organisatieaspecten, zoals algemeen beveiligingsbeleid (zie hoofdstuk 2), organisatiebeleid (zie hoofdstuk 3), informatisering beleid (zie hoofdstuk 4), bedrijfscontinuïteit (zie hoofdstuk 11), personeelsbeleid (zie hoofdstuk 5), ICT-beheer (zie hoofdstuk 7), privacy beleid (zie hoofdstuk 4), (digitale) dienstverleningsconcept en juridisch beleid (zie hoofdstuk 2);
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst. Het beleidsdocument heeft in principe een looptijd van drie tot vier jaar, maar moet in de jaarlijkse evaluatie meegenomen worden en zo nodig tussentijds worden geactualiseerd (zie 2.4)

2.2 Informatiebeveiligingsplan

Op basis van dit strategische beleidsdocument wordt door het MT het informatiebeveiligingsplan vastgesteld waarin wordt aangegeven op welke wijze het beleid uitgevoerd zal worden.
De kernelementen in het informatiebeveiligingsplan zijn:

- Beschrijving van het huidige niveau van informatiebeveiliging en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van het gemeentebrede informatiebeveiligingsplan wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau;
- Voor het bepalen van afhankelijkheden en risico's wordt een risico analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:
  - Risico's die onvoldoende af te dekken zijn door maatregelen;
  - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen;
  - Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden. Dit overzicht moet jaarlijks geactualiseerd worden;
  - De beschrijving van een periodiek controle- en evaluatieproces waarmee de opzet en het bestaan van de maatregelen kan worden getoetst en de werking ervan kan worden geborgd (zie hoofdstuk 11);
  - Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfskritische zijn. Dit overzicht kan als bijlage aan het plan van aanpak worden toegevoegd. Het informatiebeveiligingsplan kan maximaal dezelfde looptijd hebben als het informatiebeveiligingsbeleid, maar wordt jaarlijks geëvalueerd en zo nodig tussentijds geactualiseerd.

2.3 Aanvullende maatregelen

Afwijkend beveiligingsniveau
Als uit de risicoanalyse blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist, moet een verantwoordelijke aanvullende maatregelen treffen. Bij minder risicovolle verwerkingen kan een lager beveiligingsniveau worden overwogen (zie hoofdstuk 4).

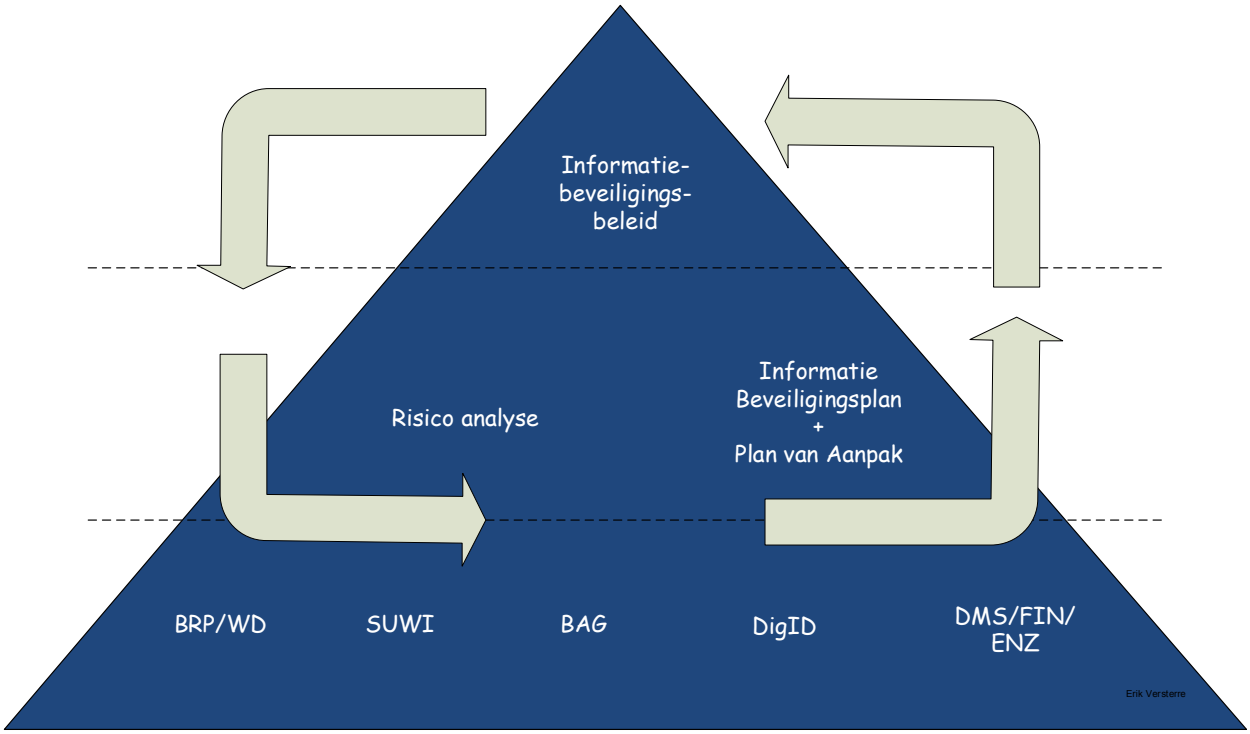
Persoonsgegevens
Bij de verwerking van persoonsgegevens zijn aanvullende maatregelen vereist, afhankelijk van de klassenindeling van de Wet Bescherming Persoonsgegevens (WBP).

2.4 Borging van het informatiebeveiligingsbeleid

Om borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 3), onderstaande PDCA cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA cyclus:

1. Informatiebeveiligingsbeleid. Bevat het informatiebeveiliging beleid en de visie op informatiebeveiliging. Bijstelling van het informatiebeveiligingsbeleid vindt plaats om de 3 tot 4 jaar;

2. Informatiebeveiligingsplan. Bevat de risicoanalyse (de toets aan de praktijk) op basis van informatiebeveiligingsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van het Informatiebeveiligingsplan vindt plaats na 2 tot 3 jaar;
3. Plan van Aanpak. Bevat de concrete acties volgend uit de risicoanalyse. Bijstelling (hieronder valt ook de voortgang op de realisatie van de afgesproken acties en maatregelen) van het Informatiebeveiligingsplan vindt zonodig (conform de bespreking in het informatiebeveiligingsoverleg zie Hoofdstuk 3) 4 tot 6 maal per jaar plaats.



3. Organisatie van de informatiebeveiliging

Doelstelling:
Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.

Resultaat:
Verankering in de gemeentelijke organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid.

3.1 Verantwoordelijkheidsniveaus binnen de gemeente Westland

Binnen de gemeente Westland worden de volgende verantwoordelijkheid- en takenniveaus met betrekking tot informatiebeveiliging onderscheiden:

3.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

Het College van B&W van de gemeente Westland draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatiebeveiligingsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan de gemeentesecretaris en het managementteam. Bij de griffie zijn deze verantwoordelijkheden belegd bij de gemeenteraad, respectievelijk het presidium en gemandateerd aan de griffier.

3.1.2 Gemandateerde verantwoordelijkheden en taken op organisatieniveau

De gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. Bij de griffie zijn deze verantwoordelijkheden belegd bij de griffier. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd op afdelingsniveau.

3.1.3 Verantwoordelijkheden en taken op afdelingsniveau en teamniveau

De afdelingshoofden respectievelijk de teamleiders zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling c.q team.

3.1.4 De medewerkers

Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien de betrouwbaarheid, de integriteit en de beschikbaarheid van de informatieprocessen waarbij zij zijn betrokken.

3.1.5 De security manager

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. De Security manager ziet organisatiebreed toe op de naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen, zorgt voor onderzoek en adviseert in complexe beveiligingsvraagstukken, initieert security audits (indien van toepassing ook risico analyses), organiseert organisatiebrede security awareness programma's en opleidingen en vervult een adviserende rol naar managementteam en gemeentebestuur. Tevens zorgt de security manager voor heldere communicatie bij incidenten op het vlak van informatiebeveiliging. De rol heeft een strategisch karakter.

3.1.6 De controller informatiebeveiliging

Deze rol is op organisatieniveau verantwoordelijk voor de interne controle op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.

3.1.7 De security officer

Deze rol is op afdelingsniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. De security officer is daarnaast verantwoordelijkheid voor het samenstellen van het deel van het informatiebeveiligingsplan met betrekking tot de betreffende afdeling en het uitvoeren of doen uitvoeren van de daaruit voortvloeiende activiteiten die zijn toegewezen aan de Security Officer.

3.1.8 Het team BAS/DIA

Het team BAS/DIA, waarvan systeembeheer deel uit maakt, beheert de werkplekken, serverplatformen, lokale netwerken, straalverbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Het team is verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

3.1.9 Het team Facilitaire zaken

Het team Facilitaire zaken is verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).

3.1.10 Het team POOC

Het team POOC is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke advies rol op het gebied van organisatie en informatieprocessen.

3.1.11 De beveiligingsbeheerder

Deze rol geldt ten aanzien van de specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumen-

ten (officieel beveiligingsfunctionaris reisdocumenten), Rijbewijzen (officieel beveiligingsfunctionaris Rijbewijzen), BAG, SUWI (officieel Security officer SUWI) en DigiD.

3.1.12 Privacy beheerder

Deze rol is gericht op de uitvoering en de naleving van de Wet Bescherming van Persoonsgegevens (WBP). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

3.1.13 Applicatiebeheerder

Verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.

3.1.14 Gegevensbeheerder

Verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening

3.1.15 Informatiebeheerder

Binnen het specifieke gebied BRP en Waardedocumenten verantwoordelijk voor het geheel van activiteiten gericht op beleidsvoorbereiding ter zake deze specifieke gegevensverzameling. Daarnaast de ontwikkeling van kwaliteitsprocedures, beveiligingsprocedures, verstrekking- en privacyprocedures, evenals de coördinatie bij de uitvoering van deze procedures.

3.1.16 Autorisatiebevoegde Reisdocumenten/Aanvraagstations

Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).

3.1.17 Autorisatiebevoegde Rijbewijzen

Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

3.2 Toewijzing verantwoordelijkheden voor informatiebeveiliging

Het *managementteam* heeft in ieder geval de volgende verantwoordelijkheden:

- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op concern risico's;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging;
- Het aanwijzen van een security manager en een controller informatiebeveiliging.

Het *afdelingsmanagement respectievelijk teammanagement* heeft in ieder geval de volgende verantwoordelijkheden*:*

- Het uit (laten) voeren van maatregelen uit het informatiebeveiligingsplan die op de afdeling van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;

- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de security manager, over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages.

De s*ecurity manager* 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;
- Rapporteert binnen de P&C cyclus over het aspect informatiebeveiliging;
- Ondersteunt de directie en de afdelingshoofden 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;
- Bevordert 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 (zie 10.1);

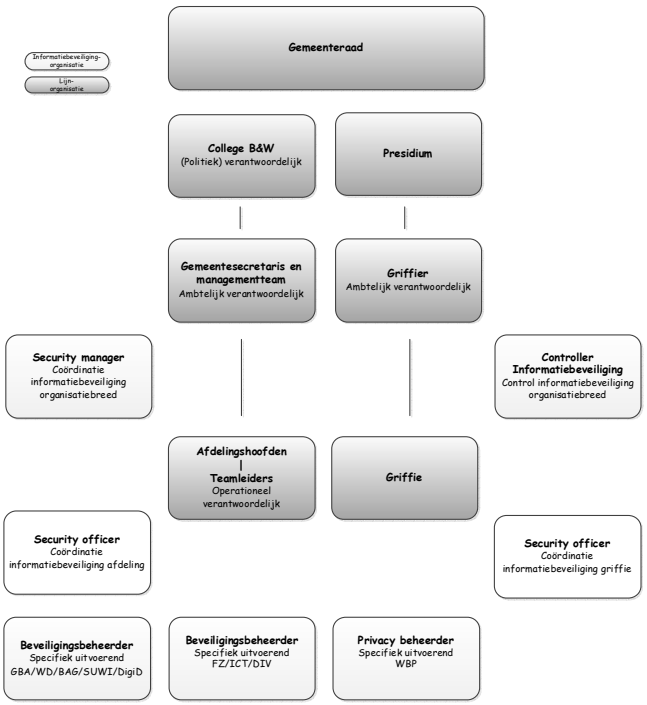
De rol van *controller informatiebeveiliging* heeft in ieder geval de volgende verantwoordelijkheden:
- De periodieke controle op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- De controle op de voortgang van het uitvoeren van de maatregelen uit het informatiebeveiligingsplan
- De controle op de periodieke actualisatie van informatiebeveiligingsbeleid en op het Informatiebeveiligingsplan;
- Toetsen/bewaken van het niveau van informatiebeveiliging;
- Evalueren van beveiligingsincidenten.

De s*ecurity officer* heeft in ieder geval de volgende verantwoordelijkheden:
- Participeert in het formuleren van het informatiebeveiligingsbeleid ;
- Stelt in het informatiebeveiligingsplan het deel met betrekking tot de afdeling op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering informatiebeveiligingsmaatregelen voor de afdeling uit het informatiebeveiligingsplan;
- Ondersteunt de het afdelingshoofd met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van de afdeling over het onderwerp informatiebeveiliging;
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de Informatiebeveiligingsplannen;
- Bevordert van het beveiligingsbewustzijn in de afdeling;

- Toetst of informatiebeveiliging een onderdeel uitmaakt van het informatieplannings-, systeemontwikkelings- en onderhoudsproces van de afdeling (zie 10.1);
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages. Hierbij bundelt de security manager de deelbijdragen van het afdelingsmanagement

De *beveiligingsbeheerder* is -voor het toegewezen deelgebied- verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatiebeveiligingsbeleid en de onderliggende informatiebeveiligingsplannen. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker voert interne controles uit en let op de naleving van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de security manager en de controller informatiebeveiliging. De beveiligingsbeheerder is tevens certificaatbeheerder. Dat wil zeggen dat hij de elektronische sleutels van PKI/Overheid conform de voorschriften beheert.

De *privacybeheerder* heeft in ieder geval de volgende verantwoordelijkheden:
- Toezicht op de naleving van de Wet Bescherming van Persoonsgegevens (WBP) en de Wet Basisregistratie Personen (BRP).
- Organisatiebreed adviseren over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.
- Aanwijzingen geven aan gebruikers van systemen met betrekking tot persoonsregistraties
- Ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de registratie van personen
- Contactpersoon van de gemeente voor het College Bescherming Persoonsgegevens (CBP)



3.3 Overleg en afstemmingsorganen

De security manager is voorzitter van het overleg informatiebeveiliging dat 4 tot 6 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De security manager
- De controller informatiebeveiliging
- De security officers
- Agendaleden: beveiligingsbeheerders t.a.v: BRP en WD, BAG, SUWI, DigiD
- Agendaleden: beveiligingsbeheerders t.a.v: FZ, ICT en DIV
- Agendalid: Privacy beheerder
- Agendaleden: managementteam lid of specialist

Onderwerpen:

- Voortgang uitvoering maatregelen Beveiligingsplan c.q. Plan van Aanpak;
- Behandeling veiligheidsincidenten;
- Planning en voorbereiding van audits, inspecties en evaluaties;
- Evaluatie en actualisatie informatiebeveiliging en informatiebeveiligingsplan.

Daarnaast vindt afstemming plaats tussen de security manager en de functioneel applicatie- en gegevens-beheerder(s) en de eigenaar van (informatie)systemen.

3.4 ICT crisisbeheersing

Voor interne crisisbeheersing dient een kernteam informatiebeveiliging geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat uit:

- De security manager
- De teamleider I&A
- De beveiligingsbeheerder ICT
- Betrokken MT lid
- Relevante experts
- Een lid van het team Communicatie

3.5 Rapporteren beveiligingsincidenten

De security manager wordt door de Servicedesk geïnformeerd omtrent beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatie-technologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatiebeveiligingsbeleid niet wordt nageleefd. Zie Hoofdstuk 10 voor meer informatie over de definitie en de procedure met betrekking tot beveiligingsincidenten.
Afspraken moeten worden gemaakt over:

- doel van de registratie;
- inhoud van de registratie;
- wijze van handelen;
- wijze van rapporteren.

Er wordt minimaal eenmaal per jaar gerapporteerd aan het MT de security manager.

3.6 Verantwoordelijkheden afdeling overstijgende (informatie)systemen

Afdeling overstijgende (informatie)systemen binnen de gemeente Westland worden onder de verantwoordelijkheid van het team I&A gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd eigenaar van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

De procesverantwoordelijke maakt schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:
- Voorwaarden voor het toegestane gebruik van het afdeling overstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatiebeveiliging;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van de afspraken en oplossing van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audit bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatiebeveiligingsbeleid voldoet.

3.7 Contracten met derden

3.7.1 Service level agreement (niveau van dienstverlening)
Bij structurele / langdurige uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen een afdeling en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatiebeveiliging en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatiebeveiliging. In het uitbestedingscontract wordt verwezen naar de SLA.

3.7.2 Inhuur derden
Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijk manager. Deze manager dient te waarborgen dat activiteiten binnen het kader van het informatiebeveiligingsbeleid worden uitgevoerd.

3.7.3 Toegang
Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden de onderstaande uitgangspunten:
- Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.

- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthenticeerde en geautoriseerde toegang vastgesteld wordt.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform WBP artikel 14) afgesloten.
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd

3.7.4 Grote projecten

Voor grote ICT-projecten gelden specifieke, op MT niveau vastgestelde, richtlijnen, met name ten aanzien van Europese aanbesteding, screening van bedrijven en juridische aspecten.

4. Classificatie en beheer van informatie en bedrijfsmiddelen

Doelstelling:
Het bepalen, handhaven en waarborgen van het juiste beveiligingsniveau voor informatie, (informatie) systemen en bedrijfsmiddelen.

Resultaat:
Een goed overzicht van alle ICT-componenten en andere relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald.

4.1 Inventarisatie van informatie en (informatie) bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden vastgelegd. Het team I&A houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (configuratiemanagement):

- Informatie (bijvoorbeeld databases, gegevensbestanden, documentatie en procedurebeschrijvingen);
- Programmatuur (bijvoorbeeld systeemprogrammatuur en standaardsoftware inclusief versiebeheer);
- Fysieke bedrijfsmiddelen (bijvoorbeeld apparatuur, schijven, accommodatie en netwerkinfrastructuur en actieve componenten);
- Diensten (bijvoorbeeld communicatiediensten, PKI diensten, energievoorziening ten behoeve van de informatievoorziening).

In de registratie is opgenomen waar de gegevens(bestanden) zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de eigenaren en beheerders zijn.

4.2 Eigendom van informatie en bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.

4.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen. Hieronder volgen de geldende uitgangspunten:

- 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 primair 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;
  - 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.

4.4 Classificatie van informatie en bedrijfsmiddelen

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid(BIV). Deze classificatie zal gebeuren op basis van de handreiking Dataclassificatie van de IBD.

5. Beveiligingsaspecten ten aanzien van personeel

Doelstelling:
Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

Resultaat:
Werknemers, ingehuurd personeel en externe gebruikers kennen en begrijpen hun verantwoordelijkheden en zijn geschikt voor de rollen waarvoor zij (beoogd) worden benoemd.

5.1 Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten

Hieronder volgen de geldende algemene uitgangspunten:

- 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. Team-BAS/POOC houdt toezicht op dit proces;
- 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;
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en gemeentelijke regelingen;
- Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

5.2 Voorwaarden tewerkstelling vast personeel

Iedere werknemer in dienst van de gemeente Westland legt de eed/belofte af en wordt geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol en het Westlandse gedragsprotocol. Daarnaast overlegt iedere nieuwe werknemer een Verklaring Omtrent Gedrag (VOG). Bij indiensttreding wijst de afdelingsmanager de werknemer bovendien op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling. Dit gebeurt in ieder geval bij de Basisregistratie Personen (BRP) en bij het team Belastingen.

5.3 Voorwaarden tewerkstelling tijdelijk personeel

Tijdelijke medewerkers die toegang hebben tot gemeentelijke informatie, zoals uitzendkrachten, stagiaires en ingehuurde externe personen tekenen een geheimhoudingsverklaring. Ook deze tijdelijke medewerkers overleggen een Verklaring Omtrent Gedrag (VOG) en worden geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol en het Westlandse gedragsprotocol. Daarnaast wijst de afdelingsmanager de tijdelijke werknemer bovendien op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling. Dit gebeurt in ieder geval bij de Basisregistratie Personen (BRP) en bij het team Belastingen.

5.4 Kwetsbare functies

De gemeente kiest voor een zorgvuldige selectieprocedure ter waarborging van een betrouwbaar personeelsbestand. Er wordt geen onderscheid gemaakt tussen functies. Van elke medewerker wordt verwacht dat hij/zij integer handelt.

5.5 Toegang en bevoegdheden personeel

Bij indiensttreding worden de fysieke en logische toegangsbevoegdheden volgens een vastgestelde procedure toegekend. De beslissing hierover moet door geautoriseerde personen worden genomen. Bij dienstbeëindiging of bij wijziging van functie worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement met onmiddellijke ingang en volgens een vastgestelde procedure verwijderd of aangepast aan de nieuwe status (zie hoofdstukken 6 en 8).

5.6 Opleiding en communicatie

Alle medewerkers (en voor zover van toepassing externe gebruikers van onze de gemeentelijke systemen) worden geacht regelmatig geïnformeerd te worden over procedures die binnen de gemeente of afdeling gelden voor informatiebeveiliging om zodoende het beveiligingsbewustzijn op peil te houden. Ten aanzien van communicatie en bewustwording geldt dat:

- Alle medewerkers binnen de organisatie worden ingelicht over het beveiligingsbeleid en de (beveiligings)procedures van de gemeente en informatie krijgen over het correcte gebruik van de ICT- en toegangsvoorzieningen. Dit geldt eventueel ook voor externe gebruikers;
- Het MT en de afdelingshoofden de algehele communicatie en bewustwording rondom informatieveiligheid bevorderen;
- Het lijnmanagement bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen;
- In werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in een HRM-gesprek.

5.7 Bijzondere situaties

In het geval van ernstige verdenkingen tegen een medewerker op het gebied van verduistering of gedrag wat in strijd is met de interne regels, is het mogelijk dat de gemeente Westland gebruik maakt van opsporingsmogelijkheden zoals verborgen camera's, microfoons en loggegevens. Ook de door de gemeente verstrekte telefoon en automatiseringsmiddelen kunnen in deze gevallen worden onderzocht. Voor de inzet van deze middelen is toestemming nodig van de gemeentesecretaris.

6. Fysieke beveiliging

Doelstelling:
De fysieke bescherming van gebouwen, terreinen, informatie en (informatie)systemen tegen onbevoegde fysieke toegang, schade of verstoring van continuïteit.

Resultaat:
Maatregelen en procedures waarmee gebouwen, informatie- en ICT-voorzieningen adequaat worden beschermd tegen ongeautoriseerde toegang, kennisneming, verminking of diefstal, waardoor schade en verstoringen worden voorkomen.

6.1 Algemene uitgangspunten ten aanzien van fysieke beveiliging:

- 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;
- 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;
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel;
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.

6.2 Inventarisatie van bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden onderkend. Het team facilitaire zaken houdt een registratie bij van alle bedrijfsmiddelen die verband houden met veiligheid van ruimten, gebouw(en) en de directe omgeving van de gebouwen, te weten de gemeentekantoren. PO vastgoed is verantwoordelijk voor overige gemeentelijke panden. Hieronder vallen:

- De preventieve, detectieve, correctieve en repressieve systemen met betrekking tot inbraak, ontruiming, brand en toegang;
- Overzicht van toegangsrechten van personen tot ruimten, gebouwen en directe omgeving van het gebouw, zoals parkeerplaatsen.

6.3 Servicetaken

Indien voor de bewaking van de gebouwen, personen en goederen een externe bewakingsdienst wordt ingehuurd, voldoet deze bewakingsdienst aan de eisen volgens de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus, beschikt deze over een vergunning van het Ministerie van Justitie en is deze

aangesloten bij een brancheorganisatie. Er zijn afspraken gemaakt bij wie de bewakingsdienst verantwoording moet afleggen.

6.4 Fysieke toegang computer- en datacomruimten

De fysieke toegang tot specifieke computer-/serverruimten onder beheer van het team I&A is voorbehouden aan de volgende categorieën personen:

- De leden van het team I&A die uit hoofde van functie (technische) werkzaamheden aan de centrale computers of telecom apparatuur moeten verrichten;
- De door de manager van de afdeling (waaronder ICT valt) geautoriseerde personen (zoals bijvoorbeeld de Bedrijfshulpverlening);
- Personen die niet onder de genoemde categorieën vallen, mogen de specifieke ruimten alleen betreden onder begeleiding van een geautoriseerde medewerker van het team ICT.

6.5 Bewegwijzering computerruimten

Binnen de vestiging zijn geen wegwijzers aangebracht waaruit de locaties van de ICT-ruimten kunnen worden afgeleid. Ook zijn deze ruimten niet aangegeven op publieke plattegronden of in publicaties, tenzij hieraan andere eisen worden gesteld, bijvoorbeeld door de brandweer.

6.6 Verwijderen apparatuur en gegevensdragers

Het team I&A heeft een procedure voor het verwijderen of gereed maken voor hergebruik van overbodige apparatuur en gegevensdragers waarop gemeentelijke informatie en in licentie gebruikte software is opgeslagen.
Denk hierbij aan de harde schijven van pc's en netwerkservers, cd's/dvd's, back-up tapes, USB sticks en overige gegevensdragers. In deze procedure staan voorschriften voor het verwijderen en zo nodig onbruikbaar maken of vernietigen van die informatie.

6.7 Datakluizen en reserve apparatuur

- De datakluizen voldoen aan de eisen die gesteld worden om opgeslagen gegevensdragers in voldoende mate te beschermen tegen stof, brand, water, beschadiging en diefstal;
- Reserve apparatuur en back-ups worden gescheiden bewaard op een andere locatie of een datacenter om de gevolgen van een calamiteit te minimaliseren.

6.8 Clean desk en clear screen beleid

De gemeente Westland stelt een "clean desk"-beleid vast voor papieren en verwijderbare opslagmedia, zodat dit soort materialen niet onbeheerd op het bureau liggen. Daarnaast een "clear screen" beleid voor ICT-voorzieningen. Dit betekent dat na een bepaald tijdsverloop het beeldscherm "op zwart" gaat en de toegang tot het werkstation wordt geblokkeerd middels een toegangscode). Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken.

6.9 Beveiliging van (mobiele) apparatuur

Informatieverwerkende mobiele apparatuur moet zowel binnen als buiten het gebouw zo mogelijk fysiek beschermd worden. Dit betreft laptops, PDA's, tablets (bijvoorbeeld iPad's), memorysticks en mobiele telefoons (smartphones). Voor het gebruik van deze apparatuur worden richtlijnen vastgesteld:

- Apparatuur en bijbehorende media mogen buiten de locatie niet onbeheerd worden achtergelaten;
- Bij het verwerken van vertrouwelijke, privacygevoelige en/of kritische gegevens zijn aanvullende maatregelen getroffen passend bij het classificatieniveau, zoals encryptie, wachtwoordbeveiliging, antivirusscanners enzovoort;
- Bij gebruik van draadloze apparatuur, via een aansluiting op een lokaal of publiek netwerk, zijn beveiligingsmaatregelen getroffen om ongeautoriseerde toegang te voorkomen.

7. Beheer van communicatie- en bedieningsprocessen

Doelstelling:
Het garanderen van correcte en veilige bediening en beheer van de ICT-voorzieningen.

Resultaat:
Maatregelen en procedures voor het beheer en de bediening van de ICT-voorzieningen en het adequaat reageren op incidenten.

7.1 Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- 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.

7.2 Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- 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 toegepast;
- Het is niet toegestaan niet-geautoriseerde (pc)programmatuur te gebruiken of te installeren op gemeentelijke ICT voorzieningen;
- Alle apparatuur die is verbonden met het netwerk van de gemeente moet kunnen worden geïdentificeerd;
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging;
- Het (ongecontroleerd) kopiëren van vertrouwelijke gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer;
- Updates die ten behoeve van het verhogen van de veiligheid worden vrijgegeven door de leverancier worden zo spoedig mogelijk via de geëigende wijzigingsprocedure doorgevoerd. Dit geldt zowel voor besturingssoftware, informatiesystemen, als voor ondersteunende software (Java, Java applets, ActiveX, Flash en Adobe) en besturingssystemen voor mobiele apparatuur en actieve componenten;
- 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;
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.

7.3 Beheerprocedures en verantwoordelijkheden

De verantwoordelijkheden en procedures voor het beheer van de bediening van de ICT-voorzieningen zijn beschreven en vastgesteld. Procedures zijn voor zover mogelijk in lijn gebracht met de ISO 20000-1 en ISO 20000-2 (ITIL 3). Ook ASL (Application Services Library*)* en BISL (Business Information Services Library) worden als beheermethodieken ingezet.

Documentatie van beheerprocedures
De beheerprocedures zijn gedocumenteerd en worden bijgehouden. Deze procedures bevatten instructies voor de planmatige uitvoering van de activiteiten met betrekking tot ICT-voorzieningen. Het gaat om de volgende processen:

Change management / release management – doorvoeren van vernieuwingen en wijzigingen
Het aanbrengen van wijzigingen in de informatie-infrastructuur of het installeren van nieuwe versies vindt plaats volgens een vastgestelde wijzigingsprocedure waarin de formele goedkeuring geregeld is. Dit geldt voor apparatuur, programmatuur, productiesystemen en procedures. Voornaamste aspect bij dit proces is het garanderen van de continuïteit van het productiesysteem. Uitgangspunten hierbij zijn:

- 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 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.

Incident management – afhandeling van incidenten in de ICT infrastructuur
Om te waarborgen dat incidenten snel, effectief en ordelijk worden afgehandeld, zijn verantwoordelijkheden en procedures voor beheer vastgesteld. Hierbij worden verschillende typen incidenten onderscheiden en wordt gezorgd voor registratie en gedocumenteerde afhandeling van de incidenten.

Capaciteitsmanagement – omgang met de capaciteit van ICT voorzieningen
Om te waarborgen dat informatiesystemen conform de gestelde eisen van continuïteit en snelheid blijven werken stelt het team I&A verantwoordelijkheden en procedures op ten aanzien van de monitoring van de capaciteit.

Problemmanagement – identificeren en afhandelen van fouten in de ICT infrastructuur
BAS/DIA richt een organisatie in en stelt procedures op ten aanzien van het achterhalen en wegnemen van fouten in de infrastructuur.

IT service continuity management – waarborgen van de continuïteit van de ICT-dienstverlening in geval van calamiteiten
BAS/DIA stelt procedures op ten aanzien van voldoende technische, financiële en organisatorische voorzieningen ten behoeve van het waarborgen van de overeengekomen continuïteit van de ICT-dienstverlening in geval van calamiteiten. Uitgangspunten hierbij zijn:

- 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;
- De back-up wordt iedere dag buiten het gebouw opgeslagen;
- De back-up- en recovery-maatregelen worden regelmatig, doch minimaal één maal per jaar op een uitwijkcentrum en één keer per jaar in de eigen ICT-omgeving, getest;
- Over het resultaat van de test wordt aan de procesverantwoordelijken, de coördinator informatiebeveiliging en de controller informatiebeveiliging gerapporteerd.

Configuratie management – registratie van ICT voorzieningen
BAS/DIA stelt procedures op ten aanzien van het registreren en muteren van ICT voorzieningen en de daaraan gerelateerde documentatie.

Information security management – omgang met de veiligheid van ICT voorzieningen
De security manager richt een organisatie in, stelt procedures op en traint personeel zodanig dat aan de eisen van het Informatiebeveiligingsbeleid wordt voldaan.

7.4 Uitgangspunten voor controle en logging

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. 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 log-regel bevat minimaal: een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
de gebeurtenis, waar mogelijk de identiteit van het werkstation of de locatie, het object waarop de handeling werd uitgevoerd, het resultaat van de handeling, de datum en het tijdstip van de gebeurtenis.

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.

7.5 Beheer van de dienstverlening door een derde partij

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.
Uitgangspunten bij externe hosting van data en/of services zijn:

- Goedgekeurd door verantwoordelijke lijnmanager;
- Voldoet aan de criteria voor leveranciers van webapplicaties en webservices opgenomen in de norm ICT-beveiligingsassessments DigiD;
- In overeenstemming met informatiebeveiligingsbeleid en algemeen gemeentelijk beleid;
- Vooraf gemeld bij BAS/DIA ten behoeve van toetsing op beheeraspecten;
- 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 er bestaat de mogelijkheid voor het uitvoeren van (periodieke) audits;
- 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 de kaders staan voor de toegang tot ICT-voorzieningen door derden.

7.6 Telewerken en thuiswerken

De gemeente Westland staat telewerken toe (op afstand werken op het netwerk van de gemeente, bijvoorbeeld thuiswerken). Hiervoor worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatiebeveiligingsbeleid en voor zover niet wordt verboden door wet en regelgeving.[3]

Minimaal wordt aan onderstaande punten aandacht besteed:

- Afspraken tussen de procesverantwoordelijke en “de telewerker”, bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke, en/of kritische informatie en/of documenten;
- Richtlijnen voor identificatie en authenticatie;
- Richtlijnen voor wachtwoordgebruik;
- Richtlijnen voor de technische inrichting van de telewerkplek (firewall, virusscanner);
- Afspraken omtrent de telewerkplek (ARBO normen);
- Het inloggen met bijzondere systeembeheer bevoegdheden (administrator en root) via de telewerkplek is niet toegestaan tenzij er aanvullende maatregelen zijn getroffen.

7.7 Mobiele (privé-)apparatuur

Ten aanzien van 'Bring Your Own Device/ Choose Your Own Device'' (BYOD/CYOD) wordt beleid opgesteld en worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatiebeveiligingsbeleid en voor zover niet wordt verboden door wet en regelgeving.[4]
Minimaal wordt aan onderstaande punten aandacht besteed:

[3] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.
[4] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.

- Afspraken tussen de leidinggevende en “de gebruiker van mobiele en/of privé apparatuur”, bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke, en/of kritische informatie en/of documenten;
- Alle getroffen beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als op privé-apparatuur;
- 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, antivirusprogrammatuur en de instellingen van deze programmatuur, 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.

7.8 Gebruik internet en email

E-mail- en internetprotocol
De gemeente Westland heeft een protocol (gedragscode) ten aanzien van het gebruik van e-mail en het gebruik van internet. In deze protocollen zijn maatregelen opgenomen om beveiligingsrisico’s, verbonden aan het gebruik van e-mail en internet, te beperken.

7.9 Sociale media

Het gebruik van sociale media door medewerkers van de gemeente Westland is toegestaan. De medewerkers dienen zich ervan bewust te zijn dat ze online gezien worden als vertegenwoordigers van de organisatie. Uitingen op het internet worden permanent opgeslagen en kunnen eventueel via andere media opnieuw worden gepubliceerd. Voor het gebruik van sociale media wordt een protocol opgesteld. Hierin worden in ieder geval de volgende onderdelen belicht:

- Geef nooit persoonlijke gegevens van jezelf of collega’s zoals adressen en telefoonnummers. Dit om identiteitsfraude te voorkomen;
- Ook op internet is het wettelijk kader van toepassing en besef dat smaad, laster, auteursrecht en wetgeving op het gebied van gegevensbescherming van toepassing is;
- Bij de uitingen op het internet dient rekening gehouden te worden met het effect op het imago van de gemeente Westland;
- Uitingen op het internet mogen geen uitingen inzake klanten of zaken bevatten.

7.10 Uitwisseling van informatie over netwerken

Bij het beheren van netwerken moet onderscheid gemaakt worden tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn extra maatregelen nodig.
Bij gebruik van andere netwerken moet geanalyseerd worden of eigen eisen en de eisen van het andere netwerk in overeenstemming met elkaar zijn en niet leiden tot onoverkomelijke problemen.

Verantwoordelijkheden en procedures voor toegang en het beheer van netwerken
en apparatuur op afstand (inclusief de apparatuur op de werkplek) zijn vastgelegd en worden gecommuniceerd naar betrokken partijen.

8. Logische toegangsbeveiliging

Doelstelling:
Het beheersen van de toegang tot informatie en (informatie)systemen.

Resultaat:
Gedocumenteerd beleid en daarvan afgeleide maatregelen en procedures voor effectieve toegangsbeveiliging tot de informatie-infrastructuur en gegevens en het voorkomen van ongeautoriseerde toegang.

8.1 beleid voor logische toegangsbeveiliging

Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen implementeren en onderhouden is er een gemeentebreed toegangsbeleid. Naast dit gemeentebrede toegangsbeleid heeft ieder informatiesysteem nog een specifiek gedefinieerd toegangsbeleid, wat is afgestemd op de classificatie van de informatie.
Het toegangsbeleid is vastgesteld. In het beleid komen de volgende aspecten aan de orde:

- Aanvragen voor toegang worden geautoriseerd door de procesverantwoordelijke (eigenaar van de data/applicatie);
- 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);
- Alle toegekende bevoegdheden worden geregistreerd en beheerd, bijvoorbeeld in een autorisatiematrix;
- Het gebruik van speciale bevoegdheden wordt beperkt.

De procesverantwoordelijke toetst of de door het team I&A of applicatiebeheer geïmplementeerde bevoegdheden zijn toegekend of verwijderd conform de aanvraag.

8.2 Beheer van toegangsrechten

Voor de beheersing van toewijzing van toegangsrechten is een procedure vastgesteld, waarin de gehele cyclus is opgenomen van het registreren tot het afmelden van gebruikers. Naast wachtwoorden kunnen ook andere technologieën worden toegepast voor gebruikersidentificatie en authenticatie, zoals biometrie, handtekeningverificatie, hardware (bijvoorbeeld token), SMS authenticatie en cryptografische sleutels. Bij het beheer van gebruikerswachtwoorden is vastgelegd op welke wijze het initiële wachtwoord aan de gebruiker kenbaar wordt gemaakt en hoe gehandeld wordt bij het vergeten van het wachtwoord. Verstrekte wachtwoorden moeten onmiddellijk na het eerste gebruik door de gebruiker worden gewijzigd.

8.3 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.

8.4 Mobiel werken, thuiswerken en internetfaciliteiten

Uitgangspunten voor beleid ten aanzien van Mobiel werken, thuiswerken en internetfaciliteiten:

- Voor werken op afstand is een thuiswerk- c.q mobiele werkplekomgeving 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;
- Voorzieningen als webmail, als ook sociale netwerk en clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam, wachtwoord en het ontbreken van versleuteling) en internationale regelgeving (veelal beschikbaar voor buitenlandse onderzoekdiensten), niet geschikt voor het delen van vertrouwelijke informatie.

8.5 Controle op toegangsrechten

Alle medewerkers die van het netwerk of applicaties gebruikmaken, moeten door het systeem of applicatie op unieke wijze geïdentificeerd kunnen worden. Om de toegang tot de Informatiearchitectuur effectief te beheren, wordt per applicatie of groep van applicaties een autorisatieplan opgesteld. Dit plan bevat onder andere informatie inzake wie er toegang heeft tot de applicatie, waarom en welke toegangsrechten. Daarnaast ook ene controlesysteem om de toegekende rechten periodiek te controleren en zonodig aan te passen.

8.6 Toegangsbeveiliging met betrekking tot netwerkdomeinen en componenten

Aanbrengen van scheidingen
Daar waar de risico's dit noodzakelijk maken, is scheiding in de netwerken aangebracht. De toegang tussen deze gescheiden 'netwerkdomeinen' zijn beveiligd via bijvoorbeeld gateways, firewalls en routers. Afhankelijk van de toegangseisen voor de betreffende ICT-voorziening is het gebruik van de verbindingsmogelijkheden beperkt.

Demilitarized Zone (DMZ)
Voor wat betreft de internetfacing systemen moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke. O.a. de webapplicaties die gebruik maken van DigiD bevinden zich in deze DMZ. Door middel van minimaal van 2 (virtuele) firewalls worden verkeersstromen tussen het internet, de (web)applicaties in het DMZ en het interne netwerk waar de backoffice applicaties en de gemeentelijke basisregistraties zich bevinden, tot een minimum beperkt.

Intrusion Detection Systeem
De gemeente maakt gebruik van een intrusion detection systeem zodat tijdig wordt gedetecteerd dat kwaadwillenden misbruik willen maken van de webapplicatie. Intrusion Detection Systemen (IDS) helpen bij het detecteren van aanvallen op webapplicaties. Een IDS monitort continu het netwerk verkeer dat zich door de DMZ compartimenten verplaatst en kunnen, veelal op basis van aanvalspatronen, misbruik van webapplicaties en andere infrastructuurcomponenten detecteren. *Het detecteren van aanvallen gebeurt veelal op basis van bekende aanvalspatronen. Deze manier van detectie, op basis van 'handtekeningen' van bekende aanvallen, wordt ook wel signature-based genoemd. Tegenover de signature-based IDS'en staan de anomaly-based systemen. Deze systemen werken niet op basis van handtekeningen, maar op basis van afwijkingen (anomalieën).*

Beveiliging van poorten voor diagnoseprotocollen
De poorten die gebruikt worden voor diagnoseprotocollen, zoals SNMP, moeten met een geschikt beveiligingsmechanisme beveiligd zijn.

Netwerkadres
Servers, werkstations, pc's, laptops en thin cliënts worden in het netwerk geïdentificeerd door een centraal systeem dat inkomend en uitgaand verkeer wel of niet doorlaat, bijvoorbeeld op basis van het netwerkadres (IP-adres).

Netwerken met externe verbindingen
Bij gebruik van externe koppelingen buiten het gemeentelijke data- en telecommunicatienetwerk, bijvoorbeeld voor internet of connectie naar andere gebouwen, voldoet de beveiliging hiervan tenminste aan de geldende aansluitvoorwaarden om ongeautoriseerde toegang via "achterdeuren" te voorkomen. Dit moet door middel van documentatie aangetoond worden.
Bij gebruik van een draadloze externe verbinding moeten aanvullende maatregelen worden getroffen om ongeautoriseerde toegang en misbruik door derden te voorkomen. Bij het aanbieden van online diensten en transacties via de eigen website zijn adequate beveiligingsmaatregelen getroffen.

Draadloze en openbare netwerken
Gebruik van draadloze netwerken vraagt om specifieke beveiligingsmaatregelen. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn eveneens extra maatregelen nodig. Wettelijk is ten aanzien van persoonsgegevens minimaal encryptie vereist.

Actieve componenten
Voor logische toegang tot actieve componenten als routers, switches en firewalls gelden als basis dezelfde toegangsprocedures als voor de overige ICT voorzieningen. Daarbij voldoet de procedure aan de normen zoals gesteld Norm ICT-beveiligingsassessments DigiD.

8.7 Toegangsbeveiliging met betrekking tot werkstations

Inlogprocedure werkstations
De toegang tot een informatiesysteem verloopt via een inlogprocedure, bedoeld om het risico van ongeautoriseerde toegang te beperken. In de procedure is onder meer het maximale aantal toegestane inlogpogingen, wachtwoordlengte en frequentie van wijziging vastgelegd.

Gebruikersidentificatie en -authenticatie
Identificatie en authenticatie van de gebruiker vindt altijd plaats. Hierdoor zijn activiteiten in het (informatie)systeem herleidbaar tot een natuurlijk persoon. Identificatie en authenticatie kunnen plaatsvinden door middel van gebruikersnamen in combinatie met wachtwoorden, smartcards, tokens of SMS authenticatie.

Gebruik van systeemhulpmiddelen ('utilities')[5]
Het gebruik van systeemhulpmiddelen waarmee toegangscontroles in systemen en toepassingen kunnen worden getest en mogelijk worden doorbroken (bijvoorbeeld sniffers), wordt beperkt tot een klein aantal bevoegde gebruikers en nauwlettend beheerst.

Schermbeveiliging (clear screen)
Na een vaste periode van inactiviteit wordt een werkstation automatisch geblokkeerd. Bij werkstations op locaties met verhoogd risico moeten de programma- en netwerksessies afgesloten worden en wordt de gebruiker uitgelogd.

8.8 Toegangsbeveiliging met betrekking tot (informatie)systemen

Toegang tot (informatie)systemen
Autorisatie voor (informatie)systemen wordt verleend op grond van de rol van de medewerker.
Binnen het (informatie)systeem krijgt de medewerker alleen toegang tot de functionaliteit en gegevens die nodig zijn voor de uitvoering van zijn of haar rol/taken. Alle medewerkers hebben een individueel gebruikersprofiel zowel op netwerk als op applicatieniveau waardoor mutaties en zo mogelijk ook raadplegingen altijd zijn terug te herleiden tot een individu.

Componenten van (informatie)systemen
Een (informatie)systeem kan uit meerdere componenten bestaan, zoals applicatie, pc, netwerk, besturingssysteem, database, firewall. Voor elk van deze componenten moet autorisatie apart worden verleend.

(Informatie)systemen met vertrouwelijke of privacygevoelige gegevens
(Informatie)systemen die vertrouwelijke of privacygevoelige gegevens verwerken, vereisen speciale maatregelen, zoals het plaatsen in een aparte beveiligde omgeving of domein. De procesverantwoordelijke stelt expliciet de gevoeligheid van een (informatie)systeem vast en de noodzaak voor aanvullende maatregelen.

[5] Deze tools worden uitsluitend door de ICT-specialisten conform procedure gebruikt.

9. Verwerving, ontwikkeling en onderhoud van systemen

Doelstelling:
Het waarborgen dat beveiliging wordt ingebouwd in (informatie)systemen en dat beveiligingseisen worden meegenomen in het proces van systeemontwikkeling en -onderhoud.

Resultaat:
(Informatie)systemen waarin zoveel mogelijk geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Maatregelen en procedures waarmee de beveiliging tijdens de ontwikkeling en het onderhoud van (informatie)systemen wordt gegarandeerd.

9.1 Beveiligingseisen voor (informatie)systemen

Bij de ontwikkeling van (informatie)systemen moeten beveiligingseisen vanaf aanvang in het ontwerpproces worden meegenomen. Dit geldt ook voor afdeling overstijgende (informatie)systemen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Bij het onderhoud van (informatie)systemen moet informatiebeveiliging een vast aandachtspunt zijn. De volgende aspecten moeten bij ontwikkeling en onderhoud aan de orde komen:

- Beveiligingseisen zijn zoveel mogelijk onderkend, gedocumenteerd en goedgekeurd voordat een (informatie)systeem wordt ontwikkeld of aangekocht;
- Benodigde beveiligingsmaatregelen met betrekking tot audittrails en validatie van invoergegevens, interne verwerking en uitvoergegevens zijn, waar mogelijk, ingebouwd;
- Voor (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten, kunnen aanvullende beveiligingsmaatregelen nodig zijn die, op basis van classificatie en risicoanalyse, zijn vastgesteld;
- Bij extern toegankelijke applicaties, bijvoorbeeld webapplicaties, wordt extra aandacht besteed aan het voorkomen van ongeautoriseerde toegang.

9.2 Cryptografische beveiliging

Cryptografische systemen en technieken moeten worden toegepast in (informatie)systemen die vertrouwelijke en/of privacygevoelige gegevens verwerken en die onvoldoende kunnen worden beveiligd door andere maatregelen. Dit geldt met name voor gegevens die via openbare, grensoverschrijdende en draadloze netwerken worden getransporteerd (ook USB-sticks) en voor systemen die als standalone toepassing gebruikt worden, bijvoorbeeld op laptops, PDA's, tablets en smartphones.

Vertrouwelijkheid en onweerlegbaarheid zijn nauw aan elkaar verbonden door het gebruik van cryptografische sleutels. Als gebruik wordt gemaakt van asymmetrische versleuteling (verschillende sleutels voor versleuteling en ontsleuteling), is het publieke deel van de sleutel bestemd voor versleuteling (vertrouwelijkheid) van gegevens. Het privédeel van de sleutel is bestemd voor ontsleuteling en het plaatsen van digitale handtekeningen onweerlegbaarheid/onloochenbaarheid).
PKI-certificaten worden herkend in veel standaardtoepassingen, zoals webbrowsers en e-mailpakketten. Met behulp van algemene PKI-certificaten is de informatie die personen en organisaties over het internet sturen, op een hoog niveau beveiligd.

PKIoverheid-certificaten bieden aanvullende zekerheden. Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevens-uitwisseling.
PKIoverheid-certificaten worden gebruikt bij:

- het zetten van een rechtsgeldige elektronische handtekening;
- het beveiligen van websites;
- het op afstand authenticeren van personen of services;
- het versleutelen van berichten.

Wanneer er gebruik gemaakt wordt van cryptografische sleutels dan dient het sleutelbeheer te zijn georganiseerd. Het gaat dan met name om de bescherming van de sleutels, het inrichten van de beheersrollen en de recoverymogelijkheden. Een sleutelbeheersysteem moet er minimaal voor zorgen dat sleutels niet onversleuteld op de servers te vinden zijn.

9.3 Digitale handtekening

Bij gebruik van digitale handtekeningen als middel om de authenticiteit en integriteit van elektronische documenten te waarborgen, worden alle sleutels afdoende beveiligd tegen wijziging en vernietiging. Ook worden persoonlijke sleutels (private keys) beschermd tegen onbevoegde openbaarmaking.

9.4 Uitbesteding ontwikkeling van (informatie)systemen

In deze situatie ontwikkelt de gemeente niet zelf een (informatie) systeem, maar besteedt het ontwikkel- en productiewerk uit. De gemeente gaat vervolgens over tot aanschaf van het (informatie) systeem of afname van een dienst. Bij uitbesteding van de ontwikkeling van (informatie)systemen wordt rekening gehouden met:

- Aangaan van een formele overeenkomst op basis van de algemene leveringsvoorwaarden van de gemeente Westland;
- Licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten;
- Beoordeling en controle van de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
- Privacygevoeligheid en bedrijfsvertrouwelijkheid van testgegevens, bijvoorbeeld door het gebruik van anonieme of fictieve gegevens en ingeval door de leverancier persoonsgegevens worden bewerkt of deze meewerkt aan de totstandkoming van een bewerkersovereenkomst met de gemeente meewerkt in de zin van de Wet Bescherming Persoonsgegevens;
- Mogelijkheid tot uitvoeren van IT audits bij de leverancier op de interne beheersingsmaatregelen of bij de door de leverancier ingeschakelde derden namens de gemeente;
- Zorgen voor een borg in geval de externe partij in gebreke blijft (b.v. Escrow);
- De leverancier een Third Party Memorandum (TPM) of ISAE3402 verklaring verzorgt, of vergelijkbare verklaring van een onafhankelijke partij (Register EDP auditor) over de relevante interne beheersing van processen en in het bijzonder de beveiligingsprocessen en aan de gemeente verstrekt indien deze daarom verzoekt;
- De beschrijving van de dienst is opgenomen in de overeenkomst. Verwijzing per geleverde dienst naar de betreffende service level specificaties. Denk hierbij aan een concrete beschrijving van diensten, servicetijden (normale servicetijden, weekends, feestdagen en vakantiedagen), service beschikbaarheid, responsetijden, oplostijden et cetera;
- De beschrijving van de overlegstructuren, de contactpersonen en de onderlinge communicatie is opgenomen in de overeenkomst. Vastleggen wanneer gestructureerd overleg plaatsvindt, wie aan dit overleg deelnemen. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten (escalatiematrix);

- De beschrijving van de geschillenregeling is opgenomen in de overeenkomst. Beschrijving wat de procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener (-aanbieder);
- De beschrijving van prestatie indicatoren, de manier van meten en de rapportagestructuur is opgenomen in de overeenkomst. Beschrijving van de prestatie indicatoren (Key Performance Indicators (KPI's)), hoe deze worden gemeten en hoe hierover wordt gerapporteerd;
- Om zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de dienstverlening. Denk hierbij aan afspraken over de inhoud, de frequentie en de verspreiding (distributie) van de rapportage;
- De leverancier toereikende technische en organisatorische maatregelen heeft genomen om de webapplicatie en gerelateerde gegevens te beveiligen tegen verlies, diefstal en inzage door daartoe niet bevoegde personen;
- De leverancier in de overeenkomst aangeeft dat de gehanteerde beveiligingsmaatregelen, zowel technisch als organisatorisch up to date worden gehouden en voldoen aan de laatst bekende beveiligingsinzichten, beveiligingsnormen en –richtlijnen;
- Of ingeval van een webapplicatie tenminste jaarlijks penetratietesten worden uitgevoerd waarbij uitgangspunt is dat de leverancier de gemeente in staat stelt om aan haar verplichtingen als verantwoordelijke, voortvloeiend uit de aan de DigiD gekoppelde wet- en regelgeving, en de Wet Bescherming Persoonsgegevens (WBP) te voldoen.

9.5 Security baseline voor hardening

De gemeente hanteert een security baseline voor de systemen. De hardening van alle systemen maar met name de internet facing systemen dient strak te zijn geregeld. Voor de webapplicaties en systemen geldt: alles dat open staat moet een reden hebben en alles dat open staat moet secure worden aangeboden.

De hardening van interne systemen mag minder stringent. Voor interne systemen moeten de management functies secure zijn, er geen onveilige protocollen worden gebruikt, de default wachtwoorden zijn gewijzigd, en ongebruikte applicaties worden verwijderd.
Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaard (default) installatie proces. Alle componenten van de ICT-infrastructuur moeten deel uitmaken van het hardeningsproces.

Voorbeelden van risico's die door hardening teniet worden gedaan zijn:
- Indien (externe) systemen, zoals webservers en mailservers 'reclame' maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren;
- Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

De gemeente neemt de configuratiebaseline van de Security Benchmarks division (voorheen het Center for Internet Security (zie https://www.cisecurity.org) over. Het CIS levert ook een configuratie assessment (CIS CAT) tool om voor verschillende platforms afwijkingen van de benchmark vast te kunnen stellen.

9.6 Hardening van websites

Speciale aandacht krijgen hierbij de websites van de gemeente. Aangezien niet langer gebruikte websites of verouderde informatie die toegankelijk is via het internet een beveiligingsrisico opleveren dient de gemeente deze informatie te (laten) verwijderen. De gemeente en meer in het bijzonder de eigenaar van de specifieke website is hiervoor verantwoordelijk.

10. Beveiligingsincidenten

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

Resultaat:
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.

10.1 Definitie beveiligingsincident

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen.

Hierbij staat beschikbaarheid voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. Integriteit staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).

Voorbeelden van beveiligingsincidenten zijn: besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), niet beschikbaar zijn van de website met dienstverleningsportaal, verlies van usb-stick met gevoelige informatie, diefstal van data of hardware of een gecompromitteerde mailbox

10.2 Procedure melding en omgang beveiligingsincidenten

Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Hiervoor gelden de volgende uitgangspunten:

- De security manager is de beheerder van de registratie van beveiligingsincidenten;
- Een medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de Servicedesk van de gemeente;
- De beveiligingsincidenten worden bij de helpdesk als zodanig geregistreerd en vervolgens doorgegeven aan de security manager;
- Vermissing of diefstal van apparatuur of media die gegevens van de gemeente kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident;
- Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens en foutieve inlogpogingen worden regelmatig nagekeken.

- Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt;
- Afhankelijk van de ernst van een incident is er een meldplicht bij het College Bescherming Persoonsgegevens;
- Er is een procedure voor communicatie met de Informatiebeveiligingsdienst;
- De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

11. Continuïteitsbeheer

Doelstelling:
Het voorkomen van onderbreking van activiteiten van de gemeentelijke ICT-infrastructuur en het beschermen van de kritische bedrijfsprocessen tegen de effecten van ingrijpende storingen of calamiteiten.

Resultaat:
Een beheerst proces voor het waarborgen van de bedrijfscontinuïteit, waarmee de gebruikers, binnen een vastgestelde periode na het optreden van een beveiligingsincident of calamiteit, op aanvaardbaar niveau hun taken kunnen hervatten.

11.1 Proces van continuïteitsmanagement

Er is een beheerst proces vastgesteld om de bedrijfscontinuïteit van de organisatie als geheel te waarborgen. Het proces kent de volgende onderdelen:

- Elk gemeentelijke 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 het continuïteitsplan worden de maatregelen beschreven waarmee de kritische bedrijfsprocessen van een afdeling na een onderbreking of verstoring voortgezet of tijdig hersteld kunnen worden. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - De risico's van bedreigingen worden beoordeeld naar de waarschijnlijkheid dat zij zich voordoen, de eventuele schade als gevolg daarvan en het herstel;
  - 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 m.b.t de noodprocedures;
  - Kennis en kundigheid van personeel om de processen weer op te starten;
  - Wijze en frequentie van testen van het plan.
- Indien interne of externe uitwijk is gerealiseerd, wordt minimaal jaarlijks een uitwijktest uitgevoerd. De uitwijkprocedures zijn ondergebracht in het draaiboek uitwijk.

11.2 Relatie met nood- en ontruimingsplan

Het team I&A zorgt voor het vaststellen van een ontruimingsregeling voor de computerruimte(n). Dit in aansluiting op het algemene noodplan en ontruimingsplan. Hierin is aangegeven op welke wijze de computerfaciliteiten worden uitgeschakeld bij calamiteiten, eventueel van buitenaf op afstand te regelen. Voorts is vastgesteld hoe het team I&A de afgesproken regeling zal testen en met welke frequentie.

11.3 Veiligstelling programmatuur

Voor alle systeemsoftware en informatiesystemen moet een afweging gemaakt worden of de broncodes door middel van bijvoorbeeld een Escrow-contract bij derden moeten worden ondergebracht.

11.4 Monitoring capaciteit

Voor alle relevante ICT-middelen wordt het capaciteitsbeslag dusdanig gepland dat continu wordt voldaan aan de eisen die gesteld worden vanuit de afspraken met de afnemers van het systeem. Performanceproblemen worden tijdig gesignaleerd en geanalyseerd op basis van betrouwbare gegevens.

12. Naleving

Doelstelling:
Het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen en waarborgen dat systemen en processen voldoen aan het beveiligingsbeleid van de gemeente Westland.

Resultaat:
Maatregelen en procedures waarmee naleving van wetten, verplichtingen en beveiligingseisen uit het beleid van de gemeente bewaakt wordt.

12.1 Organisatorische uitgangspunten

- 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 het plan van aanpak 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 Securitymanager zorgt namens de gemeentesecretaris voor het toezicht op de uitvoering van het informatiebeveiligingsbeleid;
- ICT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatiebeveiligingsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring);
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI en BRP. Aanvullend op dit concern IB-beleid kunnen daarom specifieke normen gelden voor afdelingen;
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de controller informatiebeveiliging onderzocht door gemeentelijke auditors en door onafhankelijke externen (bijvoorbeeld door middel van ‘penetratietesten’). Jaarlijks worden meerdere audits/onderzoeken uitgevoerd. 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.

12.2 Naleving van informatiebeveiligingsbeleid en -plan

Om de naleving van de beveiligingseisen uit het informatiebeveiligingsbeleid en -plan te bewaken, legt de procesverantwoordelijke adequate organisatorische en procedurele afspraken vast. Kernelementen in het controle- en evaluatieproces zijn:

- Zelfevaluatie en/of een audit, tenminste eenmaal per jaar, door de Securitymanager;
- Managementrapportages, tenminste eenmaal per jaar, door de controller informatiebeveiliging voor zover mogelijk ingebed in bestaande P&C -cyclus.

12.3 Naleving van wettelijke voorschriften

Relevante eisen uit wet- en regelgeving en contractuele eisen moeten voor ieder (informatie)systeem zijn vastgelegd. Er wordt deskundig advies over specifieke juridische eisen ingewonnen bij de juridische adviseur(s) van de gemeente. Conform de Archiefwet beschikt de gemeente Westland over een Documentair Structuur Plan (DSP) waarin opslag, bewaartermijn en vernietiging van gegevens en informatie in analoge en digitale vorm is geregeld.

Aan de bescherming van persoonsgegevens stelt de Wet Bescherming Persoonsgegevens (WBP) duidelijke eisen. De gemeente Westland stelt een privacy beheerder aan, die de uitvoering en de naleving van de WBP bewaakt.

12.4 Beoordeling van de naleving

De procesverantwoordelijken controleren en evalueren de naleving van wettelijke voorschriften en van het informatiebeveiligingsbeleid. Zij beoordelen of alle beveiligingsprocedures binnen hun verantwoordelijkheidsgebied correct worden uitgevoerd en of hun processen en (informatie)systemen voldoen aan relevante wet- en regelgeving, beveiligingsbeleid, normen en andere beveiligingseisen. Zij controleren de naleving van technische normen door productiesystemen te onderzoeken op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen, bijvoorbeeld door het uitvoeren van een security scan. Daarnaast worden controles uitgevoerd door externe auditors (bv BRP-, SUWI- en BAG-audit en de externe accountant).

Begrippenlijst

Acceptatieprocedure
Procedure om vast te stellen of een nieuw (informatie)systeem voldoet aan de gestelde eisen Applicatiebeheer Onderhoud en exploitatie van de geautomatiseerde gedeeltes (software) van een informatiesysteem

Application controls
Geprogrammeerde maatregelen binnen een applicatie ter waarborging van de vertrouwelijkheid, juistheid en volledigheid van de data. We kunnen hierbij denken aan het afschermen van menukeuzes, waardoor informatie niet oproepbaar is of het controleren van input op juistheid (postcode check) of volledigheid.

Audit (informatiebeveiligings-)
Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid

Authenticatie
Verificatie van de geclaimde identiteit, bijvoorbeeld door gebruik van wachtwoord, token, biometrie of een combinatie hiervan

Autorisatie / autoriseren
Toekenning / toekennen van rechten (aan (groepen van) personen, processen en/of systemen)

Back-up
Reservekopie van een computerbestand of programmatuur

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen

Beschikbaarheid
zie Continuïteit

Beveiligingsincident
Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatiebeveiliging kan aantasten

Calamiteit
Gebeurtenis die een zodanige verstoring van de geautomatiseerde gegevensverwerking tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen

Change management
Beheer en beheersing van alle wijzigingen van componenten van (informatie)systemen en de ICT-infrastructuur

Classificatie
Indeling in risicoklassen voor de aspecten beschikbaarheid, betrouwbaarheid en vertrouwelijkheid

Clean desk
Een opgeruimde werkplek waar geen vertrouwelijke of privacygevoelige documenten of andere informatiebronnen rondslingeren

Clear screen
Een uitgeschakeld of afgesloten beeldscherm dat alleen met een inlogprocedure weer actief gemaakt kan worden

Afdelingoverstijgend informatiesysteem (CIS)
Systeem dat door meer dan één afdeling wordt gebruikt en waarin gegevens van meerdere organisatieonderdelen worden vastgelegd

Configuratie management
Beheer en beheersing van de samenstelling en de status van de ICTinfrastructuur en de (informatie)systemen die er gebruik van maken

Configuratieschema
Overzicht van de onderdelen waaruit een (informatie)systeem is opgebouwd

Continuïteit (bedrijfs-)
De mate waarin bedrijfsprocessen ongestoord doorgang kunnen hebben

Continuïteitsmanagement
Stelsel van samenhangende activiteiten, mensen en middelen met als doel de continuïteit van de (kritische) bedrijfsprocessen te waarborgen

Database
Een bestand waarin gedigitaliseerde gegevens op een gestructureerde manier zijn opgeslagen en bevraagd kunnen worden

Datakluis
Brand- en inbraakwerende ruimte voor de opslag van (elektronische) gegevensdragers

Document Structuurplan (DSP)
De Archiefwet maakt het maken en onderhouden van een Documentair Structuur Plan (DSP) verplicht. Een DSP biedt een overzicht van alle aanwezige informatie- en archiefbestanden van een organisatie in relatie tot het werk dat in die organisatie gedaan wordt.

Eigenaar
De eigenaar van een proces of een systeem is vanuit het informatiebeveiligingsbeleid verantwoordelijk voor het stellen van eisen en de inrichting van de controle hierop, zodat voldaan wordt aan het informatiebeveiligingsbeleid en aan de wettelijke eisen.

Escrow
Specifiek in de softwaresector wordt escrow aangewend ter vrijwaring van de belangen van de softwareklant indien die zich wil indekken tegen bepaalde risico's in hoofde van de softwareleverancier (het meest gevreesde daarbij wellicht het faillissement van de leverancier).
De softwareleverancier zal de broncode van de software (en de bijhorende documentatie) in bewaring geven bij de escrowagent, en deze broncode regelmatig updaten indien nieuwe versies op de markt gebracht worden. Indien de leverancier dan failliet zou gaan, heeft de klant tenminste de broncode van haar applicatie en kan zij alsnog trachten haar applicatie aan de praat te houden.

Functiescheiding
Het scheiden van gerelateerde taken en bevoegdheden met als doel het voorkomen van fouten en fraude

Fysieke beveiliging
Beveiliging die met behulp van fysieke (bouwkundige, technische en/of organisatorische) middelen gerealiseerd wordt

Gateway
Verbinding tussen verschillende netwerken waarop wordt bijgehouden welke computers c.q. protocollen met elkaar verbonden mogen worden

Gebruiker / gebruikende partij
Degene die geautoriseerd gebruik maakt van een (informatie)systeem

Gegevensdrager
Een fysiek object waarin/waarop informatie is vastgelegd, bijvoorbeeld een boek, harde schijf, DVD of USB-stick

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens

Informatie- en communicatietechnologie (ICT)
Het vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers.
Hieronder valt het ontwikkelen en beheren van systemen, netwerken, databanken en websites. Ook het onderhouden van computers en programmatuur en het schrijven van administratieve software valt hieronder. Vaak gebeurt dit in een bedrijfskundige context.

ICT-component
Onderdeel van de informatie- en communicatie infrastructuur, zoals netwerk, bekabeling, servers, werkstations.

Identificatie
Bepaling van de identiteit van een persoon, bijvoorbeeld door een unieke gebruikersnaam of netwerkadres

Incident
Onverwachte of ongewone gebeurtenis

Incident management
Beheer en beheersing van de afhandeling van incidenten

Informatiebeveiliging
Samenhangend stelsel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, integriteit, betrouwbaarheid en vertrouwelijkheid.

Informatievoorziening
Informatiebeveiligingsbeleid Strategie van een organisatie met betrekking tot informatiebeveiliging.

Informatiebeveiligingscoördinator
Medewerker die adviseert over informatiebeveiligingsvraagstukken in brede zin en activiteiten op het gebied van informatiebeveiliging coördineert

Controller informatiebeveiliging
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid en de escalatie van beveiligingsincidenten.

Informatiebeveiligingsplan
Document waarin beschreven staat welke beveiligingsmaatregelen getroffen worden/zijn op basis van het informatiebeveiligingsbeleid

Informatiesysteem
Een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen

Informatievoorziening
Het geheel aan processen, bestaande uit het verzamelen, het opslaan, het verwerken van gegevens en het beschikbaar stellen ervan

Internet Protocol (IP)
Veel gebruikt protocol voor netwerkverkeer

Information Technology Infrastructure Library (ITIL)
Een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie. ITIL is geen methode of model, maar eerder een reeks van best practices (de beste praktijkoplossingen) en concepten.
Local Area Network (LAN)
Zie Lokaal netwerk

Logische (toegangs)beveiliging
(Toegangs)beveiliging die met behulp van programmatuur gerealiseerd wordt

Lokaal netwerk (LAN)
Fysiek afgegrensd, instellinggebonden netwerk

Maatwerkprogrammatuur
Op specifiek (deel)proces toegesneden programmatuur

MARAP
Management Rapportage

Medium (opslag-)
Fysieke gegevensdrager

Netwerk
Een verzameling objecten voor communicatie tussen tenminste twee knooppunten van apparatuur en programmatuur, waarbij gebruik gemaakt wordt van voorgeschreven communicatieprotocollen

Netwerkadres (IP Adres)
Unieke identificatie van een element in een netwerk

Netwerkconfiguratie
Overzicht van de objecten waaruit het netwerk bestaat en de relaties tussen deze objecten

Noodplan
Document waarin beschreven staat welke acties een organisatieonderdeel moet ondernemen in een noodsituatie

Ontruimingsplan
Document waarin beschreven staat op welke wijze een gebouw ontruimd moet worden in een noodsituatie

OTAP
Een methodiek die wordt gebruikt in de ICT. Dit geeft een pad aan dat wordt doorlopen tijdens onder andere softwareontwikkeling of het implementeren van nieuwe applicaties.
Het pad dat wordt doorlopen is als volgt: Een programma of component wordt eerst ontwikkeld in de ontwikkelomgeving. Als de programmeur denkt klaar te zijn wordt het gekopieerd naar de testomgeving. Daar kan gecontroleerd worden of het programma of component naar behoren werkt en of het goed kan communiceren met zijn omgeving. Als het goed is bevonden wordt het gekopieerd naar de acceptatieomgeving. Dit is een omgeving waar een gebruiker in kan kijken maar waar normaal gesproken geen gebruikers bij kunnen. De gebruiker kan dan beoordelen of aan zijn eisen en specificaties is voldaan. Indien de gebruiker het programma of component goedkeurt wordt het gekopieerd naar de productieomgeving waar het gebruikt kan worden door alle gebruikers van het systeem.

Personal Digital Assistant (PDA)
Kleine computer, formaat “binnenzak”

PKI (Public Key Infrastructure)
Een Public Key Infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd. Een onafhankelijke partij waarborgt de integriteit en authenticiteit van het certificaat. Hiermee wordt gegarandeerd dat de identiteit van de certificaatbezitter klopt ("je bent wie je zegt dat je bent") en dat gegevens veilig kunnen worden uitgewisseld.

Privacy-beheerder
Medewerker die adviseert over privacybescherming en activiteiten ter bescherming van persoonsgegevens en privacy coördineert

Proces
Een samenhangende serie activiteiten ten behoeve van een van tevoren bepaald doel

Procesverantwoordelijkheid / procesverantwoordelijke
Verantwoordelijkheid / verantwoordelijke voor het geheel van activiteiten van een bepaald proces

Programmatuur
Het geprogrammeerde deel van (informatie)systemen

Recovery
Herstel van een computerbestand of programmatuur

Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen

Routering
Het bepalen van de weg die berichten volgen Security scan Gericht onderzoek naar de mate van implementatie van beveiligingsmaatregelen

Service Level Agreement (SLA)
Schriftelijke overeenkomst tussen een aanbieder (service provider) en een afnemer (klant) van bepaalde diensten

Smartphone
Programmeerbare telefoon die voor vele uiteenlopende doeleinden gebruikt kan worden, zoals internet

SNMP
Simple Network Management Protocol: zie diagnoseprotocol

Systeem
Een verzameling van één of meer samenhangende objecten met tezamen een gespecificeerde functionaliteit. Objecten kunnen zowel fysiek (computersysteem) als logisch (besturingssysteem) zijn

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem

Systeemhulpmiddel
Hulpprogramma voor beheer en onderhoud van (informatie)systemen en ICT-infrastructuur

Systeemklok
Interne klok in een computersysteem

Systeemprivilege
Recht op het gebruik van of toegang tot (een onderdeel van) een (informatie)systeem

Systeemprogrammatuur
Fundamentele, ondersteunende programmatuur die behoort tot de technische infrastructuur van een (informatie)systeem

Technisch beheer
Opslag en onderhoud van digitale informatie door middel van technische Maatregelen

Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding

Third Party Mededeling (TPM)
Verklaring van een onafhankelijke derde partij die door betrokken partijen vertrouwd wordt

Utility
Zie Systeemhulpmiddel

Voice over IP (VOIP)
Gebruik van dezelfde netwerkbekabeling voor zowel spraak- als datacommunicatie

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden

Wide Area Network (WAN)
Netwerk dat zich niet beperkt tot één fysieke locatie en waaraan meerdere lokale netwerken (LAN's) gekoppeld kunnen zijn