BELEIDSNOTA INFORMATIEBEVEILIGINGSBELEID 2018-2021

GEMEENTE WESTLAND

Cluster	Bedrijfsvoering
Auteur(s)	A.J. den Drijver / MT van Rijn
Datum	11 december 2018
Status	Definitief

ALG HS 020

Inhoudsopgave

Wijzigingentabel

Wijzigingentabel oude beleid vs geactualiseerd beleid.

Oude beleid	14-0428020, Gemeentebreed Informatiebeveiligingsbeleid
Geactualiseerd beleid	18-0251091, Informatiebeveiligingsbeleid 2018-2021
Wijzigingentabel	18-0287914, Wijzigingentabel Informatiebeveiligingsbeleid 2018-2021

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 inwoners en bedrijven de klanten optimaal te kunnen helpen en adviseren. Daarnaast moeten burgers en bedrijven erop kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

Informatisering en koppelingen van systemen speelt een steeds prominentere rol in de gemeentelijke organisatie. De gemeente is 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 de menselijke factor (het menselijk gedrag) een doorslaggevende rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk.

De veiligheid van informatie speelt vandaag de dag en in de toekomst een belangrijke rol. Om te voorkomen dat binnen ieder domein separaat beleid ontwikkeld en geïmplementeerd wordt, is in 2015 de keuze gemaakt om een gemeentebreed informatiebeveiligingsbeleid op te stellen. Voor u ligt het geactualiseerde beleid voor 2018 tot en met 2021[1]. In de basis is het beleid gebaseerd op het voorgaande vastgestelde beleid (B&W, 8 maart 2016) en zijn er kleine inhoudelijke aanpassingen gedaan. Daarnaast is beleid geformuleerd ten aanzien van Eigentijds Werken dat verbonden is aan voorliggend informatiebeveiligingsbeleid.
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 technische beveiligingsmaatregelen, aanvullende richtlijnen en 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 VNG-realisatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG 2013) vormt hiervan een voorbeeld. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die gebaseerd zijn op de internationale standaarden voor informatiebeveiliging NEN/ISO 27001:2005 en 27002:2005, bieden een meetlat voor gemeenten om hun Informatiebeveiliging op orde te brengen en te houden.

[1] De verwachting is dat medio 2019 de Baseline Informatiebeveiliging Overheid (BIO) in de plaats komt van de BIG. Omdat de grondslag van BIG en BIO beide ISO 27001/27002 zijn heeft dit voor het beleid nauwelijks gevolgen.

Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000:2005 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG-realisatie) 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 Basisregistratie Personen (Wet BRP), Algemene Verordening Gegevensbescherming (AVG), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en Wet Openbaarheid Bestuur (Wob).

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 Basisregistratie Grootschalige Topografie (BGT) Wet Kenbaarheid Publiekrechtelijke Beperkingen (Wkpb), de 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 figuur 1 aangegeven welke stappen in de implementatie en doorlopende borging van informatiebeveiliging te onderscheiden zijn.

Figuur 1: De informatiebeveiligingspiramide

Bovenaan de piramide treffen we het informatiebeveiligingsbeleid aan. Dit is een organisatiebreed 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 door de verantwoordelijke.

De tweede laag van de piramide is gericht op het continue verbeteren van de informatie-beveiliging. De basis daarvoor vormen de zelfevaluatie ENSIA (Eenduidige Normatiek Single Information Audit zie pagina 10 2.4 punt 2) en eenmaal per drie jaar uitvoeren van een GAP/Impact analyse. Uitkomsten van deze twee leiden tot een verbeterplan van te nemen maatregelen.

Daarnaast vindt er jaarlijks volgend uit de BRP een risico inventarisatie en evaluatie (RI&E) plaats. Daarin wordt ingeschat hoe kwetsbaar de gemeente is op basis van een risicocatalogus met informatiebeveiligingsrisico's.

In de Informatiebeveiligingsanalyse 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.

In de derde laag volgt, na de Informatiebeveiligingsanalyse, de vorming van een actieplan vanuit het verbeterplan. Tijdens deze stap worden de geconstateerde risico's gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van de risico's en de te treffen maatregelen.

- Het actieplan komt tot stand door middel van een prioriteringssessie van het verbeterplan waarin de procesverantwoordelijke zelf aangeeft welke specifieke verbeteracties zij willen en kunnen oppakken voor een periode van één jaar;
- Naast het formuleren van de specifieke verbeteracties worden onder andere de uitvoerders, de kosten en de planning vastgelegd;
- Dit compacte actieplan vormt de praktische leidraad voor de te implementeren maatregelen van de BIG door de beveiligingsorganisatie.

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 de BRP, de BAG of het financiële pakket, maar kan ook gericht zijn op bijvoorbeeld de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.

1.3. Toelichting op ISO 27001/27002 (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 planmatige 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) maar ook de BIO (2019/2020) zijn afgeleid van deze internationale informatiebeveiligingsnormen. Eventuele veranderingen in deze grondslagen en de gevolgen daarvan voor de organisatie worden door de CISO gevolgd en geïnitieerd.

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, alarmering);
- 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, Eigentijds 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. 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):
- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Wet Bescherming Persoonsgegevens (WBP);
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet/Archiefregeling;
- Databankenwet;
- Wet Elektronisch Bestuurlijk Verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer;
- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet Openbaarheid Bestuur (WOB);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet ruimtelijke ordening (WRO).

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.

2. Informatiebeveiligingsbeleid

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

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 behoort een gemeentebreed beleidsdocument voor informatiebeveiliging goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen.

Minimaal zijn de volgende aspecten in dit beleidsdocument aanwezig:

- De doelstellingen van informatiebeveiliging voor de gemeente;
- De beveiligingseisen;
- De organisatie van informatiebeveiliging (zie hoofdstuk 3);
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging voor leidinggevenden, medewerkers en ondersteunende teams en rollen;
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd ;
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst.

2.2. Scope van het informatiebeveiligingsbeleid

De scope van dit beleid omvat alle informatieprocessen die onder verantwoordelijkheid van de gemeente vallen. Dit betreft zowel de ambtelijke als bestuurlijke informatieprocessen. Het beleid heeft niet alleen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook op informatie in fysieke c.q. analoge vorm, ongeacht de locatie, tijdstip en gebruikte apparatuur. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college en de gemeenteraad. Daarnaast bevat dit document de uitgangspunten voor handelen ten aanzien van informatieprocessen met keten- en uitvoeringspartners. Alle beleidsuitgangspunten met betrekking tot informatiebeveiliging en de organisatie van informatiebeveiliging zijn in dit gemeentebreed document samengebracht.

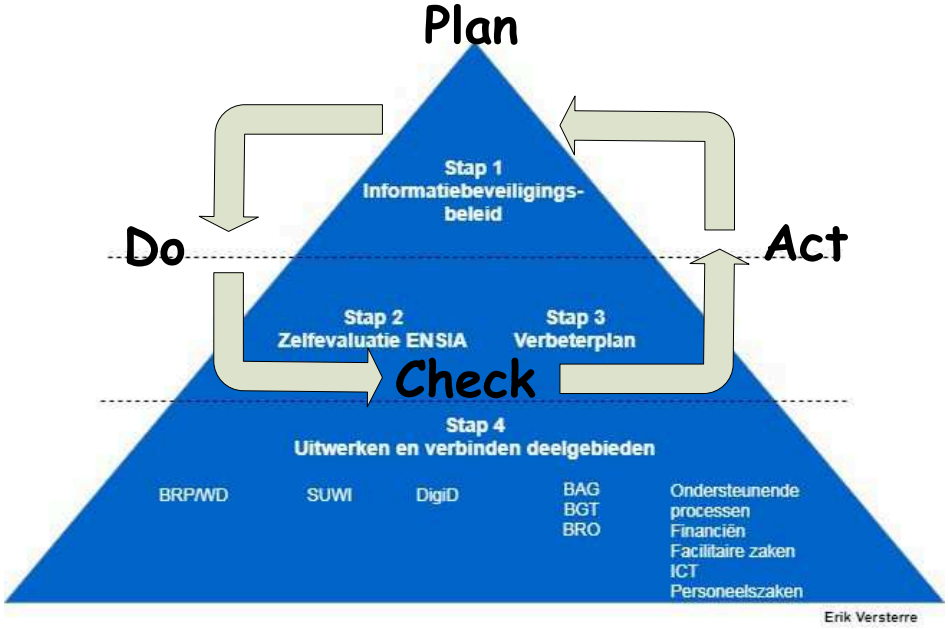
2.3. Aanvullende maatregelen

Als uit risicoanalyses blijkt dat voor bepaalde gegevensverwerkingen of omstandigheden meer of andere maatregelen nodig zijn dan de maatregelen die in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) zijn beschreven moeten door de daarvoor verantwoordelijke proces of systeem eigenaar aanvullende maatregelen worden getroffen. Bij minder risicovolle verwerkingen of omstandigheden kan worden overwogen maatregelen uit de BIG deels of niet te implementeren (pas toe of leg uit).

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:

1. Informatiebeveiligingsbeleid. Bevat het informatiebeveiligingsbeleid en de visie op informatiebeveiliging. Bijstelling van het informatiebeveiligingsbeleid vindt plaats om de 3 jaar of bij grote wijzigingen;
2. Informatiebeveiligingsanalyse.
    a) De risicoanalyse en de GAP-analyse (de toets aan de praktijk) op basis van het informatiebeveiligingsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd.
    b) Jaarlijks wordt een zelfevaluatie uitgevoerd, georganiseerd door de Rijksoverheid. Via deze ENSIA-methode (Eenduidige Normatiek Single Information Audit) wordt de gemeente bevraagd op getroffen maatregelen ten aanzien van informatiebeveiliging. Een selectie van normen uit de BIG wordt getoetst middels een zelfevaluatie; daarnaast wordt van de gemeente een verantwoording gevraagd over aangewezen normenkaders. Het college legt vervolgens met een collegeverklaring verantwoording af aan het Rijk en de gemeenteraad over de mate van voldoen aan deze aangewezen normenkaders.
3. Verbeterplan. Bevat de concrete verbeteracties volgend uit de risicoanalyse, GAP-analyse en de ENSIA-zelfevaluatie. Dit verbeterplan wordt periodiek geëvalueerd en waar nodig bijgesteld. Over de uitvoering van het verbeterplan wordt aan het bestuur en voor wat betreft de verbeteracties voortvloeiend uit ENSIA aan de toezichthoudende instanties gerapporteerd.



Figuur 2: De informatiebeveiligingspiramide met PDCA-cyclus

18-0251091

3. Organisatie van 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 informatiebeveiliging.

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. Controle en toetsing door de Raad

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging. Elk jaar wordt de raad door middel van een paragraaf Bedrijfsvoering in de jaarrekening op de hoogte gebracht over de stand van zaken en in hoeverre de gemeente voldoet aan de BIG.

3.1.2. 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 met het voorliggende beleid de kaders vast 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 bevoegdheden op het gebied van beveiliging gemandateerd aan de gemeentesecretaris.

3.1.3. Gemandateerde verantwoordelijkheden op organisatieniveau

De bevoegdheden voor informatiebeveiliging zijn gemandateerd aan de Directeur Bedrijfsvoering. Deze stelt met het directieteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De Directeur Bedrijfsvoering is verantwoordelijk voor de juiste implementatie van het informatiebeveiligingsniveau in de bedrijfsprocessen en wijst daarvoor een verantwoordelijke aan (procesverantwoordelijke). Ondersteunend aan de processen zijn de in- en externe (informatie)systemen en ook hiervoor wijst de Directeur Bedrijfsvoering een verantwoordelijke aan (systeemeigenaar). De operationele verantwoordelijkheid ligt bij leidinggevenden op organisatieniveau. De Directeur Bedrijfsvoering heeft in ieder geval de volgende verantwoordelijkheden:

- Het stellen van operationele kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op risico's omtrent informatiebeveiliging;
- Periodiek (laten) evalueren van beleidskaders en deze (laten) 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.

3.1.4. Verantwoordelijkheden op cluster- en direct onderliggend niveau

De leidinggevenden (clusterdirecteuren en respectievelijk teammanagers) zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun cluster c.q. taakveld. Zij hebben in ieder geval de volgende verantwoordelijkheden:

- Dataclassificatie van applicaties en gegevensverzamelingen
- Medewerkers meenemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen;
- Het (laten) uitvoeren van maatregelen uit de informatiebeveiligingsanalyse die op het cluster van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor hun informatiesystemen;
- 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).

3.1.5. Taakveldverantwoordelijke I&A

Het Taakveld I&A van de gemeente Westland, waarvan systeembeheer deel uit maakt, beheert de werkplekken, serverplatformen, lokale netwerken, wifi-verbindingen, externe netwerkverbindingen en verzorgt het technische en functionele (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij medeverantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. De Taakveldverantwoordelijke I&A is tevens verantwoordelijk voor de implementatie van ICT-technische beveiligings-maatregelen. Door I&A wordt verantwoording over de getroffen beveiligingsmaatregelen aan de procesverantwoordelijken en systeemeigenaren afgelegd.

3.1.6. Taakveldverantwoordelijke Facilitaire Zaken en Huisvesting

De Taakveldverantwoordelijke Facilitaire Zaken en Huisvesting is verantwoordelijk voor de fysieke toegangsbeveiliging en de kantoorinrichting (gebouwen, archiefkasten, kluizen enzovoort).

3.1.7. Taakveldverantwoordelijke POO

De Taakveldverantwoordelijke POO is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviserende rol op het gebied van organisatie- en informatieprocessen.

3.1.8. Functionaris gegevensbescherming

De FG is de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente. De FG heeft een aantal wettelijke taken volgens artikel 39, lid 1 van de Algemene Verordening Gegevensbescherming (AVG). De invulling van deze rol is vastgelegd in de Regeling Functionaris Gegevensbescherming (corsanummer 18-0160917).

18-0251091

3.1.9. De Chief Information Security Officer (CISO[2])

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages. De CISO is tevens de ENSIA-coördinator voor de gemeente. De CISO heeft in ieder geval de volgende verantwoordelijkheden:

- Kan rechtstreeks rapporteren aan de Directeur Bedrijfsvoering;
- Coördineert het formuleren van informatiebeveiligingsbeleid;
- Stelt de risicoanalyse en de GAP-analyse op en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatiebeveiligingsmaatregelen uit de informatiebeveiligingsanalyse en de uitvoering van het actieplan informatiebeveiliging;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatiebeveiliging;
- Ondersteunt de Directeur Bedrijfsvoering en het DT met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatiebeveiliging;
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse;
- Bevordert het beveiligingsbewustzijn in het kader van informatiebeveiliging en privacy in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Rapporteert over de informatiebeveiliging van de gemeente in het jaarverslag en met de collegeverklaring die voortkomt uit ENSIA.
- Coördineren van de jaarlijkse verantwoording over informatiebeveiliging aan de hand van ENSIA.

3.1.10. De controller informatiebeveiliging

Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten. De rol van controller is belegd binnen het cluster Bedrijfsvoering en is verantwoordelijk voor de verbijzonderde interne controle (VIC) op informatiebeveiliging. De controller heeft in ieder geval de volgende verantwoordelijkheden:

- Periodiek toetsen op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatiebeveiliging. De controller informatiebeveiliging is hiervoor verantwoordelijk, maar organiseert dit proces waar mogelijk met de inzet van beveiligingsbeheerders;
- Controleren op de voortgang van het uitvoeren van de maatregelen uit de informatiebeveiligingsanalyse en actieplan informatiebeveiliging;
- Controleren op de periodieke actualisatie van het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse;
- Toetsen/bewaken van het niveau van informatiebeveiliging;
- Toetsen van evaluatieproces van beveiligingsincidenten.

[2] Binnen de gemeente Westland wordt deze functionaris ook aangeduid als de security manager.

- Rapporteren van bevindingen aan de gemeentesecretaris en het college van B&W.

Naast de gemeentebrede rol van controller voor informatiebeveiliging, wordt er binnen twee specifieke deelgebieden wettelijk een controlefunctionaris voorgeschreven. Dit betreft het gebied van reisdocumenten en van rijbewijzen. Het betreft de volgende benamingen:

- *Beveiligingsfunctionaris reisdocumenten*
  Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- *Beveiligingsfunctionaris rijbewijzen*
  Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

3.1.11. Privacy officer

Deze rol is gericht op de uitvoering en naleving (op uitvoerend niveau) van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De privacy officer heeft in ieder geval de volgende verantwoordelijkheden:

- Beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de privacywetgeving en adviseert het DT en CT bij wijzigingen in procesuitvoering, bedrijfsvoering en de toepassing van een privacy impact assessment.
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- De privacy officer heeft verder als taak:
  a) Uitleggen van de privacy voorschriften in de AVG, en daarnaast in de sectorale wetgeving;
  b) Coördineren van de privacy werkzaamheden;
  c) Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
  d) Verzorgen van meldingen bij de functionaris gegevensbescherming (FG).
  e) Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
  f) Rapporteren aan het DT;
  g) Informeren van de Functionaris Gegevensbescherming (FG);
  h) Inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
  i) Beheer en onderhoud van de standaarddocumenten voor bewerkersovereenkomsten, convenanten en reglementen;
  j) Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van bewerkersovereenkomsten en convenanten en de vaststelling van reglementen.

3.1.12. Security Officer SUWI

De Security Officer SUWI (de beveiligingsbeheerder SUWI) betreft een wettelijk voorgeschreven functionaris en wordt hierom nader beschreven. De Security Officer SUWI beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet en ziet er daarnaast op toe dat de maatregelen worden nageleefd. Ook adviseert de Security Officer medewerkers en management, doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet en

evalueert de uitkomsten van de IT-audit in het kader van ENSIA. De resultaten uit de IT-audit kunnen aanleiding zijn tot het opstellen van een verbeterplan voor SUWI. De Security Officer SUWI stelt dit plan op en verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de voortgang van de verbetermaatregelen aan het hoogste management en/of college. De Security Officer SUWI vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

3.1.13. De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatiebeveiliging binnen een specifiek deelgebied. 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:

- DigiD (per DigiD-aansluiting een beheerder),
- BRP (Gegevens- en Informatiebeheerder),
- Waardedocumenten (Autorisatiebevoegde Reisdocumenten en Rijbewijzen),
- SUWI (Security Officer SUWI), zie paragraaf 3.1.9,
- BAG,
- BGT,
- BRO,
- Eventuele nader te bepalen rollen met betrekking tot de ENSIA-verantwoording.

<u>Gegevens- en Informatiebeheerder BRP</u>
Verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening en verantwoordelijk voor het geheel van activiteiten gericht op beleidsvoorbereiding ter zake de gegevensverzameling, de ontwikkeling van kwaliteitsprocedures, beveiligingsprocedures, verstrekking- en privacyprocedures, evenals de coördinatie bij de uitvoering van deze procedures.

<u>Autorisatiebevoegde Reisdocumenten en Rijbewijzen</u>
Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations) en verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering:

- Facilitaire Zaken,
- ICT,
- DIV (Archivering),
- P&O,
- Financiën.

De beveiligingsbeheerder is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die

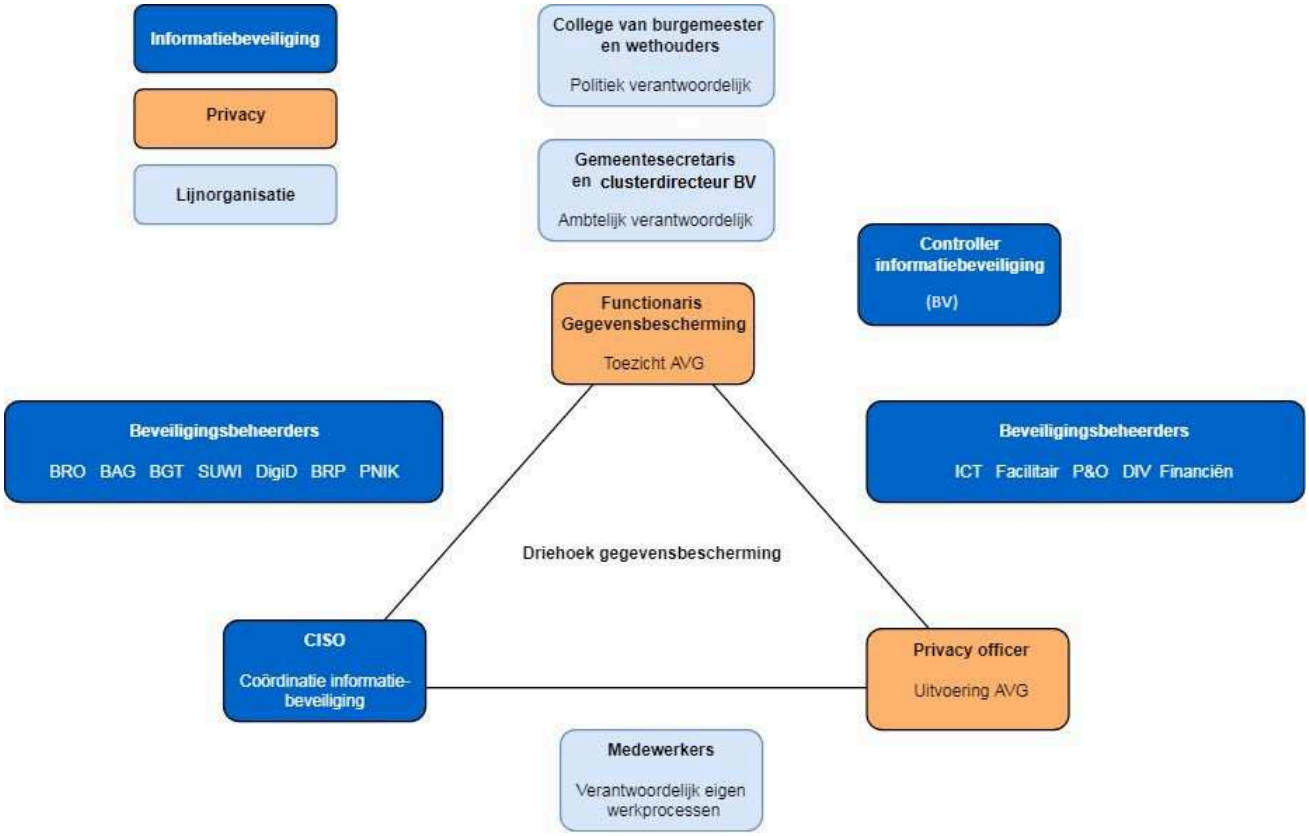
voortkomen uit het informatiebeveiligingsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie-onderdelen gelden. Hieronder vallen:

- De voorbereiding en coördinatie van audits en (zelf)evaluaties;
- De preventie en detectie van beveiligingsincidenten en het geven van een adequate respons;
- Coördineren en toepassen van specifieke wet- en regelgeving;
- Rapporteren aan de CISO.

3.1.14. De medewerkers

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

De personen met de toegewezen rollen in de beveiligingsorganisatie zijn benoemd in het document “Beveiligingsorganisatie 2018-2021” 18-0252872.



3.2. Overleg en afstemmingsorganen

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

- De CISO;
- Privacy officer;
- Beveiligingsbeheerders;
- Agendaleden: controller informatiebeveiliging en FG.

Onderwerpen (niet uitputtend):

- Voortgang uitvoering maatregelen verbeterplannen;
- Behandeling beveiligingsincidenten;
- Behandeling IBD-meldingen;
- Planning en voorbereiding van audits, inspecties en evaluaties;
- Evaluatie en actualisatie informatiebeveiliging en informatiebeveiligingsanalyse.

3.3. Informatiebeveiliging crisisbeheersing

Voor potentiele interne crisisbeheersing dient een kernteam informatiebeveiliging geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Het team staat onder leiding van de Driehoek Gegevensbescherming. Het team wordt ingezet in lijn met de mogelijke impact van de betreffende calamiteit. Dit team bestaat uit:

- De CISO;
- De Functionaris Gegevensbescherming;
- De privacy officer;
- Clusterdirecteur Bedrijfsvoering
- Taakveldverantwoordelijke I&A;
- Betrokken DT/CT-lid;
- De beveiligingsbeheerder ICT;
- Relevante experts, zoals beveiligingsbeheerders;
- Een lid van het Taakveld Communicatie.

3.4. Rapporteren informatiebeveiligingsincidenten

De CISO wordt door de procesverantwoordelijken geïnformeerd over informatiebeveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, 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 incidenten.
Incidenten worden bijgehouden in een registratie, hierbij wordt in ieder geval vastgelegd:

- Wat is de aard van het (bijna) incident?
- Wat is de oorzaak dat dit (bijna) incident heeft plaatsgevonden?
- Is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures?
- Is het (bijna) incident verwijtbaar?
- Is een eventuele tekortkoming in de beveiliging inmiddels hersteld?
- Welke acties moeten worden getroffen om herhaling te voorkomen?

Er wordt minimaal eenmaal per jaar gerapporteerd aan de directie door de Driehoek Gegevensbescherming.

3.5. Verantwoordelijkheden systeemeigenaren

De eigenaar van een (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. Voor cluster overstijgende systemen is de taakveldverantwoordelijke I&A aangewezen als eigenaar.

3.6. Verantwoordelijkheden procesverantwoordelijken

De procesverantwoordelijke draagt er zorg voor dat:

- De inrichting van een proces voldoet aan de daaraan te stellen beveiligingsnormen;
- Alleen die medewerkers toegang hebben tot gegevens die zij voor de uitoefening van hun taak nodig hebben;;
- De medewerkers bekend zijn met de voor hun geldende beveiligingsnormen.

3.7. Contracten met derden

3.7.1. Service level agreement (niveau van dienstverlening)

Bij structurele en/of langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations wordt tussen een cluster c.q. team 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 verlenen aan derde partijen

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 geauthentiseerde en geautoriseerde toegang vastgesteld wordt;
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt in het kader van de AVG een door Westland vastgestelde verwerkersovereenkomst 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 wordt door de externe partij jaarlijks gerapporteerd.

3.7.4. Overeenkomsten met een derde partij en met betrekking tot ICT voorzieningen

Bij het aangaan van overeenkomsten met derde partijen is er minimaal aandacht voor beveiligingsmaatregelen zoals vastgelegd in de GIBIT en de BIG. Aan minimaal de volgende beveiligingsmaatregelen wordt aandacht besteed:

- Te nemen beveiligingsmaatregelen zijn voorafgaand aan het ingaan van het contract gedefinieerd en geïmplementeerd;
- Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden;
- In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen;
- In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring;
- Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid;
- In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn;
- Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken;
- De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

3.7.5. Verwerkers van persoonsgegevens

De algemene verordening gegevensbescherming (AVG) (van kracht per 25 mei 2018) stelt regels voor het verwerken van persoonsgegevens. Wanneer de gemeente het verwerken van persoonsgegevens bij een andere partij uitbesteedt noemt men deze andere partij ‘een verwerker’. Het gemeentebestuur van de gemeente Westland blijft in dat geval de verantwoordelijke voor de verwerking van persoonsgegevens.
Nadere regels over de omgang met verwerkers zijn vastgelegd in de Regeling Functionaris Gegevensbescherming (corsanummer 18-0160917).

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 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 Taakveld 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 procesverantwoordelijken en beheerders zijn.

Het Cluster Bedrijfsvoering (in uitvoering door “De Groene Schakel)) houdt een registratie bij van alle fysieke voorzieningen die verband houden (informatie) veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.

Het Cluster Bedrijfsvoering (POO) houdt in nauwe samenwerking met de Servicedesk een registratie bij van alle medewerkers en extern personeel dat vanwege uitoefening van de opgedragen werkzaamheden gebruik moet kunnen maken van gemeentelijke ICT-voorzieningen.

4.2. Eigendom van informatie en bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen behoren een eigenaar te hebben. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit wordt een verantwoordelijke 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 informatie-processen. Hieronder volgen de geldende uitgangspunten:

- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming, al dan niet generiek geregeld, vooraf van de locatie worden meegenomen;

- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de proceseigenaar worden gedelegeerd, maar de proceseigenaar 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. Hierbij wordt nadrukkelijk rekening gehouden met de privacy van eventuele betrokkenen;
- Medewerkers gebruiken gemeentelijke informatie uitsluitend 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;
- Ten aanzien van het gebruik van mobiele apparatuur van de gemeente, en eventueel privémiddelen die worden gebruikt voor werkzaamheden voor de gemeente, worden nadere handreikingen opgesteld ten aanzien van veilig gebruik. In ieder geval geldt:
  - Illegale software, of niet goedgekeurde software, mag niet worden gebruikt voor de uitvoering van het werk;
  - Wanneer privémiddelen worden gebruikt voor werkzaamheden voor de gemeente, geldt de plicht deze middelen adequaat te beveiligen;
  - Gedragsregels gelden ook wanneer werkzaamheden worden uitgevoerd met privémiddelen.
- 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
  - 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. Minimaal worden de primaire gemeentelijke informatiesystemen geclassificeerd op de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatie niveaus per kwaliteitsaspect weer. Na deze classificatie is duidelijk welke maatregelen per informatiesysteem nodig zijn.

Classificatietabel				
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**	**Imago**
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner of Google maps)*	**Niet van belang** het image wordt niet beïnvloed bij afwijking van een van de drie classificaties
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*	**Intern** het image wordt intern beïnvloed bij afwijking van een van de drie classificaties
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: voorwaardelijke primaire proces informatie)*	**Extern: lokaal** het image wordt beperkt regionaal beïnvloed bij afwijking van een van de drie classificaties
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke gemeentelijke informatie op de website o.a waaraan rechten zijn te ontlenen)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties BRP en SUWI)*	**Extern: landelijk** het image wordt regionaal en landelijk beïnvloed bij afwijking van een van de drie classificaties

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. Het Cluster Bedrijfsvoering (POO) 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 de CAR/UWO en gemeentelijke protocollen;
- Regels die volgen uit dit beleid en andere gemeentelijke protocollen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

5.2. Voorwaarden personeel in dienst

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 Westlands gedragsprotocol. Daarnaast overlegt iedere nieuwe werknemer een Verklaring Omtrent Gedrag (VOG). Daarnaast wijst de teammanager de medewerker op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of binnen het cluster of team.

5.3. Voorwaarden externen

Externe medewerkers die toegang hebben tot gemeentelijke informatie tekenen een geheimhoudingsverklaring en dienen te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol en het Westlands gedragsprotocol. Alle externe medewerkers die toegang hebben tot vertrouwelijke (persoons)gegevens overleggen een VOG. Dit wordt in contracten met de werkgever van extern personeel vastgelegd. Daarnaast wijst de teammanager de externe bovendien op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of binnen het cluster of team.

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. Afwijkingen hierop worden door de teammanager goed

gekeurd. Bij dienstbeëindiging worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement met onmiddellijke ingang en volgens een vastgestelde procedure verwijderd bij dienst beëindiging of aangepast aan bij wijziging van functie.

5.6. Opleiding en communicatie

Alle medewerkers (in- en extern) hebben basiskennis met betrekking tot procedures voor de informatiebeveiliging. Ten aanzien van communicatie en bewustwording geldt dat:

- Alle medewerkers binnen de organisatie worden ingelicht over het informatiebeveiligingbeleid 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 DT en de leidinggevenden de algehele communicatie en bewustwording rondom informatiebeveiliging bevorderen;
- Het lijnmanagement bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen;
- In werkoverleggen periodiek aandacht wordt geschonken aan informatiebeveiliging. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

5.7. Bijzondere situaties

In het geval van ernstige verdenkingen tegen een medewerker of derde 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 opsporingsmogelijkheden is vooraf schriftelijke toestemming nodig van de gemeentesecretaris. Bij het gebruik daarvan wordt in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) gehandeld en wordt van rechtswege (Wet op de ondernemingsraden, artikel 27, lid k) toestemming aan de Ondernemingsraad gevraagd.

Specifiek bij het inrichten, testen en onderhouden van: systemen; apparatuur; software; en bij incidenten, kan zonder toestemming van de gemeentesecretaris toegang worden verkregen. Wanneer tijdens deze handeling iets wordt geconstateerd ten aanzien van een eigen medewerker, kan dient hier uitsluitend via de formele weg (via de gemeentesecretaris) melding van te worden gemaakt.

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. Indien hieraan niet wordt voldaan overtreedt de gemeente de Algemene Verordening Gegevensbescherming, artikel 32, waarin wordt voorgeschreven dat passende technische en organisatorische maatregelen moeten worden genomen om persoonsgegevens te beschermen;
- 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 Algemene Verordening Gegevensbescherming (AVG) en nadere regels;
- 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 (zie 4.1). Voor het gemeentehuis en het gemeentekantoor ligt dit in uitvoering bij De Groene Schakel, onder verantwoordelijkheid van het Cluster bedrijfsvoering. Voor de overige gemeentelijke panden en locaties is het Cluster Ruimte verantwoordelijk. Hieronder vallen:

- De preventieve, detectieve, correctieve en repressieve systemen met betrekking tot inbraak, ontruiming, brand en toegang;
- Overzicht van toegangsrechten van personen tot besloten ruimten, gebouwen en terreinen van de gemeente.

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 ICT-ruimten

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

- De leden van Taakveld I&A die uit hoofde van functie (technische) werkzaamheden aan de centrale computers of telecom apparatuur moeten verrichten;
- De door de clusterdirecteur van het cluster (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 Taakveld I&A.

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 Taakveld 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 heeft een "clean desk"-beleid voor papieren en verwijderbare opslagmedia, zodat dit soort materialen niet onbeheerd op het bureau mogen liggen. Daarnaast een "clear screen" -beleid voor ICT-voorzieningen. Dit betekent dat men actief en zonnodig 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, mobiele apparatuur en ICT-voorzieningen tijdens en buiten normale werktijden te beperken.

6.9. Beveiliging van mobiele apparatuur

Mobiele apparatuur moet zowel binnen als buiten het gebouw fysiek beschermd worden naar de aard van het gebruik. Dit betreft laptops, 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 nooit 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, multifactor-authenticatie, enzovoort;
- Bij gebruik van draadloze apparatuur 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 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 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;
- Updates die ten behoeve van het verhogen van de veiligheid worden vrijgegeven door de leverancier worden zo spoedig mogelijk via de 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. Papier wordt door een gecertificeerde partij afgevoerd en vernietigd.

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 voor het technisch beheer met de ISO 20000-1 en ISO 20000-2 (ITIL 3) en voor het functioneel beheer met de uitgangspunten van BISL.

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:

Changemanagement / 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). (De gehele OTAP procedure wordt echter alleen voor grote informatiesystemen toegepast);
- 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, waaronder persoonsgegevens, 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;
- De capaciteit 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-voorzieningen
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 Taakveld I&A verantwoordelijkheden en procedures op ten aanzien van de monitoring van de capaciteit.

Probleemmanagement – identificeren en afhandelen van fouten in de ICT-voorzieningen
Het Taakveld I&A richt een organisatie in en stelt procedures op ten aanzien van het achterhalen en wegnemen van veelvoorkomende incidenten.

IT service continuity management – waarborgen van de continuïteit van de ICT-dienstverlening
Het Taakveld I&A 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 I&A reservekopieën van alle essentiële bedrijfsgegevens en programmatuur, zodat in het geval van een incident de gegevensverwerking binnen acceptabele tijd kan worden hervat;
- 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 in de dataclassificatie 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 CISO en de controller informatiebeveiliging gerapporteerd.

Configuratie management – registratie van ICT voorzieningen
Het Taakveld I&A stelt procedures op ten aanzien van het registreren en muteren van ICT voorzieningen en de daaraan gerelateerde documentatie.

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 in het geval van het beheer van DigiD-voorzieningen aan de criteria voor leveranciers van webapplicaties en webservices opgenomen in de norm ICT-beveiligingsassessments DigiD;
- In overeenstemming met informatiebeveiligingsbeleid, de BIG en algemeen gemeentelijk beleid;
- Vooraf gemeld bij ICT ten behoeve van toetsing op beheeraspecten;
- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (verwerkers)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. Werken buiten het gemeentehuis en Eigentijds Werken (ETW)

De gemeente Westland staat werken buiten het gemeentehuis toe. Hiervoor zijn beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatiebeveiligingsbeleid en voor zover niet verboden door wet en regelgeving.

Om de kaders te stellen voor het werken buiten het gemeentehuis en Eigentijds Werken wordt aanvullend beleid opgesteld. Hierin wordt minimaal aan onderstaande punten aandacht besteed:

- Afspraken tussen de procesverantwoordelijke en de medewerker 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 een thuiswerkplek (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 en Eigentijds Werken

Ten aanzien van Eigentijds Werken 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. Het werken op privéapparatuur kan alleen via een beveiligde verbinding met het netwerk van de gemeente op een virtuele werkplek. Gegevens kunnen vanuit deze virtuele werkplek niet lokaal worden opgeslagen (zero footprint).

De gemeente gaat hierbij uit van de verantwoordelijkheid van de medewerker, maar er wordt minimaal aan de onderstaande basisuitgangspunten aandacht besteed:

- Afspraken tussen de procesverantwoordelijke 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 apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk worden door de gemeente beveiligingsinstellingen via MDM afgedwongen. 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 bovenstaande beveiligingsinstellingen zijn verwijderd of aangepast is niet toegestaan;
- De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie, privacy van betrokkenen en integriteit van het gemeentelijke netwerk;
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen ook, 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 (AVG) 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 conform privacywetgeving (AVG) geen uitingen inzake klanten of vertrouwelijke 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 en bekend gemaakt aan de organisatie. 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 en beheerd.
- De procesverantwoordelijke toetst of de door het Taakveld I&A 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), tweefactor-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. Eigentijds werken en internetfaciliteiten

Uitgangspunten voor beleid ten aanzien van Eigentijds Werken en internetfaciliteiten:

- Voor Eigentijds Werken is een mobiele werkplekomgeving beschikbaar. Toegang tot het netwerk (en daarmee vertrouwelijke informatie) buiten gemeentelijke panden wordt verleend op basis van tweefactor-authenticatie;
- 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 toegestaan voor het delen van vertrouwelijke informatie;
- Toegang tot het publieke WiFi-netwerk van de gemeenten is gescheiden van het gemeentelijke bedrijfsnetwerk.

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 periodiek een uitdraai gemaakt van de verstrekte toegangsmachtigingen.
Deze uitdraai wordt gecontroleerd op juistheid en volledigheid door de controller informatiebeveiliging.

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 in de 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 tweefactor-authenticatie

Gebruik van systeemhulpmiddelen ('utilities')3
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.

18-0251091

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

Schermbeveiliging (clear screen)
Na een vaste periode van inactiviteit wordt een werkstation automatisch geblokkeerd.

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, device, netwerk, besturingssysteem, database, firewall. Voor elk van deze componenten moet apart worden geautoriseerd.

(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 op basis van het model voor dataclassificatie.

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 (Security by Design). Dit geldt ook voor cluster 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, tablets en smartphones.

Vertrouwelijkheid en onweerlegbaarheid worden beide geborgd 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 gegevensuitwisseling.

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 verwerkersovereenkomst met de gemeente meewerkt in de zin van de Algemene Verordening Gegevensbescherming;
- 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 Algemene Verordening Gegevensbescherming 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.

Voor interne systemen moeten de management functies secure zijn, alleen veilige 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 gebruikt een erkende configuratiebaseline, zoals aanbevolen door de Informatiebeveiligingsdienst voor gemeenten (IBD).

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 proceseigenaar 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 informatiebeveiligingsincident

Een informatiebeveiligingsincident 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 incidenten 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 informatiebeveiligingsincidenten

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 incident. Hiervoor gelden de volgende uitgangspunten:

- De CISO is de beheerder van de geregistreerde beveiligingsincidenten;
- Een medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de helpdesk van de gemeente;
- De beveiligingsincidenten worden bij de helpdesk als zodanig geregistreerd en vervolgens doorgegeven aan de CISO;
- 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. De CISO bekijkt periodiek een samenvatting van de informatie;
- Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt;

- Afhankelijk van de ernst van een incident is er een meldplicht bij de Functionaris Gegevensbescherming en de Autoriteit 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 cluster voert een business impactanalyse uit. Afhankelijk van de bevindingen worden per cluster vervolgacties gepland;
- Elke cluster heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfs-continuïteitsbeheer). In het continuïteitsplan worden de maatregelen beschreven waarmee de kritische bedrijfsprocessen van het cluster 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 Taakveld 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 Taakveld I&A de afgesproken regeling zal testen en met welke frequentie.

11.3. 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 informatiebeveiliging is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatiebeveiliging is een kwaliteitskenmerk van het primaire proces, waarop het management van elke cluster stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en effectiviteit van de geïmplementeerde maatregelen;
  - de mate waarin informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt;
  - de verantwoording en evaluatie over informatiebeveiliging die jaarlijks via ENSIA plaatsvindt.
- De CISO zorgt namens de Directeur Bedrijfsvoering voor het toezicht op de uitvoering van het informatiebeveiligingsbeleid;
- I&A 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 informatiebeveiligingsbeleid kunnen daarom specifieke normen gelden voor cluster en/of teams;
- Periodiek wordt de kwaliteit van informatiebeveiliging 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 informatiebeveiliging;
- Bij de jaarlijkse accountantscontrole worden ook maatregelen ten aanzien van informatiebeveiliging getoetst (bijvoorbeeld functiescheiding en autorisatie tot ICT-voorzieningen). Bevindingen en aanbevelingen hieruit worden meegenomen in de PDCA-cyclus van informatiebeveiliging;
- In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het ‘in control’ statement. Dit gebeurt via de ENSIA-verantwoording;
- 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 actieplan

Om de naleving van de beveiligingseisen uit het informatiebeveiligingsbeleid en actieplan 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, in opdracht van de procesverantwoordelijke en in opdracht van de toezichthouders vanuit het Rijk;
- Managementrapportages, tenminste eenmaal per jaar, door de concern control voor zover mogelijk ingebed in bestaande P&C-cyclus.
- Opstellen en het uitvoeren van een jaarlijkse intern controleplan voor informatiebeveiliging onder coördinatie van de CISO en onder (verbijzonderde) toezicht van de controller informatiebeveiliging.
- Opstellen van kwartaalrapportages inzake interne controles informatiebeveiliging voor het DT door de CISO in samenwerking met de controller informatiebeveiliging.

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 Algemene Verordening Gegevensbescherming duidelijke eisen. De gemeente Westland stelt een Privacy officer en Functionaris Gegevensbescherming aan, die de uitvoering en de naleving van de AVG bewaakt. De Functionaris Gegevensbescherming is voor 25 mei 2018 aangemeld bij de Autoriteit Persoonsgegevens.

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

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.

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

BiSL
Business Information Services Library is een raamwerk voor het uitvoeren van functioneel beheer en informatiemanagement.

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.

Changemanagement
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.

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

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.

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, betrouwbaarheid en vertrouwelijkheid.

Informatievoorziening
Informatiebeveiligingsbeleid Strategie van een organisatie met betrekking tot informatiebeveiliging.

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.

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.

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.

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.

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.

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.

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

Tweefactor-authenticatie
Het gebruik van meer dan een authenticatiemiddel om in te loggen in systemen of applicaties. Bijvoorbeeld de combinatie van een wachtwoord en een code die per SMS wordt verstrekt aan de gebruiker.

Utility
Zie Systeemhulpmiddel.

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden.