Gemeente Bergeijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Bergeijk

Nr. 276102

21 december 2018

Informatieveiligheidsbeleid Kempengemeenten en de Gemeenschappelijke Regeling Samenwerking Kempengemeenten 2018

Burgemeester en wethouders van Bergeijk;

Overwegende dat, het huidige Informatiebeveiligingsbeleid Kempengemeenten en de Gemeenschappelijke Regeling Samenwerking Kempen gemeenten (GRSK) geactualiseerd dient te worden;

Gelet op artikel 160 , lid 1 onder a van de Gemeentewet;

Besluit vast te stellen het:

Informatieveiligheidsbeleid Kempengemeenten en de Gemeenschappelijke Regeling Samenwerking Kempengemeenten 2018

Voorwoord

Totstandkoming

In dit document is het informatieveiligheidsbeleid beschreven van de Kempengemeenten en de Gemeenschappelijke Regeling Samenwerking Kempengemeenten (GRSK). De GRSK betreft een samenwerking tussen de gemeenten Oirschot, Bergeijk, Bladel, Reusel-De Mierden en Eersel.
De Kempengemeenten werken middels het aangaan van de gemeenschappelijke regeling samen rond de onderwerpen sociale dienst, jeugdhulp en vergunningen, alsmede de ondersteunende functies informatievoorziening en personeelszaken.
De Kempengemeenten en de GRSK hebben zich tot doel gesteld informatieveiligheid als samenwerkingsverband aan te pakken. Afgeleide doelstellingen hiervan zijn onder meer het aanbrengen van beleidsmatige eenduidigheid over informatieveiligheid, het ontlasten van de gemeenten door beveiligingswerkzaamheden waar het kan te bundelen, het beheer van informatieveiligheidsproducten te vereenvoudigen en de onderlinge samenwerking verder te versterken.
Het informatieveiligheidsbeleid is gebaseerd op de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002 uit 2005. Op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgeleverd. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd. De uitgangspunten uit deze baseline zijn integraal opgenomen in dit informatieveiligheidsbeleid. Hierdoor is een actueel en volledig naar de laatste inzichten opgesteld beleidsdocument ontstaan.
Het beleid is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en management die in het kader van werkzaamheden of een project moeten weten aan welke kwaliteitsaspecten aandacht moet worden besteed. De intentie is niet dat alle medewerkers exact weten wat er in het informatieveiligheidsbeleid staat, maar men moet wel weten dat het beleid er is, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn.
De basis van dit informatieveiligheidsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) (VNG/KING). De specifieke vertaling en inrichting voor de Kempengemeenten en de GRSK heeft plaatsgevonden in een aantal workshops met een afvaardiging van de gemeenten en de GRSK. Tijdens deze bijeenkomsten zijn de specifieke gemeentelijke inzichten en accenten opgehaald en samengebracht in dit document. Het ontwikkelproces is onder begeleiding van BMC Implementatie doorlopen.

Leeswijzer en ambitieniveau

Dit document bevat een groot aantal beleidsuitgangspunten op het gebied van de veiligheid van informatieprocessen. De gebieden waar informatieveiligheid betrekking op heeft, worden tijdens de fase van risicoanalyse geïnventariseerd en vervolgens van een prioriteit voorzien. De organisatie maakt tijdens dit proces zelf keuzes over de prioritering en fasering van de implementatie van de onderdelen van het beleidsplan.
Enkele beleidsuitgangspunten hebben betrekking op aandachtsgebieden die pas actueel worden indien de organisatie voor een dergelijke keuze of vraagstuk staan, bijvoorbeeld de inzet van Cloud technologie, gezamenlijk uitbesteden van software ontwikkeling of de aanschaf van een nieuw informatiesysteem. In dat specifieke geval hanteert de organisatie de beleidsuitgangspunten in dit document om de veiligheid van informatie bij deze keuze te vergroten.

Met dit document wordt daarnaast bepaald dat de organisatie bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document als uitgangspunt hanteert.

Waarom informatieveiligheidsbeleid?

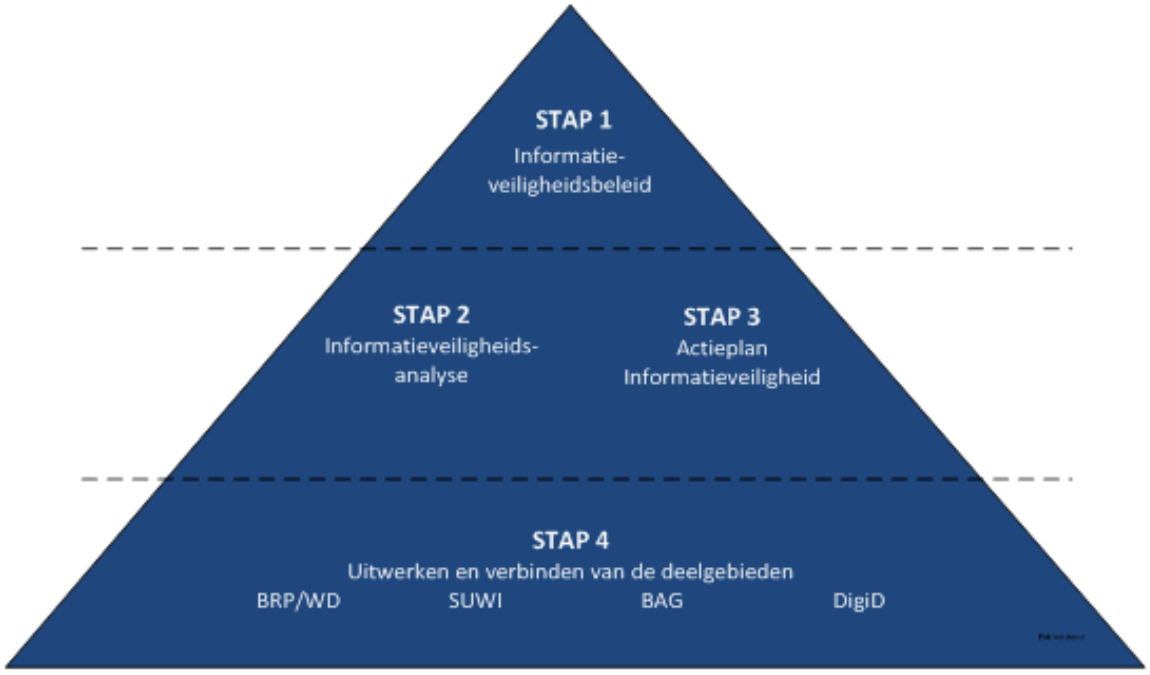
Inleiding

De Kempengemeenten en de GRSK vormen een informatie-intensief samenwerkingsverband met een primaire focus op dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de organisatie moeten kunnen beschikken over betrouwbare informatie om burgers en bedrijven optimaal te helpen en adviseren. Voor een optimale dienstverlening is een koppeling van informatiesystemen noodzakelijk. Bovendien moeten burgers en bedrijven er op kunnen vertrouwen dat hun gegevens in goede handen zijn.
Informatisering speelt een steeds prominentere rol. Deze rol wordt in het kader van het stelsel van basisregistraties en de toenemende complexiteit van het digitale dienstverleningskanaal steeds belangrijker. Ook de Kempengemeenten en de GRSK richten zich op het koppelen van systemen waardoor grote gegevensverzamelingen ontstaan die vervolgens weer specifieke informatie opleveren voor interne en externe afnemers.
Daarnaast is de organisatie steeds afhankelijker van goed werkende informatiesystemen. Dit betekent dat de Kempengemeenten en de GRSK alert zijn 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 technische middelen kan worden bereikt is begrensd en wordt al vanouds ondersteund met passende beheerprocessen en procedures. Daarnaast speelt ook de menselijke factor (het menselijk gedrag) een steeds grotere rol in het daadwerkelijk realiseren van de veiligheid van informatie. Deze factor speelt, door steeds complexer wordende informatieprocessen, veelal zelfs een doorslaggevende rol.
Informatie komt in verschillende vormen voor. Het kan zijn geschreven, gesproken, gedrukt of digitaal zijn verwerkt en-/of opgeslagen. Al deze verschijningsvormen van informatie vragen voor een deel dezelfde generieke aanpak, maar kennen ook verschillen. Dit document besteedt hier aandacht aan.
De veiligheid van informatie speelt binnen een groot aantal gebieden van de organisatie een rol. Om te voorkomen dat binnen elk van die gebieden (bijvoorbeeld rondom de SUWI, DigiD, BRP, WD, BGT, BRO of BAG) separaat beleid ontwikkeld en geïmplementeerd moet worden, is de keuze gemaakt dit brede informatieveiligheidsbeleid op te stellen. In dit brede informatieveiligheidsbeleid worden beleidsuitgangspunten vastgelegd ten aanzien van alle onderliggende informatiedomeinen. Hieronder vallen niet alleen de informatie-intensieve domeinen zoals sociaal domein, samenlevingszaken, publieksdiensten of financiën, maar eveneens domeinen als beheer en onderhoud, ruimtelijke ordening en facilitaire zaken.
Vanaf 2017 wordt gewerkt met een nieuwe verantwoordingssystematiek, de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA biedt handvatten om een optimaal verantwoording-stelsel voor informatieveiligheid, dat gestoeld is op de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) te ontwerpen. Middels ENSIA kan in één keer effectief verantwoording afgelegd worden over de volle breedte van de BIG en de verschillende vakgebieden (BRP, PUN, DigiD, BAG, BGT, BRO en SUWI).
In dit informatieveiligheidsbeleid wordt op strategisch en tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatieveiligheid van de Kempengemeenten en de GRSK. Dit document zal samen met de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie moeten opleveren waardoor de kwaliteitskenmerken van informatie, te weten: de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van informatie binnen alle domeinen van de organisatie zijn gewaarborgd.

De informatieveiligheid pyramide

Ook de centrale overheid heeft veel aandacht voor de veiligheid van informatie binnen de verschillende overheidslagen. Naast het ontwikkelen van nieuwe wet- en regelgeving op dit gebied uit zich deze aandacht ook in bewustwordingscampagnes en ondersteuning van gemeentelijke overheden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen. De ontwikkeling door KING/VNG van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) vormt hiervan een voorbeeld. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die gebaseerd zijn op de internationale standaarden voor informatieveiligheid NEN/ISO 27001 en 27002 uit 2005, bieden een meetlat om informatieveiligheid op orde te brengen en te houden.
Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden uit 2005, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) 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 de Wet Openbaarheid Bestuur (Wob).
Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo 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 nieuwe Wet Ruimtelijke Ordening (Wro) en de Archiefwet. Deze stroomlijning van de informatievoorziening vereist in steeds ruimere mate aansluiting op zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van 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 onderstaande afbeelding aangegeven welke niveaus van informatieveiligheid zijn te onderkennen.



Afbeelding de informatieveiligheid-pyramide
Bovenaan de piramide treffen we het informatieveiligheidsbeleid aan. Dit is een organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar. Het informatieveiligheidsbeleid is zodanig opgezet dat praktijksituaties eenvoudig kunnen worden opgezet of hieraan worden getoetst.
De tweede laag van de piramide is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een risico-inventarisatie en evaluatie (RI&E). Tijdens deze RI&E worden de uitgangspunten in het informatieveiligheidsbeleid getoetst met de praktijksituatie. Hier worden niet alleen de 'harde aspecten' onderzocht. Dat wil zeggen de techniek, de regels en de procedures. Maar worden ook de 'zachte aspecten' meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie. Na de risico-inventarisatie vindt risicoweging en prioritering plaats. Tijdens deze stap worden de geconstateerde risico's gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van risico's en te treffen maatregelen.
Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht zijn op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals het BRP, BAG of het financiële systeem, maar kan ook gericht zijn op IT-beheerprocessen, de inrichting van de IT-platformen of de juistheid van de crediteurenadministratie.

Toelichting op ISO 27001 en ISO 27002

Het informatieveiligheidsbeleid is volledig gebaseerd op de internationale standaard voor informatieveiligheid NEN-ISO/IEC 27001 en 27002 uit 2005. De eerste standaard (27001) biedt een richtlijn voor de implementatie en planmatige borging van Informatieveiligheid binnen de organisatie. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde 'best practices' voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. De Baseline Informatiebeveiliging Nederlandse Gemeenten (2013) is afgeleid van deze beide internationale informatieveiligheidsnormen, waarbij in de Baseline Informatiebeveiliging Nederlandse Gemeenten de methodiek en de terminologie is aangepast voor de situatie bij gemeenten.

Algemene oriëntatie en positionering

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

- Algemene beveiliging (bijv. deuren, kluizen, toegangscontrole, alarmering).
- Personeel (bijv. screening, opleiding en functietypering).
- Organisatie (bijv. functiescheiding).
- Informatisering (bijv. standaardisatie, internet en Cloud functionaliteit).
- Privacy (bijv. correct gebruik van persoonsgegevens).
- Juridische zaken (bijv. afbreukrisico's bij privacyschendingen, clausulering in overeenkomsten met derden, Third Party Mededelingen).
- Dienstverlening (bijv. website, het Nieuwe Werken, DigiD).

Het doel van informatieveiligheid is het behoud van:

- Beschikbaarheid / continuïteit (voorkomen van uitval van systemen).
- Integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig, ook tijdens en na het transport van gegevens).
- Vertrouwelijkheid / exclusiviteit (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn).
- Controleerbaarheid.

Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid

De Gemeenteraden van de Kempengemeenten zijn het hoogste bestuurlijke niveau waaraan verantwoording wordt afgelegd. De verantwoording over informatieveiligheid is per 2017 onderdeel geworden van de jaarrekening. De gemeenteraden worden conform de Eenduidige Normatiek Single Information Audit (ENSIA) jaarlijks door de colleges van burgemeester en wethouders geïnformeerd over de staat van de informatiebeveiliging.
De bestuurlijke verantwoordelijkheid voor informatieveiligheid ligt bij de colleges van burgemeester en wethouders van de gemeenten.
De verantwoordelijkheid voor informatieveiligheid over bedrijfsfuncties die zijn ondergebracht bij de gemeenschappelijke regeling ligt bij het dagelijkse bestuur van de gemeenschappelijke regeling. De vaststelling van de informatieveiligheidsorganisatie en de beleidsnormen (het informatieveiligheidsbeleid) dient door de vijf gemeenten en de GRSK afzonderlijk te worden gedaan.
De gemeentesecretarissen van de Kempengemeenten zijn verantwoordelijk voor de informatiebeveiliging binnen hun eigen organisatie. De directeur van de gemeenschappelijke regeling is dat voor de processen en systemen die in de gemeenschappelijke regeling zijn ondergebracht.
De afdelingshoofden c.q. managers van zowel de gemeenten als van de gemeenschappelijke regeling zijn verantwoordelijk voor de informatiesystemen waarvan zij eigenaar zijn. Zij dienen deze systemen te classificeren en in te richten zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

Wettelijke basis en controle beveiligingsnormen

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

- Grondwet.
- Auteurswet.
- Telecommunicatiewet.
- Ambtenarenwet.
- Wet computercriminaliteit.
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet / Archiefregeling.
- Databankenwet.
- Wet Elektronisch Bestuurlijk Verkeer.
- Wet elektronische handtekeningen.
- Wet algemene bepalingen Burgerservicenummer.
- Paspoortwet.
- Wet BasisRegistratie Personen (BRP).
- Wet Openbaarheid Bestuur (Wob).
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).
- Wet Basisregistratie Adressen en Gebouwen (BAG).
- Wet Basisregistratie Grootschalige Topografie (BGT).

- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB).
- Nieuwe Wet Ruimtelijke Ordening (nWRO).

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

Informatieveiligheidsbeleid

Doelstelling:
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid.
Resultaat:
Strategisch beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

Beleidsdocument voor informatieveiligheid

Het beleidsdocument voor informatieveiligheid wordt afzonderlijk door de vijf gemeenten en de GRSK vastgesteld. Minimaal zijn de volgende aspecten in dit beleidsdocument aanwezig:

- De doelstellingen van informatieveiligheid.
- De beveiligingseisen en prioriteiten.
- De organisatie van de informatieveiligheidsfunctie.
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatiebeveiligingsbeheerders 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.
- Een verwijzing naar een specifieke informatieveiligheidsanalyse en procedures, gedragsregels en overige relevante documentatie.
- Het benoemen van de raakvlakken met andere relevante organisatieaspecten, zoals algemeen beveiligingsbeleid, organisatiebeleid, informatiseringsbeleid, bedrijfscontinuïteit, personeelsbeleid, IT-beheer, privacybeleid, (digitale) dienstverleningsconcept en juridisch beleid.
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst middels de PDCA-cyclus.

Scope van informatieveiligheidsbeleid

De scope van dit beleid omvat alle informatieprocessen, hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. Het beleid heeft niet alleen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook informatie in fysieke c.q. analoge vorm, ongeacht de locatie, het tijdstip en gebruikte apparatuur. Daarnaast bevat dit document de uitgangspunten voor handelen ten aanzien van informatieprocessen met keten- en uitvoeringspartners.

Informatieveiligheidsanalyse

Op basis van dit strategische beleidsdocument worden de Informatieveiligheidsanalyse en het actieplan informatieveiligheid vastgesteld. Hierin wordt aangegeven op welke wijze het beleid uitgevoerd zal worden. De kernelementen in de informatieveiligheidsanalyse zijn:

- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van de informatieveiligheidsanalyse wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau.

Voor het bepalen van afhankelijkheden en risico's wordt een analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de IT-omgeving. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:

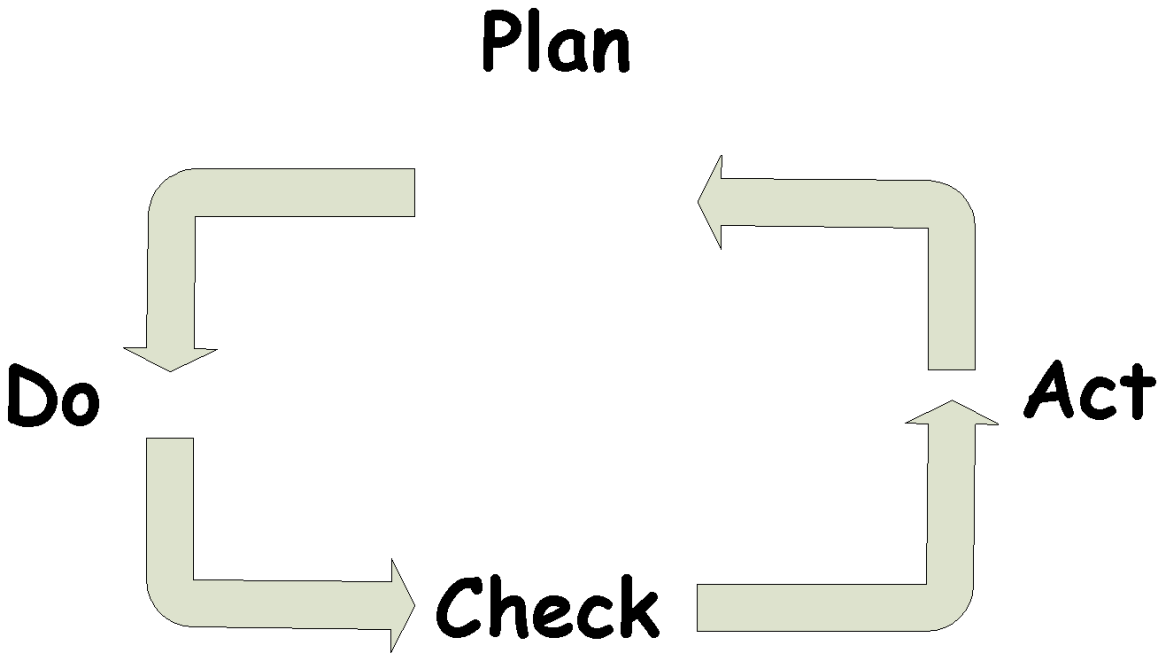
- Risico's die onvoldoende af te dekken zijn door maatregelen.
- Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen.
- Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden.
- Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfskritisch zijn. Dit overzicht kan als bijlage aan het uitvoeringsplan worden toegevoegd.

Afwijkend beveiligingsniveau
Als uit de risicoanalyse blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist, moet een daarvoor verantwoordelijke persoon aanvullende beveiligingsmaatregelen treffen. Bij minder risicovolle verwerkingen kan een lager beveiligingsniveau worden overwogen.
Persoonsgegevens

Bij de verwerking van persoonsgegevens zijn aanvullende maatregelen vereist, afhankelijk van de risicoklassen van de Algemene Verordening Gegevensbescherming (AVG).

Borging van het informatieveiligheidsbeleid
Om borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen, de Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA cyclus:

1. Informatieveiligheidsbeleid: bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 3 jaar.
2. Informatieveiligheidsanalyse: bevat de risicoanalyse (de toets aan de praktijk) op basis van informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar.
3. Actieplan Informatieveiligheid: bevat de concrete geprioriteerde acties volgend uit de informatieveiligheidsanalyse. Bijstelling (hieronder valt ook de voortgang op de realisatie van de afgesproken acties en maatregelen) van het actieplan Informatieveiligheid vindt elk jaar plaats.



Afbeelding van de Plan, Do, Check, Act (PDCA) cyclus

Organisatie van de informatiebeveiliging

Doelstelling:
Het benoemen van het eigenaarschap van bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.
Resultaat:
Verankering in de organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid.

Verantwoordelijkheden binnen de Kempengemeenten en de GRSK
Binnen de Kempengemeenten en de GRSK worden de volgende verantwoordelijkheid- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:
Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden
De colleges van burgemeester en wethouders van de gemeenten, als ook het bestuur van de GRSK, dragen als eigenaar van informatieprocessen en (informatie)systemen de bestuurlijke verantwoordelijkheid voor een passend niveau van informatieveiligheid. De colleges stellen de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.
De colleges zijn verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleren het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar

van informatie en (informatie)systemen hebben de colleges hun verantwoordelijkheden op het gebied van beveiliging gemandateerd aan de gemeentesecretarissen.

Gemandateerde verantwoordelijkheden en taken

De gemandateerde verantwoordelijkheid voor informatieveiligheid ligt op directieniveau. Bij de gemeenten zijn dat de gemeentesecretarissen en bij de gemeenschappelijke regeling is dat de directeur. Deze directies stellen met de proces- c.q. de gegevens-eigenaren (de afdelingshoofden) het gewenste niveau van informatieveiligheid vast.

De afdelingshoofden zijn verantwoordelijk voor de juiste implementatie van beveiliging in de bedrijfsprocessen en systemen. Ze wijzen voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij leidinggevenden op organisatieniveau.

De gemeentesecretarissen hebben binnen hun eigen organisatie in ieder geval de volgende verantwoordelijkheden:

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

Verantwoordelijkheden en taken op afdelingsniveau

De afdelingshoofden zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling.

De afdelingshoofden hebben in ieder geval de volgende verantwoordelijkheden:

- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn.
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen.
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- Het rapporteren, via de controller, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de organisatie in de P&C rapportages.

De coördinator informatieveiligheid

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. De coördinator informatieveiligheid heeft binnen de eigen organisatie in ieder geval de volgende verantwoordelijkheden:

- Rapporteert rechtstreeks aan de eigen directie.
- Coördineert in samenwerking met de andere gemeenten het formuleren van informatieveiligheidsbeleid.
- Stelt voor de eigen organisatie de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan.
- Coördineert in samenwerking met de andere gemeenten de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid.
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid.
- Ondersteunt de directie en de afdelingshoofden met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen.
- Is aanspreekpunt voor medewerkers van de organisatie over het onderwerp informatieveiligheid.
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Bevordert het beveiligingsbewustzijn in de organisatie.
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten.
- Rapporteert over de informatieveiligheid in de P&C managementrapportages. Hierbij bundelt de coördinator informatieveiligheid de deelbijdragen van het afdelingsmanagement.

De controller informatieveiligheid

Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie

van beveiligingsincidenten. De controller informatieveiligheid heeft in ieder geval de volgende verantwoordelijkheden:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid. De controller informatieveiligheid is hiervoor verantwoordelijk, maar organiseert dit proces waar mogelijk met de inzet van beveiligingsbeheerders. Het principe hierbij is dat de toetsing binnen een bepaald domein plaatsvindt door een beveiligingsbeheerder van een ander domein en visa versa.
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan informatieveiligheid.
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Toetsen/bewaken van het niveau van informatieveiligheid.
- Toetsing van evaluatieproces van beveiligingsincidenten.

De beveiligingsfunctionaris reisdocumenten
Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
De beveiligingsfunctionaris rijbewijzen
Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.
De autorisatiebevoegde reisdocumenten/aanvraagstations
Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumenten modules (RAAS en aanvraagstations).
De autorisatiebevoegde rijbewijzen
Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
De beveiligingsbeheerders
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de informatieveiligheid verantwoordelijkheid 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 rol benaming:

- Basis Registratie Personen
- Reisdocumenten en Nederlandse Identiteitskaarten (autorisatiebevoegde Reisdocumenten en Aanvraagstations)
- Rijbewijzen (autorisatiebevoegde Rijbewijzen)
- SUWInet (officieel Security Officer SUWI)
- Basisregistratie Adressen en Gebouwen
- Basisregistratie Grootschalige Topografie
- Basisregistratie Ondergrond
- DigiD

Ook worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de bedrijfsvoering:

- Facilitaire Zaken
- IT (zo nodig te onderverdelen in automatisering en informatisering)
- Documentaire Informatie Voorziening
- Personeel & Organisatie

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 informatieveiligheidsbeleid, 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 van het toepassen van specifieke wet- en regelgeving.
- Rapporteert aan de coördinator informatieveiligheid en de controller informatieveiligheid.

De security Officer SUWI
De Security Officer SUWI beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. Dit laatste impliceert eveneens de kwaliteitszorg, de kwaliteitsborging en de controle op de toegang en gebruik van Suwinet.
De security Officer SUWI heeft in ieder geval de volgende verantwoordelijkheden:

- Bevordert de beveiliging van Suwinet.
- Ziet er op toe dat de beveiligingsmaatregelen worden nageleefd.
- Adviseert en informeert medewerkers en management.
- Doet voorstellen tot implementatie of aanpassing van plannen op het gebied van de beveiliging van Suwinet.
- Evalueert de resultaten van verbetermaatregelen.

- De Security Officer verzorgt periodiek een rapportage met betrekking tot de beveiligingsstatus en het gebruik van Suwinet aan het hoogste management en/of het college.

Rol- en functiescheiding en autorisatie tot Suwinet

Onderdeel van een rechtmatig en veilig gebruik van Suwinet is het gescheiden beleggen van taken en verantwoordelijkheden. Hiervoor zijn de volgende functiescheidingen aangebracht:

- De gebruikers van Suwinet.
- De lijnmanager van de ISD.
- De technisch IT beheerder.
- De applicatiebeheerder Suwinet.
- Security Officer SUWI.

Technisch IT beheer zorgt voor de technische aansluiting-, werking- en beveiliging- van Suwinet. De lijnmanager is verantwoordelijk voor de aanvraag van mutaties in geval van instroom, doorstroom en uitstroom van medewerkers. Deze aanvraag wordt door de Security Officer SUWI gecontroleerd. De Security Officer SUWI gaat hierbij na of de gevraagde autorisatie overeenkomt met de uit te voeren functie/rol. Indien de aanvraag akkoord is, worden de autorisaties en toegang inclusief wachtwoorden in orde maakt.

De privacy officers

Deze rol is gericht op de uitvoering en de naleving van de privacywetgeving. Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens. De Privacy Officer heeft in ieder geval de volgende verantwoordelijkheden:

- Beheren van het register van verwerkingen van persoonsgegevens tegen de achtergrond van de kaders van de privacywetgeving en adviseert directie, sector- en afdelingshoofden bij wijzigingen in procesuitvoering en 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:

- De uitleg van de privacyvoorschriften uit de privacywetgeving.
- Coördineren van de privacy werkzaamheden.
- Coördineren, samenvoegen en beheren van de overzichten van gegevensverwerkingen.
- Verzorgen van meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP) respectievelijk Functionaris voor de gegevensbescherming (FG).
- Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling.
- Inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn.
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen.
- Advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

De functionaris voor de gegevensbescherming (FG)

De functionaris voor de gegevensbescherming (FG), ook wel Data Protection Officer (DPO) genoemd, is de interne toezichthouder op de verwerking van persoonsgegevens. De FG houdt bij alle vijf gemeenten alsmede de gemeenschappelijke regeling toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Naast deze toezichthoudende taken is de functionaris voor de gegevensbescherming verantwoordelijk voor de uitvoer van de klachtenafhandelingsprocedure betreffende het nakomen van de AVG door de gemeenten en de gemeenschappelijke regeling. Dit betekent het initiëren, doorlopen, verzorgen van interne en externe communicatie en afsluiten van de klachtenafhandelingsprocedure.

Het Shared Service C enter De Kempen

Het Shared Service Center De Kempen, waarvan systeembeheer deel uitmaakt, beheert de werkplekken, server platformen, lokale netwerken, WiFi verbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatisering hulpmiddelen. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd. Namens het shared service center De Kempen sluit de beveiligingsbeheerder IT aan bij het informatieveiligheidsoverleg.

Facilitaire zaken

Facilitaire Zaken is lokaal geregeld (elke vestiging heeft een eigen facilitair beheerder). Zij zijn verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).

Personeelszaken

Personeelszaken is met uitzondering van gemeente Bergeijk centraal geregeld bij de gemeenschappelijke regeling. Zij is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten

binnen de organisatie en speelt hiermee een belangrijke adviesrol op het gebied van organisatie en informatieprocessen.

De functioneel applicatiebeheerders

De functioneel applicatiebeheerders zijn verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.

De medewerkers

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

De gegevensbeheerders

De gegevensbeheerders zijn voor een of meerdere informatiesystemen verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

Overleg en afstemming

De voorzitter van het informatiebeveiligings-overleg regelt dat de informatieveiligheid-coördinatoren van de gemeenten 4 tot 6 maal per jaar bij elkaar komen. Bij dit overleg zijn aanwezig:

- De controllers Informatieveiligheid.
- Een vertegenwoordiging van de beveiligingsbeheerders BRP/Reisdocumenten, BAG, BGT, BRO, SUWI en DigiD.
- Een vertegenwoordiging van de beveiligingsbeheerders FZ, IT, DIV en personeelszaken.
- Functionaris Gegevensbescherming.
- Agendaleden: MT lid of specialist.
- Onderwerpen van het afstemmingsoverleg:
- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse en/of uit het actieplan Informatieveiligheid.
- Beveiligingsincidenten.
- Planning en voorbereiding van Audits, controles en zelfevaluaties.
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse.

Daarnaast vindt ook afstemming plaats tussen de coördinatoren informatieveiligheid en de functioneel applicatie- en gegevensbeheerder(s) en de procesverantwoordelijken) van (informatie)systemen.

IT crisisbeheersing

Voor interne crisisbeheersing dient een team geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Het team bestaat uit de voorzitter van het informatiebeveiligings-overleg, de coördinator IT van het Shared Service Center, de beveiligingsbeheerder IT, een lid van het MT, relevante experts en een lid van team communicatie. Op basis van de mogelijke politieke gevolgen van het incident kiest de verantwoordelijk lijnmanager er voor om al dan niet de verantwoordelijke portefeuillehouder in te lichten.

Rapporteren van beveiligingsincidenten en datalekken

De coördinator informatieveiligheid van elke gemeente wordt door de medewerkers geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en verstoringen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd. Afspraken moeten worden gemaakt over:

- Doel van de registratie.
- Inhoud van de registratie.
- Mate van detaillering.
- Wijze van handelen.
- Wijze van rapporteren.

In geval van een datalek in de zin van de AVG moet dit ook aan de eigen Privacy Officer van het organisatieonderdeel worden gemeld alsmede aan de Functionaris Gegevensbescherming (FG).
De coördinator informatieveiligheid en de controller informatieveiligheid rapporteren minimaal eenmaal per jaar aan de verantwoordelijke over informatieveiligheid. De verantwoordelijken van de gemeenten zijn de gemeentesecretarissen en voor de onderdelen van de GRSK die gedelegeerd zijn, is dat de directeur.

Verantwoordelijkheden afdeling overstijgende informatiesystemen

Afdelingsoverstijgende informatiesystemen worden onder de verantwoordelijkheid van het shared service center De Kempen gefaciliteerd en onderhouden. Deze systemen, die door meer dan één organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdelingsoverstijgend (informatie)systeem hebben de gemeentesecretarissen c.q. de directeur het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem. De procesverantwoordelijke van een afdelingsoverstijgend (informatie)systeem draagt er zorg voor

dat bij het gebruik ervan de wettelijke eisen en de voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.
De gemandateerd eigenaar maakt schriftelijk afspraken met het organisatieonderdeel of de externe organisatie dat van de afdelingsoverstijgend informatiesysteem gebruik maakt.
Minimaal worden in deze afspraken vastgelegd:

- Voorwaarden voor het toegestane gebruik van de afdelingsoverstijgend (informatie)systeem.
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit de afdelingsoverstijgend (informatie)systeem.
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens.
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatieveiligheid.
- Procedure(s) betreffende autorisatie van medewerkers.
- Procedure(s) betreffende toezicht op de naleving van de afspraken en oplossing van eventuele geschillen.
- Het recht op inzage in de resultaten van de externe audits en zelfevaluaties bij de gebruikende partij waaruit blijkt in welke mate deze aan het informatieveiligheidsbeleid voldoet.

Contracten met derden

Service Level A greement
Bij structurele / langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de informatiesystemen, netwerken, en/of werkstations of hosting van websites wordt tussen een organisatieonderdeel en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatieveiligheid en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatieveiligheid. In het uitbestedingscontract wordt verwezen naar de SLA.
Inhuur derden
Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijk leidinggevende van de organisatie. De verantwoordelijke dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.
Toegang tot IT voorzieningen
Bij toegang van derden tot IT voorzieningen gelden in principe de onderstaande uitgangspunten:

- Informatieveiligheid is (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.
- 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.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een verwerkersovereenkomst (conform Algemene Verordening Gegevensbescherming) afgesloten.
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

Overeenkomsten met derden
Bij het aangaan van overeenkomsten met derde partijen gelden de volgende beveiligingseisen:

1. De maatregelen zijn voorafgaand aan het ingaan van het contract gedefinieerd en geïmplementeerd.
2. Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
3. 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.
4. In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.
5. Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.

6. In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
7. 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.
8. 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.

Verwerkers van persoonsgegevens
De Algemene Verordening Gegevensbescherming (AVG) stelt regels voor het opslaan, verzamelen, vernietigen, verstrekken en combineren (kort gezegd: het verwerken) van persoonsgegevens. Wanneer een partij het verwerken van persoonsgegevens bij een andere partij uitbesteedt noemt men deze andere partij 'een verwerker'. De verantwoordelijke voor de persoonsgegevens legt in een register vast welke derden persoonsgegevens bewerken. Ook wordt vastgelegd of een verwerkersovereenkomst nodig is in de relatie tot die andere partij. In een verwerkersovereenkomst leggen de partijen onder andere vast voor welke doeleinden de gegevens mogen worden verwerkt, welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen, welke beveiligingsmaatregelen moeten worden genomen en hoe het zit met de onderlinge aansprakelijkheid.

Classificatie en beheer van informatie en bedrijfsmiddelen

Doelstelling:
Het bepalen, handhaven en waarborgen van het juiste beveiligingsniveau voor informatie, informatiesystemen en bedrijfsmiddelen.
Resultaat:
Een goed overzicht van alle IT-componenten en andere relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatie classificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald.

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 Shared Service Center De Kempen houdt een registratie bij van alle bedrijfsmiddelen die verband houden met informatiesystemen (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 zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de procesverantwoordelijken en beheerders zijn.
Facilitaire Zaken houdt een registratie bij van alle fysieke voorzieningen die verband houden met de veiligheid van ruimten, gebouwen en de directe omgeving van de kantoren.

Eigendom van informatie en bedrijfsmiddelen
Alle informatie en bedrijfsmiddelen die verband houden met IT voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Voor elk bedrijfsproces, applicatie, gegevensverzameling en IT faciliteit is een verantwoordelijk leidinggevende benoemd.

Aanvaardbaar gebruik van bedrijfsmiddelen
Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT voorzieningen en informatieprocessen.
Hieronder volgen de geldende uitgangspunten:
- Apparatuur en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gemandateerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.

- Medewerkers dienen bij het gebruik van IT-middelen, social media en overheidsinformatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de organisatie te waarborgen.
- Medewerkers gebruiken informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van overheidsinformatie en bestanden is niet toegestaan.

Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:

- Illegale software, of niet goedgekeurde software mag niet worden gebruikt voor de uitvoering van het werk.
- Er bestaat geen plicht de eigen computer te beveiligen, maar de informatie daarop wel.
- Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.

De medewerker neemt passende technische en organisatorische maatregelen om 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 organisatie gestelde beveiligingsvoorschriften (o.a. dit informatieveiligheidsbeleid).
- Aan de werkplek verbonden risico's.
- Het risico door het benaderen van overheidsinformatie met andere dan door de organisatie verstrekte of goedgekeurde IT-apparatuur.

Classificatie van informatie en bedrijfsmiddelen

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen worden beveiligingsclassificaties gebruikt. De informatiesystemen worden geclassificeerd op de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatie niveaus weer. Na deze classificatie is onder meer duidelijk welke specifieke informatie als vertrouwelijk wordt geclassificeerd. Na dit inzicht is duidelijk welke maatregelen per informatiesysteem nodig zijn.

Classificatietabel

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen / 0	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag / I	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden / II	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: voorwaardelijke primaire proces informatie)*
Hoog / III	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke 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)*

Tabel classificatie matrix

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.

Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten

Hieronder volgen de geldende algemene uitgangspunten:

- De leidinggevende is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen.

- De leidinggevende bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, invoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en andere regelingen.
- Regels die volgen uit dit beleid en andere regelingen gelden ook voor externen, die in opdracht van de organisatie werkzaamheden uitvoeren.

Kritische functies
De organisatie kiest voor een zorgvuldige selectieprocedure ter waarborging van een betrouwbaar personeelsbestand. Er wordt daarbij geen onderscheid gemaakt tussen 'reguliere' en 'kritische' functies. Van elke medewerker wordt verwacht dat hij of zij integer handelt.

Voorwaarden tewerkstelling vast personeel
Iedere medewerker in dienst van de organisatie, legt de eed of belofte af. Alle medewerkers worden geacht te handelen conform de 'Gedragscode Ambtelijke integriteit'. Hiertoe wordt een integriteits-/geheimhoudingsverklaring ter ondertekening voorgelegd. Daarnaast overleggen alle medewerkers eenmalig een Verklaring Omtrent Gedrag (VOG). Bij indiensttreding wijst de leidinggevende de werknemer op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP), Waardedocumenten en SUWI. De documenten zijn terug te vinden op het intranet.

Voorwaarden tewerkstelling extern personeel
Externen die tewerkgesteld worden bij de organisatie, zoals uitzendkrachten, stagiaires en ingehuurde externe personen (zoals leveranciers) die toegang hebben tot vertrouwelijke informatie tekenen een integriteits-/geheimhoudingsverklaring en worden geacht te handelen conform de voorschriften zoals vermeld in de 'Gedragscode Ambtelijke integriteit'. Ook overleggen externen een Verklaring Omtrent Gedrag (VOG). Daarnaast wijst de leidinggevende de tijdelijke werknemer op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP,) Waardedocumenten en SUWI. De documenten zijn ook hier terug te vinden op het intranet.

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

Opleiding en communicatie
Alle medewerkers (en voor zover van toepassing externe gebruikers van de systemen) worden geïnformeerd over de procedures die binnen de organisatie gelden voor informatieveiligheid. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden. Ten aanzien van communicatie en bewustwording geldt dat:
- Alle medewerkers binnen de organisatie worden ingelicht over het informatieveiligheidsbeleid en de beveiligingsprocedures van de organisatie en informatie krijgen over het correcte gebruik van de IT- en toegangsvoorzieningen. Dit geldt eventueel ook voor externe gebruikers.
- Het MT en de leidinggevenden de algehele communicatie en bewustwording rondom informatieveiligheid bevorderen.
- De leidinggevenden dragen er zorg voor dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen.
- In werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

Bijzondere situaties
In het geval van ernstige verdenkingen tegen een medewerker op het gebied van verduistering of gedrag dat in strijd is met de interne regels, is het mogelijk dat de organisatie gebruik maakt van opsporingsmogelijkheden zoals (verborgen) camera's en microfoons. Ook de door de organisatie verstrekte telefoon en automatiseringsmiddelen kunnen in deze gevallen met onder meer logfiles worden onderzocht. Voor de inzet van deze opsporingsmiddelen is schriftelijke toestemming nodig van de gemeentesecretaris of de directeur. Er dient tevens een zogeheten voorafgaand onderzoek te worden aangevraagd bij de FG of de Autoriteit Persoonsgegevens. De opsporingsmiddelen mogen pas worden ingezet wanneer de Autoriteit Persoonsgegevens naar aanleiding van het voorafgaand onderzoek toestemming heeft verleend.

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 IT-voorzieningen adequaat worden beschermd tegen ongeautoriseerde toegang, kennisneming, verminking of diefstal, waardoor schade en verstoringen worden voorkomen.

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 middels een passend toegangsmiddel daartoe.
- De uitgifte van toegangsmiddelen aan zowel interne als externe medewerkers wordt geregistreerd.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- Indien gebruik gemaakt wordt van beeldmateriaal wordt dit beperkt door de privacywet en nadere regels.
- De fysieke toegang tot ruimten waar zich informatie en IT-voorzieningen bevinden is voorbehouden aan bevoegd personeel.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.

Inventarisatie van bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen per organisatie of onderdeel worden geïnventariseerd en de waarde en het belang ervan worden onderkend. Facilitaire Zaken houdt een registratie bij van alle bedrijfsmiddelen die verband houden met veiligheid van ruimten, gebouw(en) en de directe omgeving van de gebouwen:

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

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.

Fysieke toegang tot computer en datacom ruimten

De fysieke toegang tot kritische ruimten (computer-/serverruimten) onder beheer van facilitaire zaken is voorbehouden aan de volgende categorieën personen:

- De leden van de IT afdeling die uit hoofde van functie (technische) werkzaamheden aan de centrale computers of telecom apparatuur moeten verrichten.
- De door de manager van de afdeling (waaronder IT valt) geautoriseerde personen (zoals bijvoorbeeld de Bedrijfshulpverlening).
- Personen die niet onder de genoemde categorieën vallen, mogen de kritische ruimten alleen betreden onder begeleiding van een geautoriseerde medewerker van het shared service center De Kempen.

Bewegwijzering computerruimten

Binnen de vestiging zijn geen wegwijzers aangebracht waaruit de locaties van de IT-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.

Verwijderen apparatuur en gegevensdragers

Het shared service center De Kempen heeft een procedure voor het verwijderen of gereed maken voor hergebruik van overbodige apparatuur en gegevensdragers waarop overheidsinformatie 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.

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.

Clean desk en clear screen

De organisatie heeft een clean desk policy vastgesteld voor papieren en verwijderbare opslagmedia, zodat dit soort materialen niet onbeheerd op het bureau liggen. Daarnaast is er een clear screen policy voor IT voorzieningen. Dit betekent dat alle medewerkers bij het verlaten van de werkplek het scherm locken en dat na een bepaald tijdsverloop het beeldscherm op zwart gaat en de toegang tot het werkstation wordt geblokkeerd middels een toegangscode. Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en IT voorzieningen tijdens en buiten normale werktijden te beperken.

Beveiliging van mobiele apparatuur

Informatie verwerkende mobiele apparatuur moet zowel binnen als buiten het gebouw zo goed mogelijk fysiek beschermd worden. Dit betreft laptops, tablets, memory sticks en mobiele telefoons. Voor het gebruik van deze apparatuur worden richtlijnen vastgesteld:

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

Beheer van communicatie- en bedieningsprocessen

Doelstelling:
Het garanderen van correcte en veilige bediening en beheer van de IT-voorzieningen.
Resultaat:
Maatregelen en procedures voor het beheer en de bediening van de IT-voorzieningen en het adequaat reageren op incidenten.

Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.
- In beginsel is er een scheiding tussen beheertaken en overige gebruikerstaken. Hierbij worden beheerwerkzaamheden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikerstaken alleen wanneer ingelogd als gebruiker. Er wordt echter per specifieke situatie bezien of deze scheiding een werkbare situatie oplevert en of de veiligheid hierdoor in dit specifieke geval wordt verhoogd.

Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectie definities vindt in beginsel dagelijks plaats.
- Op verschillende niveaus binnen de IT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirus software toegepast.
- Het is niet toegestaan niet-geautoriseerde (pc)programmatuur te gebruiken of te installeren op IT voorzieningen.
- Alle apparatuur die is verbonden met het netwerk moet kunnen worden geïdentificeerd.
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
- Het (ongecontroleerd) kopiëren van vertrouwelijke gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.
- Updates die ten behoeve van het verhogen van de veiligheid worden vrijgegeven door de leverancier worden zo spoedig mogelijk via de geëigende wijzigingsprocedure doorgevoerd. Dit geldt zowel voor besturingssoftware, informatiesystemen, als voor ondersteunende software

(Java, Java applets, ActiveX, Flash en Adobe) en besturingssystemen voor mobiele apparatuur en actieve componenten.
- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau (service levels) komt.
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.

Beheerprocedures en verantwoordelijkheden

De verantwoordelijkheden en procedures voor het beheer van de bediening van de IT-voorzieningen zijn beschreven en vastgesteld. Procedures zijn voor zover mogelijk in lijn gebracht met de ISO 20000-1 en ISO 20000-2 (ITIL 3).

Documentatie van beheerprocedures

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

Change management / release management – doorvoeren van vernieuwingen en wijzigingen

Het aanbrengen van wijzigingen in de informatie-infrastructuur of het installeren van nieuwe versies vindt plaats volgens een vastgestelde wijzigingsprocedure waarin de formele goedkeuring geregeld is. Dit geldt voor apparatuur, programmatuur, productiesystemen en procedures. Voornaamste aspect bij dit proces is het garanderen van de continuïteit van het productiesysteem. Uitgangspunten hierbij zijn:
- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever en IT (veelal de proceseigenaar). De test en de testresultaten worden gedocumenteerd.
- Systemen voor Test en/of Acceptatie (TA) zijn logisch gescheiden van Productie (P).
- Faciliteiten voor Testen, Acceptatie en Productie (TAP) zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
- In de TA worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk.
- Vertrouwelijke data uit de productieomgeving mag niet worden gebruikt in de ontwikkel-, test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data te vernietigen na ontwikkelen en testen.
- Het gebruik van IT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Incident management – afhandeling van incidenten in de IT infrastructuur

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

Capaciteitsmanagement – omgang met de capaciteit van IT voorzieningen

Om te waarborgen dat informatiesystemen conform de gestelde eisen van continuïteit en snelheid blijven werken stelt het Shared Service Center De Kempen verantwoordelijkheden en procedures op ten aanzien van de monitoring van de capaciteit.

Problem management – identificeren en afhandelen van fouten in de IT infrastructuur

Het shared service center De Kempen richt een organisatie in en stelt procedures op ten aanzien van het achterhalen en wegnemen van fouten in de infrastructuur.

IT service continuity management – waarborgen van de continuïteit van de IT-dienstverlening in geval van calamiteiten

Het Shared Service Center De Kempen stelt procedures op ten aanzien van voldoende technische, financiële en organisatorische voorzieningen ten behoeve van het waarborgen van de overeengekomen continuïteit van de IT-dienstverlening in geval van calamiteiten. Uitgangspunten hierbij zijn:
- In opdracht van de eigenaar van data maakt IT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur, zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens.
- De back-up wordt iedere dag buiten het gebouw opgeslagen.
- De back-up- en recovery-maatregelen worden regelmatig, doch minimaal één maal per jaar op een uitwijk center en één keer per jaar in de eigen IT-omgeving, getest.
- Over het resultaat van de test wordt aan de procesverantwoordelijken, de coördinator informatieveiligheid en de controller informatieveiligheid gerapporteerd.

Configuratie management – registratie van IT voorzieningen

Het Shared Service Center De Kempen stelt procedures op ten aanzien van het registreren en muteren van IT voorzieningen en de daaraan gerelateerde documentatie.
Information security management – omgang met de veiligheid van IT voorzieningen
De coördinator informatieveiligheid richt een organisatie in, stelt procedures op en traint personeel zodanig dat aan de eisen van het Informatieveiligheidsbeleid wordt voldaan.

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, met name ten aanzien van de wet BRP en SUWI. 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.
Ten aanzien van SUWI vraagt de Security Officer SUWI meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van SUWInet. Ten aanzien van de BRP worden logging rapportages minimaal maandelijks beoordeeld door de BRP beheerder.

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 de verantwoordelijke leidinggevende van de organisatie.
- Voldoet aan de criteria voor leveranciers van webapplicaties en webservices opgenomen in de norm ICT-beveiligingsassessments DigiD.
- In overeenstemming met informatieveiligheidsbeleid en algemeen beleid.
- Vooraf gemeld bij het shared service center De Kempen ten behoeve van toetsing op beheersaspecten.
- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de 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 informatieveiligheid.
- Er is een basiscontract voor de toegang tot de IT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin de kaders staan voor de toegang tot ICT-voorzieningen door derden.

Telewerken en thuiswerken
De organisatie staat telewerken toe (op afstand werken op het netwerk, bijvoorbeeld thuiswerken) na toestemming van de verantwoordelijke leidinggevende. Hiervoor worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het informatieveiligheidsbeleid en voor zover niet wordt verboden door wet en regelgeving. [1]
Minimaal wordt aan onderstaande punten aandacht besteed:
- Afspraken tussen de procesverantwoordelijke en "de telewerker", bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke en/of kritische informatie en/of documenten.
- Richtlijnen voor identificatie en authenticatie.
- Richtlijnen voor wachtwoordgebruik.
- Richtlijnen voor de technische inrichting van de telewerkplek (firewall, virusscanner).
- Afspraken omtrent de telewerkplek (ARBO normen).

- Het inloggen met bijzondere systeembeheer bevoegdheden (administrator en root) via de telewerkplek is niet toegestaan tenzij er aanvullende maatregelen zijn getroffen.

Mobiele apparatuur

Ten aanzien van 'Bring Your Own Device/ Choose Your Own Device'' (BYOD/CYOD) wordt beleid opgesteld en worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het informatieveiligheidsbeleid en voor zover niet wordt verboden door wet- en regelgeving.[2] Minimaal wordt aan onderstaande punten 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 organisatie verstrekte middelen als op privé-apparatuur.
- Op privé-apparatuur waarmee verbinding wordt gemaakt met het netwerk is de organisatie bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, anti virus programmatuur en de instellingen van deze programmatuur, etc.
- Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
- Op verzoek van de organisatie dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software').
- De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van overheidsinformatie en integriteit van het netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden.

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

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

Gebruik van internet en email

De organisatie 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.

Social media

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

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

Informatie uitwisseling over netwerken

Buiten onderstaande uitgangspunten worden beleid, formele procedures en formele beheersmaatregelen vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

- Het meenemen van vertrouwelijke of hogere geclassificeerde informatie vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is en uitsluitend indien maatregelen zijn getroffen die afgestemd zijn op de risico's en wetgeving (onder andere AVG, BRP en SUWI).
- Medewerkers zijn geïnstrueerd om zodanig om te gaan met gesprekken, e-mail, faxen, ingesproken berichten op antwoordapparaten en het gebruik van de diverse digitale berichtendiensten dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.
- Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt ten minste aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.

- Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer en dergelijke te laten liggen.

Er dienen maatregelen te zijn om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.

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.

Beveiligingseisen voor (informatie)systemen

Bij de ontwikkeling van (informatie)systemen moeten beveiligingseisen vanaf aanvang in het ontwerpproces worden meegenomen. Dit geldt ook voor afdeling overstijgende (informatie)systemen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Bij het onderhoud van (informatie)systemen moet informatieveiligheid 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 audit trails 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.

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.
PKI-certificaten worden herkend in veel standaard toepassingen, 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 authentiseren 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 beheerrollen en de recovery mogelijkheden. Een sleutelbeheersysteem moet er minimaal voor zorgen dat sleutels niet onversleuteld op de servers te vinden zijn.

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.

Uitbesteding ontwikkeling van (informatie)systemen

In deze situatie ontwikkelt de organisatie niet zelf een (informatie) systeem, maar besteedt het ontwikkel- en productiewerk uit. De organisatie 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 organisatie.
- Licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten.
- Beoordeling en controle van de kwaliteit en nauwkeurigheid van het uitgevoerde werk.
- Privacygevoeligheid en bedrijfs vertrouwelijkheid van testgegevens, bijvoorbeeld door het gebruik van anonieme of fictieve gegevens en ingeval door de leverancier persoonsgegevens worden bewerkt of deze meewerkt aan de totstandkoming van een bewerkersovereenkomst.
- Mogelijkheid tot uitvoeren van IT audits bij de leverancier op de interne beheersingsmaatregelen of bij de door de leverancier ingeschakelde derden.
- 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.
- 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, responstijden, 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 beveiliging inzichten, beveiligingsnormen en –richtlijnen.
- Of ingeval van een webapplicatie tenminste jaarlijks penetratietesten worden uitgevoerd waarbij uitgangspunt is dat de leverancier de organisatie in staat stelt om aan haar verplichtingen als verantwoordelijke, voortvloeiend uit de aan de DigiD gekoppelde wet- en regelgeving, en de Algemene Verordening Gegevensbescherming (AVG) te voldoen.

Hardening van systemen

De hardening van alle systemen maar met name de internet facing systemen dient strak te zijn geregeld. Voor de webapplicaties en systemen geldt: alles dat open staat moet een reden hebben en alles dat open staat moet secure worden aangeboden.
De hardening van interne systemen mag minder stringent. Voor interne systemen moeten de managementfuncties secure zijn, er geen onveilige protocollen worden gebruikt, de default wachtwoorden zijn gewijzigd, en ongebruikte applicaties worden verwijderd.
Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaard (default) installatie proces. Alle componenten van de IT-infrastructuur moeten deel uitmaken van het hardingsproces.
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.

Hardening van websites

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

Beveiligingsincidenten

Doelstelling:
Bewerkstelligen dat informatieveiligheid gebeurtenissen 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.

Definitie beveiligingsincident

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen. Hierbij staat beschikbaarheid voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie op de afgesproken momenten. Integriteit staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).
Voorbeelden van beveiligingsincidenten zijn: besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), niet beschikbaar zijn van de website met dienstverlening portaal, verlies van usb-stick met gevoelige informatie, diefstal van data of hardware of een gecompromitteerde mailbox.

Procedure melding en omgang beveiligingsincidenten

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

- De coördinator informatieveiligheid is de beheerder van de registratie van beveiligingsincidenten.
- Een medewerker meldt geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten bij de eindverantwoordelijke.
- Beveiligingsincidenten die worden gemeld, worden als zodanig geregistreerd en eveneens doorgegeven aan de coördinator informatieveiligheid.
- Vermissing of diefstal van apparatuur of media die gegevens van de organisatie kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
- Informatie over de beveiliging relevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De coördinator informatieveiligheid bekijkt periodiek een samenvatting van de informatie.
- Afhankelijk van de ernst van een incident is er ook een meldplicht bij de FG of de Autoriteit Persoonsgegevens (AP).
- Indien is aangesloten op de Informatieveiligheidsdienst (IBD) wordt er eveneens een procedure voor communicatie naar de Informatieveiligheidsdienst opgesteld.
- De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

Onderdeel van deze procedure of naast deze veiligheidsincidenten procedure stelt de organisatie een procedure vast voor het melden van datalekken inclusief een beslisboom inzake de meldplicht en zorgt de organisatie dat deze bekend is gemaakt. Van Algemene Verordening Gegevensbescherming (AVG) is er sprake van een datalek als de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Hier kan het ook gaan over een hack, diefstal van een laptop, een verkeerd geadresseerd mailbericht, etc. Ook indien er wel sprake is van een voldoende beveiligingsniveau kan er dus sprake zijn van een meldplicht datalek.
Beveiligingsincidenten worden afgehandeld conform onderstaand incidenten-classificatieschema.

Alarmfase	Kenmerk	Impact	Opschaling	Bijzonderheden
1	Lokaal incident bij één afdeling van een Kempengemeente.	Oplosbaar probleem: bronbestrijding.	Probleem wordt opgelost door GRSK of gemeente.Geen verdere opschaling.	Melding van incident bij de coördinator informatiebeveiliging Kempengemeenten.
2	Incident bij meerdere afdelingen binnen een Kempengemeente.	Geïsoleerd probleem: bron - en effectbestrijding.	Probleem wordt opgelost door GRSK. Geen verdere opschaling.	Melding aan coördinator informatiebeveiliging. Gemeentelijke communicatie omtrent het incident en de opvolging door GRSK door coördinator informatiebeveiliging optioneel. Melding

				bij IBD door coördinator informatiebeveiliging GRSK indien nodig.
3	Concern breed incident en mogelijk andere gemeenten binnen de GRSK.	Impact op de gemeentelijke dienstverlening wordt echt ervaren.	Kernteam GRSK komt bij elkaar. Afhankelijk van het incident (impact) treedt de GRIP structuur in werking. Bestuur Kempengemeenten en kernteamleden, GRSK worden geïnformeerd.	Melding aan coördinator informatiebeveiliging. Gemeentelijke communicatie omtrent het incident en de opvolging door GRSK door coördinator informatiebeveiliging optioneel. Melding bij IBD door coördinator informatiebeveiliging GRSK indien nodig. Melding bij IBD door coördinator informatiebeveiliging SSC indien nodig.
4	Incident is GRSK overstijgend (landelijk).	Impact op de gemeentelijke dienstverlening is manifest.	Mogelijk treedt de GRIP structuur in werking. Het kernteam GRSK is dan in beginsel adviserend en voert desgewenst coördinatie (binnen het ICT domein).	Er is sprake van landelijke opschaling via de technische lijn (IBD - NCSC) of via de maatschappelijke lijn (NCC).

Tabel incidenten-classificatieschema

Continuïteitsbeheer

Doelstelling:
Het voorkomen van onderbreking van activiteiten van de IT-infrastructuur en het beschermen van de kritische bedrijfsprocessen tegen de effecten van ingrijpende storingen of calamiteiten.
Resultaat:
Een beheerproces 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.

Proces van continuïteitsmanagement

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

- Elk organisatieonderdeel voert een business impact analyse uit. Afhankelijk van de bevindingen worden per onderdeel vervolgacties gepland.
- Elk organisatieonderdeel stelt een plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer) op. In het continuïteitsplan worden de maatregelen beschreven waarmee de essentiële bedrijfsprocessen van een afdeling na een onderbreking of verstoring voortgezet of tijdig hersteld kunnen worden. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - De risico's van bedreigingen worden beoordeeld naar de waarschijnlijkheid dat zij zich voordoen, de eventuele schade als gevolg daarvan en het herstel.
  - Identificatie van essentiële procedures voor bedrijfscontinuïteit.
  - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan.
  - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
  - Prioriteiten en volgorde van herstel en reconstructie.
  - Documentatie van systemen en processen m.b.t de noodprocedures.
  - Kennis en kundigheid van personeel om de processen weer op te starten.
  - Wijze en frequentie van testen van het plan.

Indien interne of externe uitwijk is gerealiseerd, wordt minimaal jaarlijks een uitwijktest uitgevoerd. De uitwijkprocedures zijn ondergebracht in het draaiboek uitwijk.

Relatie met nood- en ontruimingsplan

De gemeenten zorgen 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.

Veiligstelling programmatuur

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

Monitoring capaciteit
Voor alle relevante IT-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. Performance problemen worden tijdig gesignaleerd en geanalyseerd op basis van betrouwbare gegevens.

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

Organisatorische uitgangspunten
- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - De mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid.
  - Efficiency en effectiviteit van de geïmplementeerde maatregelen.
  - De mate waarin de informatieveiligheid het bereiken van de strategische doelstellingen ondersteunt.

- De coördinator informatieveiligheid coördineert namens de gemeenten de uitvoering van het informatieveiligheidsbeleid.
- Het Shared Service Center De Kempen en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatieveiligheidsbeleid. 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, BRP en waardedocumenten. Aanvullend op dit informatieveiligheidsbeleid kunnen daarom specifieke normen gelden.
- ENSIA beoogt de ontwikkeling en implementatie van een optimaal ingerichte verantwoordingssystematiek voor informatieveiligheid, gestoeld op de BIG (Baseline Informatieveiligheid Gemeenten).
- Periodiek wordt de kwaliteit van informatieveiligheid onderzocht. Bijvoorbeeld door eigen auditors, onafhankelijke externen, audits, onderzoeken of zelfevaluaties. Jaarlijks worden meerdere audits/onderzoeken/zelfevaluaties uitgevoerd. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het ‘in control’ statement.
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

Naleving van informatieveiligheidsbeleid en -plan
Om de naleving van de beveiligingseisen uit het informatieveiligheidsbeleid en -plan te bewaken, legt de procesverantwoordelijke adequate organisatorische en procedurele afspraken vast. Kernelementen in het controle- en evaluatieproces zijn:
- Zelfevaluatie en/of een audit, tenminste eenmaal per jaar, door de procesverantwoordelijke.
- Managementrapportages, tenminste eenmaal per jaar, getoetst door de controller informatieveiligheid op inhoud en vorm en ingebed in bestaande P&C -cyclus.

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). Conform de Archiefwet[3] beschikt de organisatie over een systeem 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 (AVG) duidelijke eisen. De organisatie stelt een Privacy Officer en een Functionaris Gegevensbescherming (FG) aan, die de uitvoering en de naleving van de AVG bewaken.

[3]De wettelijke plicht voor een gemeentelijk documentair structuurplan (DSP) is afgeschaft, maar het blijft verplicht om als organisatie de archiefbescheiden (document-, proces- of zaakgericht) te ordenen.

Beoordeling van de naleving

De procesverantwoordelijke leidinggevenden zorgen voor de controle en evaluatie op de naleving van wettelijke voorschriften van het informatieveiligheidsbeleid. 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) of door middel van zelfevaluaties.

Begrippenlijst

Afdelingsoverstijgend informatiesysteem (AIS)
Systeem dat door meer dan één afdeling wordt gebruikt en waarin gegevens van meerdere organisatieonderdelen worden vastgelegd
Audit (informatieveiligheids-)
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
Bedrij fskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen
Beschikbaarheid
Zie Continuïteit
Beveiligingsincident
Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten
Calamiteit
Gebeurtenis die een zodanige verstoring van de geautomatiseerde gegevensverwerking tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen
Change management
Beheer en beheersing van alle wijzigingen van componenten van (informatie)systemen en de IT-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
Compliance
Het begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving.
Configuratie management
Beheer en beheersing van de samenstelling en de status van de ICT infrastructuur en de (informatie)systemen die er gebruik van maken
Configuratieschema
Overzicht van de onderdelen waaruit een (informatie)systeem is opgebouwd
Continuïteit (bedrijfs-)
De mate waarin bedrijfsprocessen ongestoord doorgang kunnen hebben
Continuïteitsmanagement

Stelsel van samenhangende activiteiten, mensen en middelen met als doel de continuïteit van de (kritische) bedrijfsprocessen te waarborgen
Database
Een bestand waarin gedigitaliseerde gegevens op een gestructureerde manier zijn opgeslagen en bevraagd kunnen worden
Eigenaar
De eigenaar van een proces of een systeem is vanuit het informatieveiligheidsbeleid verantwoordelijk voor het stellen van eisen en de inrichting van de controle hierop, zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen.
ENSIA
ENSIA is een verantwoordingssystematiek voor informatieveiligheid, gestoeld op de BIG (Baseline Informatieveiligheid Gemeenten). Dit systematiek biedt de mogelijkheid in één keer effectief verantwoording af te leggen over de volle breedte van de BIG (BRP, PUN, DigiD, BAG, BGT en SUWI) doordat het niet alleen aansluit maar ook verbindt.
Escrow
Specifiek in de softwaresector wordt escrow aangewend ter vrijwaring van de belangen van de software klant 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 bijbehorende documentatie) in bewaring geven bij de escrow agent, 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
Hardening
Het proces van het beveiligen van een systeem en het verminderen van kwetsbaarheden door middel van het reduceren van bijvoorbeeld (onbenodigde) software, functies, gebruikersnamen, logins of diensten. (Deze zouden namelijk toegang tot het systeem kunnen genereren via achterdeurtjes).
Informatie- en communicatietechnologie (IT)
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.
IT-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
Informatieveiligheid
Samenhangend stelsel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.
Informatieveiligheidsbeleid
Strategie van een organisatie met betrekking tot informatieveiligheid.
Informatieveiligheidscontroller
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid en de escalatie van beveiligingsincidenten.
Coördinator informatieveiligheid

Medewerker die organisatiebreed adviseert over informatieveiligheidsvraagstukken in brede zin en activiteiten op het gebied van informatieveiligheid coördineert
Informatiesysteem
Een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen
Informatieveiligheidsanalyse
Document waarin beschreven staat welke beveiligingsmaatregelen getroffen worden/zijn op basis van het informatieveiligheidsbeleid
Informatievoorziening
Het geheel aan processen, bestaande uit het verzamelen, het opslaan, het verwerken van gegevens en het beschikbaar stellen ervan
Information Technology Infrastructure Library (ITIL)
Een referentiekader voor het inrichten van de beheerprocessen binnen een IT-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, instelling gebonden netwerk
Maatwerkprogrammatuur
Op specifiek (deel)proces toegesneden programmatuur
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 IT. Dit geeft een pad aan dat wordt doorlopen tijdens onder andere software ontwikkeling 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 certificaat bezitter klopt ("je bent wie je zegt dat je bent") en dat gegevens veilig kunnen worden uitgewisseld.
Privacy-beheerder
Medewerker die adviseert over privacybescherming en activiteiten ter bescherming van persoonsgegevens en privacy coördineert
Proces
Een samenhangende serie activiteiten ten behoeve van een van tevoren bepaald doel
Procesverantwoordelijkheid / procesverantwoordelijke
Verantwoordelijkheid / verantwoordelijke voor het geheel van activiteiten van een bepaald proces
Recovery
Herstel van een computerbestand of programmatuur
Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen
Routering
Het bepalen van de weg die berichten volgen Security scan Gericht onderzoek naar de mate van implementatie van beveiligingsmaatregelen
Service Level Agreement (SLA)

Schriftelijke overeenkomst tussen een aanbieder (service provider) en een afnemer (klant) van bepaalde diensten
Smartphone
Programmeerbare telefoon die voor vele uiteenlopende doeleinden gebruikt kan worden, zoals internet
SNMP
Simple Network Management Protocol: een protocol voor netwerk management en beheer
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 IT-infrastructuur
Systeemklok
Interne klok in een computersysteem
Systeem privilege
Recht op het gebruik van of toegang tot (een onderdeel van) een (informatie)systeem
Systeemprogrammatuur
Fundamentele, ondersteunende programmatuur die behoort tot de technische infrastructuur van een (informatie)systeem
Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding
Third Party Mededeling (TPM)
Verklaring van een onafhankelijke derde partij die door betrokken partijen vertrouwd wordt
Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden

Bijlage rollen informatieveiligheidsorganisatie
Zie document Bijlage IBB-rollen-gemeente-Bergeijk

Aldus vastgesteld op 13 november 2018,
Het college van de gemeente Bergeijk,
W.A.C.M. Wouters
Secretaris
A. Callewaert – de Groot
Burgemeester

Bijlage 1 Rollen, namen (vervangen door X) informatieveiligheidsorganisatie

Rol	Naam	Vervanger
Gemeentesecretaris	X	X
Coördinator informatieveiligheid	X	X
Controller informatieveiligheid	X	X
Beveiligingsbeheerder BRP	X	X
Beveiligingsfunctionaris reisdocumenten en rijbewijzen	X	X
Beveiligingsbeheerder DigiD	X	X
Beveiligingsbeheerder FZ	X	X
Beveiligingsbeheerder DIV	X	X
Beveiligingsbeheerder P&O	X	X
Contactpersoon IT	X	X
Contactpersoon ISD	X	X
Contactpersoon CJG	X	X
Beveiligingsbeheerder Vergunningen, toezicht, handhaving	X	X
Beveiligingsbeheerder BAG	X	X
Beveiligingsbeheerder BGT	X	X
Beveiligingsbeheerder BRO	X	X
Functionaris Gegevensbescherming	X	X
Privacy officer	X	X

Overige rollen

Rol	Naam	Vervanger
Contactpersoon IT	X	X
Contactpersoon ISD	X	X
Contactpersoon CJG	X	X
IBD Vertrouwde Contactpersoon Informatiebeveiliging	X	X