GEMEENTE BEVERWIJK

GEMEENTEBLAD

Officiële uitgave van de gemeente Beverwijk

Nr. 23137

5 februari

2018

Informatiebeveiligingsbeleid 2018

Burgemeester en wethouders van Beverwijk;
Overwegende dat, het huidige Strategisch Informatiebeveiligingsbeleid 2014 geactualiseerd dient te worden;
dat ten opzichte van huidige beleid het thans in concept voorliggende Informatiebeleid 2018 volledig gebaseerd is op de Baseline Informatiebeveiliging Gemeenten;
Gelet op artikel 160 , lid 1 onder a van de Gemeentewet;
besluiten:
a. Het informatiebeveiligingsbeleid vast te stellen overeenkomstig het concept Informatiebeveiligingsbeleid 2018 (INT-17-38955) onder intrekking van het Strategisch Informatiebeveiligingsbeleid 2014 (INT-13-07444).
b. Dit besluit treedt in werking op de dag na bekendmaking.

Beverwijk,
burgemeester en wethouders voornoemd,
de gemeentesecretaris, de burgemeester,
mw. mr. A.L. Schölvinck drs. M.E. Smit

Informatiebeveiligingsbeleid 2018
Beleidsuitgangspunten, beheersmaatregelen en richtlijnen inzake de informatiebeveiliging van de gemeente Beverwijk

gemeente
beverwijk

Telefoon: (0251) 256 256
Postadres: Postbus 450, 1940AL Beverwijk
E-mail: info@beverwijk.nl

Inhoudsopgave

Totstandkoming 6
Leeswijzer en ambitieniveau 7
Hoofdstuk 1: Waarom informatiebeveiliging? 8
1.1 Inleiding 8
1.2 De informatiebeveiligingspiramide 9
1.3 Toelichting op ISO 27001 en ISO 27002 11
1.4 Algemene oriëntatie en positionering 11
1.5 Verantwoordelijkheid en bevoegdheid informatiebeveiligingsbeleid 12
1.6 Wettelijke basis en controle beveiligingsnormen 13
1.7 Opbouw hoofdstukken 13
Hoofdstuk 2: Informatiebeveiligingsbeleid en -plan (BIG hoofdstuk 5). 15
2.1 Beleidsdocument voor informatiebeveiliging 15
2.2 Scope van het informatiebeveiligingsbeleid 16
2.3 Borging van het informatiebeveiligingsbeleid 16
Hoofdstuk 3: Organisatie van de informatiebeveiliging (BIG hoofdstuk 6). 18
3.1 Verantwoordelijkheidsniveaus binnen de organisatie 18
3.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau 18

3.1.2 Gemandateerde verantwoordelijkheden en taken op organisatieniveau 18
3.1.3 Verantwoordelijkheden en taken op afdelings- en teamniveau 19
3.1.4 Verantwoordelijke Informatiebeveiliging 19
3.1.5 Controleur Informatiebeveiliging 19
3.1.6 Het team Informatieregie 19
3.1.7 Het team Services 19
3.1.8 Het team Advies 20
3.1.9 De beveiligingsbeheerder 20
3.1.10 Security Officer SUWI 20
3.1.12 Functionaris voor de gegevensbescherming 21
3.1.13 Functioneel applicatiebeheerder 21
3.1.14 De medewerkers 21
3.1.15 Gegevensbeheerder 21
3.2 Toewijzing verantwoordelijkheden voor informatiebeveiliging 21
3.3 Overleg- en afstemmingsorganen 24
3.4 ICT-crisisbeheersing 24
3.5 Rapporteren beveiligingsincidenten 25
3.6 Verantwoordelijkheden afdelingsoverstijgende (informatie)systemen 25
3.7 Contracten met derden 26
3.7.1 Service Level Agreement (niveau van dienstverlening) 26
3.7.2 Inhuur derden 26
3.7.3 Toegang 27
3.7.4 Grote projecten 27
Hoofdstuk 4: Classificatie en beheer van informatie en bedrijfsmiddelen (BIG hoofdstuk 7). 28
4.1 Inventarisatie van informatie en (informatieve) bedrijfsmiddelen 28
4.2 Eigendom van informatie en bedrijfsmiddelen 29
4.3 Aanvaardbaar gebruik van bedrijfsmiddelen 29
4.4 Classificatie van informatie en bedrijfsmiddelen 30
Hoofdstuk 5: Beveiligingsaspecten ten aanzien van personeel (BIG hoofdstuk 8). 32
5.1 Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten 32
5.2 Voorwaarden tewerkstelling vast personeel in loondienst 32
5.3 Voorwaarden tewerkstelling externen 33
5.4 Kwetsbare functies 33
5.5 Toegang en bevoegdheden personeel 33
5.6 Opleiding en communicatie 34
5.7 Bijzondere situaties 34
Hoofdstuk 6: Fysieke beveiliging (BIG hoofdstuk 9). 35
6.1 Algemene uitgangspunten 35
6.2 Inventarisatie van bedrijfsmiddelen 35
6.3 Servicetaken 36
6.4 Fysieke toegang computer- en datacommunicatieruimten 36
6.5 Bewegwijzering computerruimten 36
6.6 Verwijderen apparatuur en gegevensdragers 37
6.7 Datakluizen en reserve apparatuur 37
6.8 Clear-desk-beleid en clear-screen-beleid 37
6.9 Beveiliging van (mobiele) apparatuur 37
Hoofdstuk 7: Beheer van communicatie- en bedieningsprocessen (BIG hoofdstuk 10). 39
7.1 Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen 39
7.2 Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen 39
7.3 Beheerprocedures en verantwoordelijkheden 40
7.4 Uitgangspunten voor controle en logging 43
7.5 Beheer van de dienstverlening door een derde partij 43
7.6 Telewerken en thuiswerken 44
7.7 Mobiele (privé) apparatuur 45
7.8 Gebruik internet en e-mail 46
7.9 Social media 46
7.10 Uitwisseling van informatie over netwerken 46
Hoofdstuk 8: Logische toegangsbeveiliging (BIG hoofdstuk 11). 48
8.1 Beleid voor logische toegangsbeveiliging 48
8.2 Beheer van toegangsrechten 49
8.3 Externe toegang 49
8.4 Mobiel werken, thuiswerken en internetfaciliteiten 49
8.5 Controle op toegangsrechten 50
8.6 Toegangsbeveiliging met betrekking tot netwerkdomeinen en componenten 50
8.7 Toegangsbeveiliging met betrekking tot werkstations 52
8.8 Toegangsbeveiliging met betrekking tot (informatie)systemen 53

Hoofdstuk 9: Verwerving, ontwikkeling en onderhoud van systemen (BIG hoofdstuk 8). 54
9.1 Beveiligingseisen voor (informatie)systemen 54
9.2 Cryptografische beveiliging 55
9.3 Digitale handtekening 56
9.4 Uitbesteding ontwikkeling van (informatie)systemen 56
9.5 Hardening van systemen 58
9.6 Hardening van websites 58
Hoofdstuk 10: Beveiligingsincidenten (BIG hoofdstuk 13). 60
10.1 Definitie beveiligingsincident 60
10.2 Melding en omgang beveiligingsincidenten 60
Hoofdstuk 11: Continuïteitsbeheer (BIG hoofdstuk 14). 62
11.1 Proces van continuïteitsmanagement 62
11.2 Relatie met nood- en ontruimingsplan 62
11.3 Veiligstelling programmatuur 63
11.4 Monitoring capaciteit 63
Hoofdstuk 12: Naleving (BIG hoofdstuk 14). 64
12.1 Organisatorische uitgangspunten 64
12.2 Naleving van informatiebeveiligingsbeleid en -plan 65
12.3 Naleving van wettelijke voorschriften 65
12.4 Beoordeling van de naleving 66
Begrippenlijst 67
Rollen en namen informatiebeveiligingsorganisatie 75

Totstandkoming
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » Voorwoord
In dit document wordt het gemeentebreed informatiebeveiligingsbeleid van de Gemeente Beverwijk beschreven.
Het informatiebeveiligingsbeleid is gebaseerd op de internationale standaarden voor informatiebeveiliging: NEN/ISO 27001 en NEN/ISO 27002. Voornamelijk op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgesteld. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd. De uitgangspunten uit de baseline zijn integraal opgenomen in dit gemeentebrede informatiebeveiligingsbeleid, evenals de beleidsrichtlijnen van de andere wettelijke verplichtingen op het gebied van informatiebeveiliging. Hierdoor is een actueel en volledig beleidsplan voor de Gemeente Beverwijk ontstaan, opgesteld naar aanleiding van de meest recente inzichten.
Het beleid is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en het management, die in het kader van werkzaamheden of projecten moeten weten aan welke kwaliteitsaspecten op het gebied van informatieveiligheid, aandacht moet worden besteed. De intentie is niet dat alle medewerkers exact weten wat er in het gemeentebreed informatiebeveiligingsbeleid staat, maar men moet wel weten dat het beleid bestaat, hoe dit dient te worden toegepast en wat de belangrijkste beleidsuitgangspunten zijn.
De basis van dit informatiebeveiligingsbeleid wordt gevormd door de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING).

Leeswijzer en ambitieniveau
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » Voorwoord
Dit document bevat een groot aantal doelstellingen op het gebied van de veiligheid van gemeentelijke informatieprocessen.
De gebieden waar informatieveiligheid betrekking op heeft, worden tijdens de fase van de risicoanalyse geïnventariseerd en vervolgens van een prioriteit voorzien. De gemeente maakt tijdens dit proces zelf keuzes over de prioritering en fasering van de implementatie van onderdelen van het beleidsplan.
Enkele beleidsuitgangspunten hebben betrekking op aandachtsgebieden die pas actueel worden op het moment dat de gemeente voor een dergelijke keuze of gelijksoortig vraagstuk staat, bijvoorbeeld bij het al dan niet inzetten van cloud computing, gezamenlijke uitbesteding van software ontwikkeling of bij de aanschaf van een nieuw informatiesysteem. In deze specifieke gevallen hanteert de gemeente de beleidsuitgangspunten uit dit document, om de veiligheid van informatie bij deze keuze te vergroten.
Met de opstelling van dit document is bepaald dat de gemeente bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen, de beleidsregels uit dit document als uitgangspunt hanteert.

Hoofdstuk 1: Waarom informatiebeveiliging?

1.1 Inleiding

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?

De Gemeente Beverwijk is een informatie-intensieve organisatie, primair gefocust op dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeente moeten kunnen beschikken over betrouwbare informatie om de klanten zo optimaal mogelijk te kunnen helpen en adviseren. Voor de totstandbrenging van een optimale en moderne dienstverlening is koppeling van verschillende informatiesystemen noodzakelijk. Bovendien moeten burgers en bedrijven erop kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

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

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

Informatie komt in verschillende vormen voor. Deze kan geschreven, gesproken, gedrukt, digitaal verwerkt of opgeslagen zijn. Al deze verschijningsvormen van informatie vragen voor een deel om eenzelfde generieke aanpak, maar kennen ook onderlinge verschillen waarmee rekening moet worden gehouden. Dit document besteedt hier aandacht aan.

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

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

1.2 De informatiebeveiligingspiramide

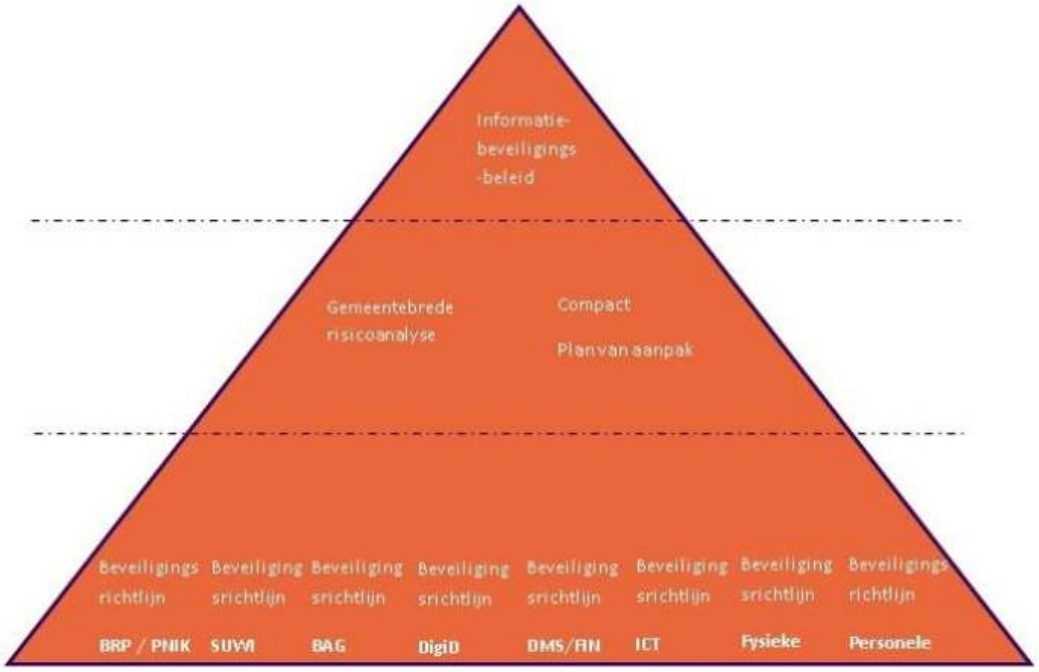
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?

De centrale overheid besteedt veel aandacht aan 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 is hier een voorbeeld van. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die gebaseerd zijn op de internationale standaarden voor informatiebeveiliging NEN/ISO 27001 en 27002, bieden een meetlat voor gemeenten om hun informatiebeveiliging op orde te brengen en te houden.

Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (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), Wet bescherming persoonsgegevens (WBP), Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en Wet openbaarheid bestuur (Wob).

Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo (aanvullingen op) wettelijke kaders met betrekking tot overige authentieke registraties, zoals de Wet basisregistratie adressen en gebouwen (BAG), Wet kenbaarheid publiekrechtelijke beperkingen (Wkpb), de nieuwe Wet ruimtelijke ordening (Wro) en de Archiefwet. Deze stroomlijning van informatievoorziening vereist in steeds ruimere mate aansluiting op de zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van de informatieprocessen biedt een helder motief voor overheden om hun aandacht nog meer te richten op de beveiliging van overheidsinformatie.

Teneinde de scope van dit document te verduidelijken, is in figuur 1 aangegeven welke niveaus van informatiebeveiliging zijn te onderkennen.



Bovenaan de piramide treffen we het informatiebeveiligingsbeleid aan. Dit is een organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar. Het informatiebeveiligingsbeleid is zodanig opgezet dat praktijksituaties eenvoudig kunnen worden opgezet of hieraan kunnen 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 uit het gemeentebrede informatiebeveiligingsbeleid getoetst aan de praktijksituatie. Hierin worden niet alleen de 'harde aspecten' onderzocht, oftewel de techniek, de regels en de procedures, maar worden ook de 'zachte aspecten' meegenomen. Deze richten zich op het menselijk handelen, cultuuraspecten en daarnaast op 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 is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals de BRP, de BAG of het financiële systeem, maar kan ook gericht zijn op de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.

1.3 Toelichting op ISO 27001 en ISO 27002

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?
Het gemeentebreed informatiebeveiligingsbeleid is volledig gebaseerd op de internationale standaard voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002. De eerste standaard (27001) biedt een richtlijn voor de implementatie en planmatige borging van informatiebeveiliging binnen de organisatie. Dit wordt ook wel het information security management system genoemd. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde 'best practices' voor een praktische en concrete aanpak van informatiebeveiliging binnen de organisatie. De Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) is afgeleid van deze beide internationale informatiebeveiligingsnormen, waarbij in de Baseline Informatiebeveiliging Nederlandse Gemeenten de methodiek en de terminologie specifiek is aangepast, om aan te sluiten op de geldende situatie binnen gemeenten.

1.4 Algemene oriëntatie en positionering

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?

Informatiebeveiliging maakt een onlosmakelijk deel uit van de bedrijfsvoering en de 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:
- Algemeen beveiligingsbeleid (bijv. deuren, kluizen, toegangscontrole, alarmering).
- Personeelsbeleid (bijv. screening, opleiding en functietypering).
- Organisatiebeleid (bijv. functiescheiding).
- Informatiseringsbeleid (bijv. standaardisatie, internet en cloud computing).
- Privacybeleid (bijv. correct gebruik van persoonsgegevens).
- Juridisch beleid (bijv. afbreukrisico's bij privacyschendingen, clausulering in overeenkomsten met derden, third party mededelingen).
- Dienstverleningsconcepten (bijv. website, het Nieuwe Werken, DigiD).

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

1.5 Verantwoordelijkheid en bevoegdheid informatiebeveiligingsbeleid
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?
De gemeenteraad heeft een specifieke bevoegdheid om de werking van beleid binnen de gemeente1 te controleren, inclusief het informatiebeveiligingsbeleid. De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris.
De vaststelling en implementatie van de informatiebeveiligingsstructuur2 en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de Gemeente Beverwijk. Voor het nemen van operationele maatregelen is de gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij afdelingsoverstijgende (informatie)systemen.
De verantwoordelijkheid op het gebied van de informatiesystemen waarvan zij eigenaar zijn, ligt bij het Algemeen Management Team (AMT). Zij dienen deze systemen te classificeren en zo in te richten, dat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers tijdens hun dagelijkse werkprocessen, mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie.

_____
1 In hoofdstuk 3 worden de verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging uitgebreider beschreven.
2 Onder het begrip informatiebeveiligingsstructuur wordt in dit verband de complete beheercyclus van het informatiebeveiligingsproces verstaan (beleidsvorming, implementatie, verantwoording, controle en bijstelling). Informatiebeveiliging wordt gedefinieerd als een verzamelbegrip voor de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

1.6 Wettelijke basis en controle beveiligingsnormen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?
De wettelijke basis van informatiebeveiliging valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):
- De Grondwet.
- De Auteurswet.
- De Telecommunicatiewet.
- De Ambtenarenwet.
- De Wet computercriminaliteit.
- De Wet bescherming persoonsgegevens (Wbp).
- De Archiefwet / Archiefregeling.
- De Databankenwet.
- De Wet elektronisch bestuurlijk verkeer.
- De Wet elektronische handtekeningen.
- De Wet algemene bepalingen burgerservicenummer.
- De Paspoortwet.
- De Wet basisregistratie personen (BRP).
- De Wet openbaarheid van bestuur (Wob).

- De Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI).
- De Wet basisregistratie adressen en gebouwen (BAG).
- De Wet kenbaarheid publiekrechtelijke beperkingen (WKPB).
- De nieuwe Wet ruimtelijke ordeningen (nWRO).

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

1.7 Opbouw hoofdstukken
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 1. Waarom informatiebeveiliging?
In de navolgende hoofdstukken worden de informatiebeveiligingsnormen beschreven. Elk hoofdstuk begint met de doelstelling en het beoogde resultaat en beschrijft vervolgens de basisnormen.
De indeling van het informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING). Als referentie zijn de hoofdstuknummers uit de Baseline Informatiebeveiliging Nederlandse gemeenten (BIG) achter ieder hoofdstuk vermeld.
- Hoofdstuk 1: Waarom informatiebeveiliging?
- Hoofdstuk 2: Informatiebeveiligingsbeleid en -plan (BIG hoofdstuk 5).
- Hoofdstuk 3: Organisatie van de informatiebeveiliging (BIG hoofdstuk 6).
- Hoofdstuk 4: Classificatie en beheer van informatie en bedrijfsmiddelen (BIG hoofdstuk 7).
- Hoofdstuk 5: Beveiligingsaspecten ten aanzien van personeel (BIG hoofdstuk 8).
- Hoofdstuk 6: Fysieke beveiliging (BIG hoofdstuk 9).
- Hoofdstuk 7: Beheer van communicatie- en bedieningsprocessen (BIG hoofdstuk 10).
- Hoofdstuk 8: Logische toegangsbeveiliging (BIG hoofdstuk 11).
- Hoofdstuk 9: Verwerving, ontwikkeling en onderhoud van systemen (BIG hoofdstuk 8).
    - Hoofdstuk 10: Beveiligingsincidenten (BIG hoofdstuk 13).
    - Hoofdstuk 11: Continuïteitsbeheer (BIG hoofdstuk 14).
    - Hoofdstuk 12: Naleving (BIG hoofdstuk 14).
    - Begrippenlijst.
    - Rollen en namen informatiebeveiligingsorganisatie.

Hoofdstuk 2: Informatiebeveiligingsbeleid en -plan (BIG hoofdstuk 5).

2.1 Beleidsdocument voor informatiebeveiliging
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 2. Informatiebeveiligingsbeleid – plan

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

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

Het college van B en W moet een gemeentebreed beleidsdocument voor informatiebeveiliging goedkeuren, uitgeven en aan alle medewerkers kenbaar maken en behoort conform dit document te handelen.
De volgende aspecten moeten minimaal in dit beleidsdocument worden opgenomen:
- De doelstellingen voor de gemeente op het gebied van informatiebeveiliging.
- De beveiligingseisen en -prioriteiten.
- De organisatie van de informatiebeveiligingsfunctie (zie hoofdstuk 3).
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging voor Algemeen Management Team (AMT), medewerkers en ondersteunende afdelingen en rollen.
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacy bescherming, integriteit, archivering en fysieke beveiliging en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie 1.6).
- Een verwijzing naar een specifieke informatiebeveiligingsanalyse (zie 2.3) en procedures, gedragsregels en overige relevante documentatie.
- Het benoemen van de raakvlakken met andere relevante organisatieaspecten (zie 1.4) zoals algemeen beveiligingsbeleid, organisatiebeleid, informatiseringsbeleid, bedrijfscontinuïteit, perso-

neelsbeleid, ICT-beheer, privacy beleid, het (digitale) dienstverleningsconcept en het juridisch beleid.
- Een beschrijving van het periodieke evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kan worden getoetst (zie 2.5).

2.2 Scope van het informatiebeveiligingsbeleid
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 2. Informatiebeveiligingsbeleid -plan
De scope van dit beleid omvat alle gemeentelijke 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 op de informatie in fysieke c.q. analoge vorm, ongeacht de locatie, het tijdstip of de gebruikte apparatuur.

2.3 Borging van het informatiebeveiligingsbeleid
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 2. Informatiebeveiligingsbeleid -plan
Om borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 3), onderstaande Plan Do Check Act cyclus (PDCA cyclus) doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA cyclus (zie figuur 2):

1. Informatiebeveiligingsbeleid: bevat het informatiebeveiligingsbeleid en de visie op informatiebeveiliging. Bijstelling van het informatiebeveiligingsbeleid vindt plaats om de 3 tot 4 jaar.
2. Informatiebeveiligingsplan: bevat de risicoanalyse (de toets aan de praktijk) op basis van het informatiebeveiligingsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid aan wordt gerefereerd. Bijstelling van het Informatiebeveiligingsplan vindt plaats om de 1 tot 2 jaar.
3. Plan van aanpak: bevat de concrete acties volgend uit de risicoanalyse. Bijstelling van het plan van aanpak (hieronder valt ook de voortgang op het gebied van de realisatie van de afgesproken acties en maatregelen) vindt viermaal per jaar plaats, conform de bespreking in de ambtelijke stuurgroep informatiebeveiliging (zie hoofdstuk 3).

Hoofdstuk 3: Organisatie van de informatiebeveiliging (BIG hoofdstuk 6).

3.1 Verantwoordelijkheidsniveaus binnen de organisatie
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging

Doelstelling

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

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

Binnen de Gemeente Beverwijk worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatiebeveiliging onderscheiden:

3.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het college van B en W van de Gemeente Beverwijk draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor het bewerkstelligen van een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging vast, op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatiebeveiligingsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging, gemandateerd aan de gemeentesecretaris.

3.1.2 Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging binnen de bedrijfsprocessen en de interne en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij leidinggevenden op organisatieniveau.

3.1.3 Verantwoordelijkheden en taken op afdelings- en teamniveau
De afdelingshoofden zijn (eind)verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling en hebben deze verantwoordelijkheid gedelegeerd aan de teamleiders binnen hun afdeling.

3.1.4 Verantwoordelijke Informatiebeveiliging
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. Deze rol is belegd bij de teamleider Informatieregie.

3.1.5 Controleur Informatiebeveiliging
Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.
De rol van Controleur Informatiebeveiliging heeft op twee specifieke deelgebieden een voorgeschreven officiële benaming. Dit betreft het gebied van reisdocumenten en rijbewijzen. Het betreft de volgende benamingen:

- Beveiligingsfunctionaris reisdocumenten. Deze is verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- Beveiligingsfunctionaris rijbewijzen. Deze is verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

De rol van Controleur informatiebeveiliging is belegd bij de medewerker kwaliteit en interne controle van team Administratie en Kwaliteit van de afdeling samenleving.

3.1.6 Het team Informatieregie
Het team Informatieregie van de afdeling Bedrijfsvoering, waarvan systeembeheer deel uit maakt, beheert de werkplekken, serverplatformen, lokale netwerken, wifi verbindingen, externe netwerkverbindingen (zoals Gemnet en Suwinet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en hulpmiddelen voor kantoorautomatisering. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

3.1.7 Het team Services
Het team Services van de afdeling Bedrijfsvoering is verantwoordelijk voor de fysieke toegangsbeveiliging en de kantoorinrichting (archiefkasten, kluizen enzovoort).

3.1.8 Het team Advies
Het team Advies van de afdeling Bedrijfsvoering is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviserende rol op het gebied van organisatie- en informatieprocessen.

3.1.9 De beveiligingsbeheerder
Deze rol draagt verantwoordelijkheid voor het beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. Binnen wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden, ten aanzien van specifieke methodes van gegevensverzameling. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan de beveiligingsbeheerder. De deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming, zijn de volgende: BRP, reisdocumenten (officieel autorisatiebevoegde reisdocumenten/aanvraagstations) , rijbewijzen (autorisatiebevoegde rijbewijzen), BAG, SUWI (officieel Security Officer SUWI) en DigiD.
De autorisatiebevoegde reisdocumenten/aanvraagstations is verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).
De autorisatiebevoegde rijbewijzen is verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
De overige beheerrollen zijn belegd bij de functioneel applicatiebeheerders van voormelde deelgebieden.

3.1.10 Security Officer SUWI
De Security Officer beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen wordt geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert deze evenals de beveiliging van Suwinet en ziet erop toe of de maatregelen worden nageleefd. Het evalueren van de uitkomsten, advies geven hierover en het doen van voorstellen tot implementatie c.q. aanpassingen van plannen op het gebied van de beveiliging van Suwinet, behoort ook tot zijn takenpakket. De Security Officer heeft wat betreft rapportages formeel gezien een bijzondere rol. Hij rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke. Deze rol is belegd bij de medewerker Kwaliteit en interne controle van team Administratie en Kwaliteit van de afdeling Samenleving.

3.1.12 Functionaris voor de gegevensbescherming
Momenteel mogen organisaties zelf bepalen of ze een functionaris voor de gegevensbescherming (FG) benoemen: benoeming van een FG is nu niet verplicht. Dit wordt anders zodra de Europese Privacy Verordening in werking treedt. Deze rol wordt functionaris voor de gegevensbescherming (FG) of Data Protection Officer (DPO) genoemd. De functionaris gegevensbescherming is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Bij organisaties met een FG stelt de Autoriteit persoonsgegevens (AP) zich terughoudend op als toezichthouder. Deze rol is belegd bij de adviseur informatievoorziening.

3.1.13 Functioneel applicatiebeheerder
Verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening, rekening houdend met de maatregelen op het terrein van informatiebeveiliging en privacy.

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

3.1.15 Gegevensbeheerder
De gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten, gericht op de inhoudelijke kwaliteitszorg van gegevensverzameling, gegevensverwerking en de informatievoorziening.

3.2 Toewijzing verantwoordelijkheden voor informatiebeveiliging
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging

De gemeentesecretaris heeft minimaal de volgende verantwoordelijkheden:
- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie.
- Het uitdragen van het belang van informatiebeveiliging (specifieke eis uit ISO 27001/2013).
- Het sturen op concern risico's.
- Het periodiek evalueren van beleidskaders en waar nodig het bijstellen hiervan.
- Het (laten) controleren of getroffen veiligheidsmaatregelen overeenkomstig zijn met de betrouwbaarheidseisen en het nagaan of deze veiligheidsmaatregelen voldoende bescherming bieden.
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en -systemen.
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken, met betrekking tot informatiebeveiliging.
- Het aanstellen van Verantwoordelijke Informatiebeveiliging en Controleur Informatiebeveiliging.

Algemeen Management Team (AMT) heeft in ieder geval de volgende verantwoordelijkheden:
- Het uit (laten) voeren van maatregelen uit het Informatiebeveiligingsplan, die op de betreffende afdelingen van toepassing zijn.
- Het op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen.
- Het aanwijzen, implementeren en uitdragen van maatregelen die voortvloeien uit de opgestelde betrouwbaarheidseisen.
- Het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op de naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- Het via de Verantwoordelijke Informatiebeveiliging in de P&C managementrapportages rapporteren over de mate van compliance op het gebied van wet- en regelgeving en tevens over het algemeen gevoerde beleid van de gemeente.

Verantwoordelijke Informatiebeveiliging heeft in ieder geval de volgende verantwoordelijkheden:
- Hij coördineert de formulering van het informatiebeveiligingsbeleid.
- Hij stelt het Informatiebeveiligingsplan op en zorgt voor de actualisatie van dat plan.
- Het coördineren van de uitvoering van de informatiebeveiligingsmaatregelen uit het Informatiebeveiligingsplan.
- Het tot stand brengen van een afstemmingsmechanisme voor overleg en rapportage, met betrekking tot informatiebeveiliging.
- Het ondersteunen van de directie en de afdelingshoofden door middel van kennisoverdracht op het gebied van informatiebeveiliging, zodat deze hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening op correcte wijze kunnen invullen.
- Fungeren als aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatiebeveiliging.
- Het volgen van externe invloeden die gevolgen hebben voor het informatiebeveiligingsbeleid en het Informatiebeveiligingsplan.
- De bevordering van het beveiligingsbewustzijn binnen de organisatie.
- Het registreren van informatiebeveiligingsincidenten in het daarvoor bestemde incidentenregister en het dragen van verantwoordelijkheid voor de juiste afhandeling en evaluatie van incidenten.
- Het controleren van de opname van informatiebeveiliging als onderdeel van het informatieplannings-, systeemontwikkelings- en onderhoudsproces (zie 10.1).
- Rapporteren over de status van de informatieveiligheid van de gemeente in P&C managementrapportages. Hierbij bundelt Verantwoordelijke Informatiebeveiliging de deelbijdragen van het afdelingsmanagement.

Controleur Informatiebeveiliging heeft in ieder geval de volgende verantwoordelijkheden:
- Periodieke toetsing op correcte naleving, werking, effectiviteit en kwaliteit van de maatregelen die ten aanzien van informatieveiligheid getroffen zijn.
- De controle op de voortgang van de uitvoer van de maatregelen uit het informatiebeveiligingsplan.
- De controle op de periodieke actualisatie van het informatiebeveiligingsbeleid en het Informatiebeveiligingsplan.
- Het minimaal ééns per jaar toetsen van de managementrapportages op inhoud en vorm, zoals ingebed in de bestaande P&C-cyclus. (De lijn rapporteert via Verantwoordelijke Informatiebeveiliging over informatiebeveiliging, waarbij de controller op inhoud en vorm toetst).
- Het toetsen/bewaken van het niveau van informatiebeveiliging.
- Toetsing van het evaluatieproces van beveiligingsincidenten.

De beveiligingsbeheerder heeft in ieder geval de volgende verantwoordelijkheden:
De beveiligingsbeheerder is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures (voor het aan hem toegewezen deelgebied) die voortkomen uit het informatiebeveiligingsbeleid en het onderliggende Informatiebeveiligingsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een ade-

quate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de Verantwoordelijke Informatiebeveiliging en Controleur Informatiebeveiliging.

De Functionaris Gegevensbescherming heeft in ieder geval de volgende verantwoordelijkheden:
- Organisatiebreed adviseren over privacy bescherming en over activiteiten ter bescherming van persoonsgegevens.
- Het geven van aanwijzingen aan gebruikers van systemen, met betrekking tot de correcte handelswijze bij persoonsregistraties.
- Het gevraagd of ongevraagd advies uitbrengen over alle procedures en producten die betrekking hebben op de registratie van personen.
- Het binnen de gemeente fungeren als contactpersoon voor de Autoriteit Persoonsgegevens (AP).

3.3 Overleg- en afstemmingsorganen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging

Verantwoordelijke Informatiebeveiliging is voorzitter van het overleg over informatiebeveiliging, dat vier maal per jaar plaatsvindt. Bij dit overleg zijn aanwezig:
- Verantwoordelijke Informatiebeveiliging;
- Controleur Informatiebeveiliging;
- beveiligingsbeheerders t.a.v.: BRP, waardedocumenten, BAG, SUWI en DigiD;
- beveiligingsbeheerders t.a.v.: FZ, ICT en DIV;
- de Functionaris Gegevensbescherming;
- agendaleden: MT leden of specialisten.

Onderwerpen:
- Voortgang uitvoering maatregelen beveiligingsplan c.q. plan van aanpak.
- Veiligheidsincidenten.
- Planning en voorbereiding van audits en controles.
- Evaluatie en actualisatie informatiebeveiliging en het Informatiebeveiligingsplan.

Tevens vindt afstemming plaats tussen Verantwoordelijke Informatiebeveiliging en de functioneel applicatie- en gegevensbeheerder(s) en de procesverantwoordelijke(n) van (informatie)systemen.

3.4 ICT-crisisbeheersing
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging
Er dient een kernteam informatiebeveiliging te zijn samengesteld, dat zich bezig houdt met interne crisisbeheersing. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Het team bestaat uit Verantwoordelijke Informatiebeveiliging, Afdelingshoofd Bedrijfsvoering, de communicatieadviseur en de communicatiemedewerker van team Advies.

3.5 Rapporteren beveiligingsincidenten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging
Verantwoordelijke Informatiebeveiliging wordt door de procesverantwoordelijken geïnformeerd over beveiligingsincidenten en legt deze vast, ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen van de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen. Dit kan gevolgen hebben voor de continuïteit en integriteit van de bedrijfsprocessen, evenals signaleringen waaruit blijkt dat het informatiebeveiligingsbeleid niet wordt nageleefd. Zie Hoofdstuk 10 voor meer informatie over de definitie en de procedure met betrekking tot beveiligingsincidenten.
Afspraken moeten worden gemaakt over:
- het doel van de registratie;
- de inhoud van de registratie;
- de mate van detaillering;
- de wijze van handelen;
- de wijze van rapporteren.

Er wordt minimaal eenmaal per jaar gerapporteerd aan Afdelingshoofd Bedrijfsvoering door Verantwoordelijke Informatiebeveiliging.

3.6 Verantwoordelijkheden afdelingsoverstijgende (informatie)systemen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging

Afdelingsoverstijgende (informatie)systemen (zoals Office en Outlook) die binnen de Gemeente Beverwijk in gebruik zijn, worden onder de verantwoordelijkheid van het team ICT gefaciliteerd en onderhouden. Deze systemen worden door meerdere gemeentelijke organisatieonderdelen gebruikt en bevatten gegevens die door verschillende organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie het gezag dit te mandateren aan een organisatieonderdeel, dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd eigenaar van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik hiervan, de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden op het gebied van beveiliging voor alle betrokken partijen duidelijk zijn omschreven.
De procesverantwoordelijke maakt schriftelijk afspraken met de gemeentelijke organisatieonderdelen of de externe organisatie die van het afdeling overstijgend (informatie)systeem gebruik maken.
De volgende afspraken dienen minimaal te worden vastgelegd:

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

3.7 Contracten met derden
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 3. Organisatie van de informatiebeveiliging

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

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

3.7.3 Toegang
Bij toegang van derden tot de gemeentelijke ICT-voorzieningen gelden in principe de onderstaande uitgangspunten:

- Informatiebeveiliging is (op basis van een risicoafweging) meegewogen bij het besluit om 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 welk gevoeligheidsniveau) de informatie heeft, waarmee de externe partij in aanraking kan komen en wordt besloten of er eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang wordt vastgesteld.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt er een bewerkersovereenkomst (conform Wbp artikel 14) afgesloten.
- Er is binnen contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij opgesteld nageleefd worden en dat voorkomende beveiligingsincidenten onmiddellijk worden gerapporteerd.

Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. aan de hand van audits en penetratietests) en hoe het toezicht is geregeld. Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

3.7.4 Grote projecten
Voor grote ICT-projecten gelden specifieke op centraal niveau vastgestelde richtlijnen, vooral ten aanzien van Europese aanbestedingen, screening van bedrijven en juridische aspecten.

Hoofdstuk 4: Classificatie en beheer van informatie en bedrijfsmiddelen (BIG hoofdstuk 7).

4.1 Inventarisatie van informatie en (informatieve) bedrijfsmiddelen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 4. Classificatie en beheer van informatie en bedrijfsmiddelen

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

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

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang hiervan worden vastgelegd.
Het team ICT houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie)systemen (dit wordt ook wel configuratiemanagement genoemd). Hieronder vallen de volgende zaken:

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

In de registratie is opgenomen waar de gegevens(bestanden) zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de procesverantwoordelijken en beheerders zijn.
De gebouwenbeheerder houdt een registratie bij van alle fysieke voorzieningen die verband houden met (informatie)veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.

4.2 Eigendom van informatie en bedrijfsmiddelen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 4. Classificatie en beheer van informatie en bedrijfsmiddelen
Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren ondergebracht te worden bij een eigenaar uit een aangewezen deel van de organisatie. Voor elke applicatie, gegevensverzameling en ICT-faciliteit en elk bedrijfsproces is een verantwoordelijk manager benoemd.

4.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 4. Classificatie en beheer van informatie en bedrijfsmiddelen
Er zijn regels vastgesteld, geïmplementeerd en gedocumenteerd ten aanzien van aanvaardbaar gebruik van informatie en bedrijfsmiddelen, verband houdende met ICT-voorzieningen en informatieprocessen.
Hieronder volgen de geldende uitgangspunten:

- Apparatuur en programmatuur die onder het eigenaarschap van de organisatie vallen, mogen niet zonder vooraf afgegeven toestemming van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de aangewezen eigenaar hiervan worden gedelegeerd, maar de eigenaar blijft eindverantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken gemeentelijke informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privé gebruik van gemeentelijke informatie en bestanden is niet toegestaan.

- Voor het werken op afstand en het gebruik maken van privé middelen 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 werkzaamheden.
  - Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop dient wel beveiligd te zijn.
  - Het verbod op ongewenst gebruik binnen de (fysieke) kantooromgeving geldt ook, als dit via de eigen computer plaatsvindt.

De medewerker treft passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
- de beveiligingsclassificatie van de informatie;
- de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
- de aan de werkplek verbonden risico's; het vergrote risico bij het raadplegen van gemeentelijke informatie, met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

4.4 Classificatie van informatie en bedrijfsmiddelen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 4. Classificatie en beheer van informatie en bedrijfsmiddelen

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen wordt gebruik gemaakt van beveiligingsclassificaties. De gemeentelijke informatiesystemen worden geclassificeerd op basis van de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatieniveaus weer. Na deze classificatie is onder meer duidelijk welke specifieke gemeentelijke informatie als vertrouwelijk wordt gezien. Aan de hand van deze informatie is duidelijk welke maatregelen per informatiesysteem nodig zijn.
Daar waar de maatregelen op de punten beschikbaarheid (niveau 'noodzakelijk'), integriteit (niveau 'hoog') en vertrouwelijkheid (niveau 'vertrouwelijk'), zoals gehanteerd in dit gemeentebreed informatiebeveiligingsbeleid (conform de BIG) als voldoende kunnen worden aangemerkt, is het niet noodzakelijk om aanvullende maatregelen te treffen. Door het implementeren van alle maatregelen, zoals beschreven in dit gemeentebreed informatiebeleid wordt het vereiste beveiligingsniveau voldoende afgedekt.

Classificatietabel

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen / 0	**Openbaar** Informatie mag door iedereen worden ingezien *(bijv: algemene informatie op de externe website van de gemeente).*	**Niet zeker** Informatie mag worden veranderd *(bijv: templates en sjablonen).*	**Niet nodig** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bijv: ondersteunende tools als routeplanners).*
Laag / I	**Bedrijfsvertrouwelijk** Informatie is toegankelijk voor alle medewerkers van de organisatie *(bijv: informatie op het intranet).*	**Beschermd** Het bedrijfsproces staat enkele (integriteits)fouten toe *(bijv: rapportages).*	**Noodzakelijk** Informatie mag incidenteel niet beschikbaar zijn *(bijv: administratieve gegevens).*
Midden / II	**Vertrouwelijk** Informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bijv: persoonsgegevens, financiële gegevens).*	**Hoog** Het bedrijfsproces staat zeer weinig fouten toe *(bijv: bedrijfsvoeringsformatie en primaire procesinformatie zoals vergunningen).*	**Belangrijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bijv: voorwaardelijke primaire procesinformatie).*
Hoog / III	**Geheim** Informatie is alleen toegankelijk voor direct geadresseerde(n) *(bijv: bijzondere persoonsgegevens zoals, zorggegevens en strafrechtelijke informatie).*	**Absoluut** Het bedrijfsproces staat geen fouten toe *(bijv: specifieke gemeentelijke informatie op de website o.a. gegevens waaraan rechten zijn te ontlenen).*	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bijv: basisregistraties BRP en SUWI).*

Hoofdstuk 5: Beveiligingsaspecten ten aanzien van personeel (BIG hoofdstuk 8).

5.1 Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. 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 worden benoemd.

_____

Hieronder volgen de geldende algemene uitgangspunten:

- Algemeen Management Team (AMT) is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van dienstverbanden of overeenkomsten met externen. Het team Advies houdt toezicht op dit proces.
- Algemeen Management Team (AMT) bepaalt welke rollen betreffende medewerkers moeten vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en binnen gemeentelijke regelingen.
- Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

5.2 Voorwaarden tewerkstelling vast personeel in loondienst
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. personeel
Alle medewerkers die in dienst van de Gemeente Beverwijk zijn leggen een eed/belofte af (die met terugwerkende kracht geldig is). Hiermee stemmen zij in te zullen handelen conform de voorschriften, zoals vermeld in het integriteitsprotocol, dat ter ondertekening wordt voorgelegd. Daarnaast overleggen nieuwe medewerkers een Verklaring Omtrent Gedrag (VOG). Bij indiensttreding wijst de leidinggevende de werknemer bovendien 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.

5.3 Voorwaarden tewerkstelling externen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. personeel
Uitzendkrachten, stagiaires en andere extern ingehuurde personen (denk hierbij aan leveranciers) die toegang hebben tot vertrouwelijke gemeentelijke informatie, tekenen een geheimhoudingsverklaring. Deze tijdelijke medewerkers worden evenals de medewerkers die in vaste dienst zijn, geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol, dat ter inzage wordt voorgelegd. Daarnaast overleggen deze externen een Verklaring Omtrent Gedrag (VOG). Het afdelingshoofd wijst 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.

5.4 Kwetsbare functies
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. personeel
De gemeente kiest ervoor een zorgvuldige selectieprocedure te handhaven, om aan de hand hiervan een betrouwbaar personeelsbestand te kunnen samenstellen. Er wordt hierbij geen onderscheid gemaakt tussen functies of functieniveaus. Van elke afzonderlijke medewerker wordt verwacht dat deze integer handelt.

5.5 Toegang en bevoegdheden personeel
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. personeel
Bij de indiensttreding van personeel vindt de toekenning van fysieke en logische toegangsbevoegdheden volgens een vastgestelde procedure plaats. De beslissing hierover word genomen door de daarvoor geautoriseerde personen. Bij de beëindiging van een dienstverband of bij functiewijzigingen dienen alle door de organisatie uitgereikte bedrijfsmiddelen te worden geretourneerd. Toegekende autorisaties worden vervolgens in opdracht van het lijnmanagement aan de hand van een vastgestelde procedure, met onmiddellijke ingang verwijderd of aangepast aan de nieuwe status (zie hoofdstukken 6 en 8).

5.6 Opleiding en communicatie
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. personeel
Alle medewerkers (en eventueel externe gebruikers van de gemeentelijke systemen) ontvangen een training waarin hen wordt uitgelegd, welke procedures aangaande informatiebeveiliging binnen de gemeente of de betreffende afdeling moeten worden toegepast. Deze training dient regelmatig te worden herhaald om het niveau van het heersende beveiligingsbewustzijn op peil te houden. Ten aanzien van communicatie en bewustwording geldt het volgende:

- Alle medewerkers binnen de organisatie worden ingelicht over het beveiligingsbeleid en de (beveiligings)procedures van de gemeente en krijgen informatie over het correcte gebruik van de ICT- en toegangsvoorzieningen. Dit geldt ook voor eventuele externe gebruikers.
- De gemeentesecretaris, het MT en Algemeen Management Team (AMT) hebben als taak de algehele communicatie en bewustwording rondom informatieveiligheid te bevorderen.
- Algemeen Management Team (AMT) hebben als taak erop toe te zien dat medewerkers (en externe gebruikers van de gemeentelijke systemen), zich aan de geldende beveiligingsrichtlijnen houden.
- In werkoverleggen wordt periodiek aandacht besteed aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in daarvoor bestemde planningsgesprekken.

5.7 Bijzondere situaties
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 5. Beveiligingsaspecten t.a.v. personeel
Indien er sprake is van ernstige verdenkingen in de richting van een medewerker, betreffende verduistering of gedrag dat in strijd is met intern gehanteerde regels, is het mogelijk dat de Gemeente Beverwijk gebruik zal maken van opsporingsmogelijkheden. Hierbij kan gebruik worden gemaakt van (verborgen) camera's, microfoons en loggegevens. Ook de door de gemeente verstrekte telefoon en automatiseringsmiddelen kunnen in deze gevallen worden onderzocht. Voor de inzet van deze methoden is schriftelijke toestemming nodig van de gemeentesecretaris.

Hoofdstuk 6: Fysieke beveiliging (BIG hoofdstuk 9).

6.1 Algemene uitgangspunten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging

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

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

Algemene uitgangspunten
Van de volgende algemene uitgangspunten wordt uitgegaan:
- De schade door bedreigingen van buitenaf (zoals brand, overstromingen, explosies, oproer, stroomonderbrekingen) wordt beperkt door het nemen van passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- In diverse panden van de gemeente wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal wordt beperkt door de Wet bescherming persoonsgegevens en andere geldende wet- en regelgeving.
- De fysieke toegang tot ruimten waarin zich informatie en ICT-voorzieningen bevinden, is voorbehouden aan daarvoor bevoegd personeel.
- Serverruimten, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.
- In serverruimten, datacenters en patchskasten is eten of drinken niet toegestaan.

6.2 Inventarisatie van bedrijfsmiddelen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
Om een passend beveiligingsniveau te kunnen bieden, moeten zowel informatie als bedrijfsmiddelen worden geïnventariseerd en dient de waarde en het belang hiervan te worden onderkend. Door Afdelingshoofd Bedrijfsvoering wordt een registratie bijgehouden van alle bedrijfsmiddelen die verband houden met de veiligheid van ruimten, gebouwen en de directe omgeving van betreffende gebouwen. Dit geldt voor de volgende zaken:
- De preventieve, detectieve correctieve en repressieve systemen met betrekking tot inbraak, ontruiming, brand en toegang.
- Toegangsrechten van personen tot ruimten, gebouwen en de directe omgeving van het gebouw, zoals parkeerplaatsen.

6.3 Servicetaken
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
Indien er bij de bewaking van gebouwen, personen en goederen sprake is van inhuur van een externe bewakingsdienst, voldoet deze externe partij aan de eisen volgens de Wet particuliere beveiligingsorganisaties en recherchebureaus en beschikt deze over een vergunning van het ministerie van Veiligheid en Justitie. De dienst is aangesloten bij een brancheorganisatie en er zijn afspraken gemaakt over de wijze waarop de bewakingsdienst verantwoording aflegt.

6.4 Fysieke toegang computer- en datacommunicatieruimten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
De fysieke toegang tot de specifieke computer-/serverruimten, die onder het beheer van het team Informatieregie staan, is voorbehouden aan de volgende categorieën personen:
- Systeembeheerders
- Teamleider informatieregie

Personen die niet onder de genoemde categorieën vallen, mogen de gespecificeerde ruimten alleen betreden onder begeleiding van een geautoriseerde medewerker van het team ICT.

6.5 Bewegwijzering computerruimten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
Binnen de vestiging zijn geen wegwijzers aangebracht waaruit de locaties van kritische ruimten zoals ICT-ruimten kunnen worden opgemaakt. Deze ruimten worden niet aangegeven op voor het publiek bestemde plattegronden of vermeld binnen publicaties, tenzij dit bijvoorbeeld in opdracht van de brandweer geschiedt.

6.6 Verwijderen apparatuur en gegevensdragers
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
De procedure voor het verwijderen (of het voor hergebruik gereedmaken) van overbodige apparatuur en gegevensdragers is door het team ICT opgesteld. Dit betreft apparatuur waarop gemeentelijke informatie en in licentie gebruikte software is opgeslagen.
Hierbij kan gedacht worden aan harde schijven van pc's en netwerkservers, cd's/dvd's, back-up tapes, USB-sticks en overige gegevensdragers. In deze procedure worden voorschriften genoemd voor het op correcte wijze verwijderen en zo nodig onbruikbaar maken of vernietigen van informatie.

6.7 Datakluizen en reserve apparatuur
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
Datakluizen voldoen aan de eisen die gesteld worden aan het in voldoende mate beschermen van opgeslagen gegevensdragers tegen stof, brand, water, beschadiging en diefstal.
Reserve apparatuur en back-ups worden apart van elkaar en op verschillende locaties bewaard, om zo de nadelige gevolgen van een calamiteit te kunnen minimaliseren.

6.8 Clear-desk-beleid en clear-screen-beleid
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
De Gemeente Beverwijk stelt een clear-desk-beleid vast voor papieren en verwijderbare opslagmedia, zodat dergelijke materialen niet onbeheerd op een bureau achterblijven. Daarnaast stelt de gemeente een clear-screen-beleid vast voor het gebruik van ICT-voorzieningen. Dit betekent dat alle medewerkers bij het verlaten van de werkplek het scherm blokkeren/afsluiten en dat na een bepaald tijdsverloop het beeldscherm zwart wordt en de toegang tot het werkstation wordt vergrendeld met een toegangscode. Dit om het risico van onbevoegde toegang tot verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken.

6.9 Beveiliging van (mobiele) apparatuur
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 6. Fysieke beveiliging
Informatiedragers zoals mobiele apparatuur dienen zowel binnen als buiten het gebouw fysiek beschermd worden. Dit betreft laptops, PDA's, tablets (bijvoorbeeld iPad's), memorysticks en smartphones. Omtrent het gebruik van deze apparatuur worden nadere afspraken gemaakt. De volgende basisregels zijn in ieder geval van toepassing:

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

Hoofdstuk 7: Beheer van communicatie- en bedieningsprocessen (BIG hoofdstuk 10).

7.1 Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen

Doelstelling
Het garanderen van correcte en veilige bediening evenals juist en veilig beheer van ICT-voorzieningen.

Resultaat
Maatregelen en procedures omtrent beheer en bediening van ICT-voorzieningen en de totstandbrenging van een adequate werkwijze in geval van incidenten.

Organisatorische uitgangspunten
Met betrekking tot organisatorische uitgangspunten, geldt het volgende:

- In beginsel mag niemand over autorisaties beschikken die het mogelijk maken een gehele cyclus van handelingen binnen een informatiesysteem te kunnen beheersen, zodat beschikbaarheid, integriteit of vertrouwelijkheid niet kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail (het spoor van een audit of controle) van alle handelingen en tijdstippen binnen het proces, op dusdanige wijze te worden vastgelegd dat mutaties kunnen worden herleid. De genoemde audit trail is niet toegankelijk voor diegene wiens handelingen worden vastgelegd.
- In beginsel is er sprake van een scheiding tussen beheertaken en overige gebruikstaken. Hierbij worden beheerwerkzaamheden alleen uitgevoerd wanneer er is ingelogd als beheerder en worden normale gebruikstaken alleen uitgevoerd wanneer er is 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. Deze keuze wordt gemaakt op basis van classificatie en een risicoanalyse.

7.2 Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen

Uitgangspunten
De volgende technische uitgangspunten gelden ten aanzien van communicatie- en bedieningsprocessen:

- Bij het ontvangen of wegschrijven van bestanden worden deze op geautomatiseerde wijze gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de antivirus software vindt in beginsel dagelijks plaats.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirus software toegepast.
- Het is niet toegestaan niet-geautoriseerde (pc)programmatuur te gebruiken of te installeren op gemeentelijke ICT-voorzieningen.
- Alle apparatuur die is verbonden met het niet-publiek toegankelijke netwerk van de gemeente moet kunnen worden geïdentificeerd.
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
- Het (ongecontroleerd) kopiëren van vertrouwelijke gegevens is niet toegestaan, met uitzondering van het uitvoeren van back-ups, ingezet door daarvoor bevoegde systeembeheerders.
- Updates die ten behoeve van het verhogen van de veiligheid door de leverancier worden vrijgegeven, dienen zo spoedig mogelijk via de geëigende wijzigingsprocedure te worden doorgevoerd. Dit geldt zowel voor besturingssoftware en 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 minimumniveau (service level) komt.
- Papieren gegevens worden beschermd door een deugdelijke opslag en de regeling voor de toegang tot archiefruimten.

7.3 Beheerprocedures en verantwoordelijkheden
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
De verantwoordelijkheden en procedures voor het beheer en de bediening van ICT-voorzieningen zijn beschreven en vastgesteld. Procedures zijn voor zover mogelijk in lijn gebracht met ISO 20000-1 en ISO 20000-2 (ITIL 3).

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

Change management/release management – het 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. De volgende uitgangspunten gelden hierbij:

- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever en het team ICT (veelal de proceseigenaar). De test en de testresultaten worden gedocumenteerd.
- Systemen voor Ontwikkeling, Test en Acceptatie (OTA) zijn in principe logisch gescheiden van Productie (P).
- Faciliteiten voor Ontwikkeling, Testen, Acceptatie en Productie (OTAP) zijn in principe gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
- In de OTA worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits dit voor de test absoluut noodzakelijk is.
- Vertrouwelijke data uit de productieomgeving mag niet worden gebruikt binnen de ontwikkel-, test-, opleidings- en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk blijkt om data uit de productieomgeving te gebruiken, is hierbij uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen de hiervoor bestemde procedures te worden gevolgd om de data te vernietigen nadat de ontwikkel- en testfase is beëindigd.
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Incident management – afhandeling van incidenten binnen de ICT-infrastructuur
Om te waarborgen dat incidenten snel, effectief en ordelijk worden afgehandeld, zijn verantwoordelijkheden en procedures omtrent beheer vastgesteld. Hierbij worden verschillende typen incidenten onderscheiden en wordt gezorgd voor een correcte registratie en documentatie van de afhandeling van deze incidenten. Dit proces is van groot belang en wordt in hoofdstuk 11 nader uitgewerkt.

Capaciteitsmanagement – omgang met de capaciteit van ICT-voorzieningen
Om zeker te stellen dat informatiesystemen conform de gestelde eisen van continuïteit en snelheid blijven werken, stelt het team ICT verantwoordelijkheden en procedures op ten aanzien van het monitoren van de capaciteit.

Probleemmanagement – identificatie en afhandeling van fouten binnen de ICT-infrastructuur
Het team ICT richt een organisatie in en stelt procedures op ten aanzien van het achterhalen en wegnemen van fouten in de infrastructuur.

IT service continuity management
Dit betreft het waarborgen van de continuïteit van de ICT-dienstverlening, in geval van calamiteiten. Het team ICT stelt procedures op ten aanzien van voldoende technische, financiële en organisatorische voorzieningen om de overeengekomen continuïteit van de ICT-dienstverlening in geval van calamiteiten, zeker te kunnen stellen. Hierbij geldt het volgende:

- In opdracht van de eigenaar van de data maakt het team ICT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur, zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups wordt afhankelijk van het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, bepaald door de eigenaar van de gegevens.
- De back-up wordt aan het einde van iedere dag op een externe locatie (buiten het betreffende gebouw) opgeslagen.
- De back-up en recovery maatregelen worden regelmatig, doch minimaal eens per jaar op een uitwijkcentrum getest. Tevens vindt er eens per jaar een test in de eigen ICT-omgeving plaats.

- Over het resultaat van de test wordt aan de procesverantwoordelijken gerapporteerd, te weten Verantwoordelijke Informatiebeveiliging en Controleur Informatiebeveiliging.

Configuratie management – registratie van ICT-voorzieningen
Het team ICT stelt procedures op ten aanzien van het registreren en muteren van ICT voorzieningen en de daaraan gerelateerde documentatie.

Information security management – omgang met de veiligheid van ICT-voorzieningen
Verantwoordelijke Informatiebeveiliging richt een organisatie in, stelt procedures op en traint personeel zodanig dat aan de eisen van het Informatiebeveiligingsbeleid kan worden voldaan.

7.4 Uitgangspunten voor controle en logging
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
Het gebruik van informatiesystemen, evenals het plaatsvinden van informatiebeveiligingsincidenten en uitzonderingen, wordt vastgelegd in logbestanden. Dit gebeurt op een wijze die in overeenstemming is met het gelopen risico, waarbij minimaal wordt voldaan aan alle relevante wettelijke eisen. De volgende zaken zijn relevant om in een logbestand op te slaan:

- Het type gebeurtenis (zoals het plaatsvinden van een back-up of restore, het resetten van een wachtwoord, of het betreden van een ruimte).
- Handelingen met speciale bevoegdheden.
- Ongeautoriseerde toegang (of een mislukte poging om toegang te verkrijgen).
- Systeemwaarschuwingen.
- De wijziging van een beveiligingsinstelling (of een mislukte poging hiertoe).

Met betrekking tot logregels, geldt het volgende:

- Een logregel bevat minimaal:
  - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
  - de gebeurtenis;
  - waar mogelijk de identiteit van het werkstation of de locatie;
  - het object waarop de handeling werd uitgevoerd;
  - het resultaat van de handeling;
  - de datum en het tijdstip van de gebeurtenis waarbij erop gelet wordt dat de verschillende systeemklokken gelijklopen zodat synchronisatie van logging mogelijk is.

- 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 stemmen overeen met geldende wettelijke eisen.

7.5 Beheer van de dienstverlening door een derde partij
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
Bij externe hosting van data of services (uitbesteding, cloud computing) blijft de gemeente eindverantwoordelijk voor de betrouwbaarheid van de uitbestede diensten. De toepassing van uitbesteding is gebonden aan regels en vereist goede (contractuele) afspraken en een strikte controle hierop. Bij voorkeur beschikt een leverancier over een ISO 27001 certificering.
Uitgangspunten bij externe hosting van data of services:

- Er is sprake van een goedkeuring door het verantwoordelijke afdelingshoofd c.q. de informatiemanager van de Gemeente Beverwijk.
- Er wordt voldaan aan de criteria voor leveranciers van webapplicaties en webservices, zoals opgenomen in de norm ICT-beveiligingsassessments DigiD.
- De toepassing stemt overeen met het informatiebeveiligingsbeleid evenals het algemeen gemeentelijk beleid.
- Voorafgaand is er melding gemaakt bij Afdelingshoofd Bedrijfsvoering ten behoeve van de toetsing op beheeraspecten.
- De beveiligingsmaatregelen, definities en niveaus van dienstverlening, komen overeen met de in de (bewerkers)overeenkomst voorgeschreven wijze van implementatie en uitvoer, omtrent dienstverlening door een derde partij.
- De diensten, rapportages en registraties die door de derde partij worden geleverd, worden gecontroleerd en hierbij bestaat de mogelijkheid om (periodieke) audits uit te voeren.
- In de basis-SLA omtrent dienstverlening wordt aandacht besteed aan informatiebeveiliging.
- Er is een basiscontract voor de toegang tot de ICT-voorzieningen en de informatievoorziening (bestanden, gegevens) opgesteld, waarin de richtlijnen aangaande toegang tot ICT-voorzieningen door derden staan vermeld.

7.6 Telewerken en thuiswerken
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
De Gemeente Beverwijk staat telewerken toe (op afstand werken op het netwerk van de gemeente, bijvoorbeeld thuiswerken) na toestemming van de verantwoordelijke manager. Hiervoor worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatiebeveiligingsbeleid, voor zover dit niet wordt verboden door wet- en regelgeving.

Minimaal wordt aan onderstaande punten aandacht besteed:
- De afspraken tussen de procesverantwoordelijke en de telewerker worden schriftelijk vastgelegd.
- 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 systeembeheerbevoegdheden (administrator en root). Het is niet toegestaan om via de telewerkplek in te loggen, tenzij er voldoende maatregelen zijn getroffen.

7.7 Mobiele (privé) apparatuur
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
Ten aanzien van mobiele apparatuur wordt beleid opgesteld en worden beveiligingsmaatregelen getroffen die in overeenstemming zijn met het gemeentelijk informatiebeveiligingsbeleid, voor zover dit in lijn is met geldende wet- en regelgeving.

Belangrijk hierbij zijn de volgende zaken:
- Geldende afspraken tussen de procesverantwoordelijke en de gebruiker van mobiele apparatuur of privé apparatuur worden vastgelegd, bij voorkeur in de vorm van een overeenkomst over het omgaan met vertrouwelijke en kritische informatie of documenten.
- Alle getroffen beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als op privé apparatuur.
- Op privé apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoorden, encryptiegebruik, aanwezigheid van malware, antivirusprogrammatuur en de bijbehorende instellingen van deze programmatuur etc.
- Het gebruik van privé apparatuur waarop beveiligingsinstellingen zijn verwijderd (denk hierbij aan jail-breaks of rooted devices) is niet toegestaan.
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk hierbij aan ‘mobile device management software’).
- De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en de integriteit van het gemeentelijke netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals bijvoorbeeld het op afstand wissen van apparatuur. Deze noodmaatregelen kunnen voor zover dit noodzakelijk is, betrekking hebben op privé apparatuur en privé bestanden.

7.8 Gebruik internet en e-mail
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen

E-mail en internetprotocol
De Gemeente Beverwijk heeft een gedragsovereenkomst (ook wel protocol genoemd) opgesteld ten aanzien van het gebruik van e-mail evenals voor het gebruik van internet. In deze protocollen zijn maatregelen om beveiligingsrisico’s die bij het gebruik van e-mail en internet ontstaan te beperken.

7.9 Social media
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
Medewerkers van de Gemeente Beverwijk mogen gebruik maken van sociale media. Zij dienen tijdens dit gebruik echter rekening te houden met het feit dat zij door derden als vertegenwoordigers van de gemeentelijke organisatie kunnen worden aangemerkt. Uitingen die via het internet worden verspreid hebben een permanent karakter en kunnen eventueel via andere media opnieuw worden gepubliceerd. Voor het gebruik van sociale media wordt een protocol opgesteld. De volgende richtlijnen zijn hier minimaal in opgenomen:
- Om zaken als identiteitsfraude of andere ongewenste zaken te voorkomen is het van belang nooit persoonlijke gegevens of gegevens van collega’s zoals adressen en telefoonnummers via sociale media te verspreiden.

- Bij het gebruik van internet geldt gangbare wet- en regelgeving nog steeds. Medewerkers dienen zich te beseffen dat zaken als smaad, laster of beledigingen ook op het internet strafbaar zijn. Ook wetgeving aangaande auteursrechten of op het gebied van gegevensbescherming is van toepassing tijdens het gebruik van internet.
- Medewerkers dienen bij het doen van uitingen via sociale media, rekening te houden met het effect dat deze uitlatingen op het imago van de Gemeente Beverwijk kunnen hebben.
- Het is niet gewenst dat medewerkers uitlatingen omtrent klanten of inhoudelijke bedrijfsprocessen doen via social media.

7.10 Uitwisseling van informatie over netwerken
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 7. Beheer van communicatie- en bedieningsprocessen
Bij het beheer van netwerken moet onderscheid worden gemaakt tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken dienen extra maatregelen ter waarborging van de veiligheid te worden getroffen.
Bij gebruik van andere netwerken moet geanalyseerd worden of netwerkeisen in overeenstemming met elkaar zijn en niet leiden tot onoverkomelijke problemen.
Verantwoordelijkheden en procedures omtrent toegang en beheer van netwerken, apparatuur op de werkplek en apparatuur die op afstand wordt bediend zijn vastgelegd en hierover wordt gecommuniceerd naar de betrokken partijen.

Hoofdstuk 8: Logische toegangsbeveiliging (BIG hoofdstuk 11).

8.1 Beleid voor logische toegangsbeveiliging
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging

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

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

Beleid voor logische toegangsbeveiliging
Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen invoeren en onderhouden bestaat er een gemeentebreed toegangsbeleid. Naast dit gemeentebrede toegangsbeleid heeft ieder informatiesysteem nog een specifiek gedefinieerd beleid omtrent toegang, dat is afgestemd op het classificatieniveau van de informatie.
Het toegangsbeleid is vastgesteld en aan de organisatie gecommuniceerd. In het beleid worden de volgende aspecten benadrukt:
- De aanvragen voor het verkrijgen van toegang worden geautoriseerd door de procesverantwoordelijke (eigenaar van de data/applicatie).
- Er worden in de regel geen algemene identiteiten (groepsaccounts) gebruikt. Om herleidbaarheid en transparantie te bewerkstelligen is het namelijk noodzakelijk om te weten wie een bepaalde actie heeft uitgevoerd. Indien hier geen (wettelijke) eis aan ten grondslag ligt, kan worden gewerkt met functionele accounts.
- De gemeente maakt waar mogelijk gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals: DigiD en eHerkenning).
- Alle toegekende bevoegdheden worden geregistreerd en beheerd, bijvoorbeeld met behulp van een autorisatiematrix.
- Het gebruik van speciale bevoegdheden wordt beperkt en beheerd.

De procesverantwoordelijke toetst of de door het team ICT of applicatiebeheer geïmplementeerde bevoegdheden, conform de aanvraag zijn toegekend of verwijderd.

8.2 Beheer van toegangsrechten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging
Voor het beheer van de toewijzing van toegangsrechten is er een procedure opgesteld, waarin de gehele cyclus (vanaf de registratiefase tot het afmelden van gebruikers) is opgenomen. Naast het gebruik van wachtwoorden kunnen ook andere methoden van gebruikersidentificatie en authenticatie worden toegepast. Voorbeelden hiervan zijn: biometrie, handtekeningverificatie, hardware (bijvoorbeeld tokens), sms authenticatie en het gebruik van cryptografische sleutels. Bij het beheer van gebruikerswachtwoor-

den staat de wijze waarop het initiële wachtwoord aan de gebruiker kenbaar wordt gemaakt vast en is duidelijk welke handelswijze moet worden toegepast indien het wachtwoord wordt vergeten. Verstrekte wachtwoorden moeten onmiddellijk na het eerste gebruik, door de gebruiker worden gewijzigd.

8.3 Externe toegang
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging
De gemeente kan een externe partij toegang tot het gemeentelijk netwerk verlenen. Hiervoor dient een procedure vastgesteld en gevolgd te worden. Externe partijen mogen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente, tenzij hier uitdrukkelijk toestemming voor is gegeven. De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente heeft het recht dat te controleren en doet dit aan de hand van een audit trail en interne logging.

8.4 Mobiel werken, thuiswerken en internetfaciliteiten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging
Uitgangspunten voor beleid ten aanzien van mobiel werken, thuiswerken en internetfaciliteiten:

- Voor werken op afstand is een thuiswerkomgeving c.q. mobiele werkplekomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie (iets wat je bent of hebt en weet).
- Onbeheerde apparatuur (prive apparaten of 'open' laptops) kan gebruik maken van draadloze toegangspunten (WiFi). Deze zijn logisch gescheiden van het gemeentelijk bedrijfsnetwerk.
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat (‘zero footprint’). Gemeentelijke informatie dient bij transport te worden versleuteld en de opslag behoort conform classificatie eisen te verlopen.
- Voorzieningen als webmail, social media en clouddiensten (Dropbox, Gmail, etc.) zijn door het geringe beschermingsniveau (veelal alleen naam en wachtwoord, terwijl verdere versleuteling ontbreekt) en internationale regelgeving (veelal beschikbaar voor buitenlandse onderzoeksdiensten), niet geschikt voor het delen van vertrouwelijke informatie indien deze informatie niet op adequate wijze versleuteld is.

8.5 Controle op toegangsrechten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging
Alle medewerkers die van het netwerk of van applicaties gebruik maken, moeten door het systeem of de applicatie op unieke wijze geïdentificeerd kunnen worden. Om de toegang tot de informatiesystemen effectief te beheren, wordt periodiek een uitdraai gemaakt van de verstrekte toegangsmachtigingen. Deze uitdraai wordt door Controleur Informatiebeveiliging op juistheid en volledigheid gecontroleerd.

8.6 Toegangsbeveiliging met betrekking tot netwerkdomeinen en componenten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging

Aanbrengen van scheidingen
Op plekken waar beveiligingsrisico’s dit noodzakelijk maken, is er binnen de netwerken een scheiding aangebracht. De toegang tussen deze gescheiden netwerkdomeinen is beveiligd via gateways, firewalls en routers. Afhankelijk van de toegangseisen voor de betreffende ICT-voorziening is het gebruik van de verbindingsmogelijkheden beperkt.

Demilitarized Zone (DMZ)
Voor wat betreft de internetfacing systemen moet gebruik worden gemaakt van een Demilitarized Zone (DMZ), waarbij compartimentering wordt toegepast en slechts de meest noodzakelijk verkeersstromen tussen de verschillende compartimenten worden toegestaan. In deze genoemde DMZ, bevinden zich webapplicaties die gebruik maken van DigiD. Door middel van minimaal van twee (virtuele) firewalls worden verkeersstromen tussen het internet, de (web)applicaties in de DMZ en het interne netwerk, waar de backoffice applicaties en de gemeentelijke basisregistraties zich bevinden, tot een minimum beperkt.
Voor wat betreft de informatiesystemen die aan het internet gekoppeld zijn, is het van belang om gebruik te maken van een DMZ. Een DMZ is een separate omgeving tussen het netwerk van de gemeente en het internet. Deze omgeving kan gebruikt worden om transacties op een veilige manier te behandelen. Een DMZ wordt gescheiden van zowel het netwerk als het internet, door middel van een of meerdere firewalls. Door deze constructie wordt het netwerk van de organisatie beschermd tegen onbevoegde toegang en kan het verkeer met de gemeente ook worden gereguleerd.

Intrusion Detection Systeem (IDS)

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

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

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

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

Draadloze en openbare netwerken
Het gebruik van draadloze netwerken vraagt om specifieke beveiligingsmaatregelen. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn eveneens extra maatregelen nodig. Wettelijk gezien is het gebruik van encryptie een minimale vereiste.

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

8.7 Toegangsbeveiliging met betrekking tot werkstations
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging

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

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

Gebruik van systeemhulpmiddelen (utilities)
Het gebruik van systeemhulpmiddelen waarmee toegangscontroles in systemen en toepassingen kunnen worden getest en mogelijk worden doorbroken (bijvoorbeeld sniffers), wordt beperkt tot een klein aantal bevoegde gebruikers en dit wordt nauwlettend beheerst.
Schermbeveiliging (clear screen)
Medewerkers moeten bij het verlaten van de werkplek het scherm blokkeren en na een vaste periode van inactiviteit wordt een werkstation automatisch geblokkeerd. Bij werkstations op locaties met verhoogd risico, moeten de programma- en netwerksessies afgesloten worden en wordt de gebruiker uitgelogd.

8.8 Toegangsbeveiliging met betrekking tot (informatie)systemen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 8. Logische toegangsbeveiliging

Toegang tot (informatie)systemen

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

Componenten van (informatie)systemen

Een (informatie)systeem kan uit meerdere componenten bestaan, zoals applicaties, pc's, netwerken, besturingssystemen, databases en firewalls. Voor elk van deze componenten moet apart autorisatie worden verleend.

(Informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten

(Informatie)systemen die vertrouwelijke of privacygevoelige gegevens verwerken, vereisen speciaal getroffen maatregelen, zoals de plaatsing ervan in een aparte beveiligde omgeving of in een apart beveiligd domein. De procesverantwoordelijke stelt de gevoeligheid van een (informatie)systeem en de noodzaak voor het treffen van aanvullende maatregelen expliciet vast.

Hoofdstuk 9: Verwerving, ontwikkeling en onderhoud van systemen (BIG hoofdstuk 8).

9.1 Beveiligingseisen voor (informatie)systemen

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 9. Verwerving, ontwikkeling en onderhoud van systemen

Doelstelling

Het waarborgen van de inbouw van beveiliging binnen (informatie)systemen en het meenemen van beveiligingseisen 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.

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

- Beveiligingseisen zijn zoveel mogelijk onderkend, gedocumenteerd en goedgekeurd voordat een (informatie)systeem wordt ontwikkeld of aangekocht.
- Benodigde beveiligingsmaatregelen met betrekking tot 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 of een risicoanalyse naar voren zijn gekomen.
- Bij extern toegankelijke applicaties als webapplicaties, wordt extra aandacht besteed aan het voorkomen van ongeautoriseerde toegang.

9.2 Cryptografische beveiliging

Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 9. Verwerving, ontwikkeling en onderhoud van systemen

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

Vertrouwelijkheid en onweerlegbaarheid zijn nauw aan elkaar verbonden door het gebruik van cryptografische sleutels. Als gebruik wordt gemaakt van asymmetrische versleuteling (verschillende sleutels voor versleuteling en ontsleuteling), is het publieke deel van de sleutel bestemd voor versleuteling

(vertrouwelijkheid) van gegevens. Het privé gedeelte van de sleutel is bestemd voor ontsleuteling en het plaatsen van digitale handtekeningen (onweerlegbaarheid/onloochenbaarheid).
PKI-certificaten worden herkend in veel standaardtoepassingen, zoals webbrowsers en e-mail pakketten. Met behulp van algemene PKI-certificaten is de informatie die personen en organisaties via het internet versturen, op een hoog niveau beveiligd.
PKI-overheid-certificaten bieden aanvullende zekerheden. Een digitaal certificaat van PKI-overheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatieuitwisseling via e-mail, websites of andere gegevensuitwisseling.
PKI-overheid-certificaten worden gebruikt bij:

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

Wanneer er gebruik gemaakt wordt van cryptografische sleutels 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 en sleutels niet verloren gaan.

9.3 Digitale handtekening
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 9. Verwerving, ontwikkeling en onderhoud van systemen
Bij gebruik van digitale handtekeningen als middel om de authenticiteit en integriteit van elektronische documenten te waarborgen, worden alle sleutels afdoende beveiligd tegen wijziging en vernietiging. Ook worden persoonlijke sleutels (private keys) beschermd tegen onbevoegde openbaarmaking.

9.4 Uitbesteding ontwikkeling van (informatie)systemen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 9. Verwerving, ontwikkeling en onderhoud van systemen
In deze situatie ontwikkelt de gemeente niet zelf een (informatie)systeem, maar besteedt ze het ontwikkel- en productiewerk uit. De gemeente gaat vervolgens over tot aanschaf van het (informatie)systeem of tot afname van een dienst. Bij uitbesteding van de ontwikkeling van (informatie)systemen wordt rekening gehouden met:

- de noodzaak tot het aangaan van een formele overeenkomst op basis van de algemene leveringsvoorwaarden van de Gemeente Beverwijk;
- licentieovereenkomsten, eigendom van broncodes en intellectuele eigendomsrechten;
- de noodzaak tot beoordeling en controle van de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
- privacygevoeligheid en bedrijfsvertrouwelijkheid van testgegevens, bijvoorbeeld door het gebruik van anonieme of fictieve gegevens. Als door de leverancier persoonsgegevens worden bewerkt, moet worden nagegaan of deze meewerkt aan de totstandkoming van een bewerkersovereenkomst (met de gemeente), in lijn met de Wet Bescherming Persoonsgegevens;
- de mogelijkheid tot het uitvoeren van IT audits bij de leverancier (aangaande interne beheersingsmaatregelen) of bij de door de leverancier (in naam van de gemeente) ingeschakelde derden;
- de noodzaak tot het verzorgen van een waardeborgregeling in geval de externe partij in gebreke blijft (denk hierbij aan een escrow-overeenkomst waarin in bredere zin alles wat te maken heeft met intellectueel eigendom van vercijfersleutels tot softwarebroncode-escrow wordt vastgelegd);
- de noodzaak tot het door de leverancier verzorgen van een Third Party Memorandum (TPM) of ISAE3402 verklaring of een vergelijkbare verklaring van een onafhankelijke partij (Register EDP auditor), omtrent de relevante interne beheersing van processen, in het bijzonder de beveiligingsprocessen. Indien de gemeente dit verzoekt moet deze aan haar verstrekt kunnen worden;
- de noodzaak tot het opnemen van een beschrijving van de dienst in de opgestelde overeenkomst. Per geleverde dienst dient er een beschrijving te zijn opgenomen, die een verwijzing naar de betreffende service level specificaties bevat. Denk hierbij aan een concrete beschrijving van diensten, servicetijden (normale servicetijden, weekenden, feestdagen en vakantiedagen), beschikbaarheid van de service, responsetijden, oplostijden etc.;
- de noodzaak tot opname van een beschrijving van de overlegstructuren, de contactpersonen en de onderlinge communicatie, in de opgestelde overeenkomst. Er dient te worden vastgelegd wanneer gestructureerd overleg plaatsvindt en welke deelnemers dit overleg heeft. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken in geval van escalatie of calamiteiten (denk hierbij aan een escalatiematrix);
- de noodzakelijke opname van een beschrijving van de geschillenregeling binnen de opgestelde overeenkomst. Ook dient beschreven te worden wat de te volgen procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener;

- het feit dat de beschrijving van prestatie indicatoren, de wijze waarop meting plaatsvindt en de rapportagestructuur dient te worden opgenomen in de bijbehorende overeenkomst. Beschrijving van de prestatie indicatoren (Key Performance Indicators), hoe deze worden gemeten en hoe hierover wordt gerapporteerd dient tevens te worden vastgelegd;
- de noodzaak tot het aanhoudend verkrijgen van zicht 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. Als deze zaken dienen te worden vastgelegd in de op te stellen overeenkomst;
- het gegeven dat de leverancier toereikende technische en organisatorische maatregelen dient te nemen om de webapplicatie en gerelateerde gegevens te beveiligen tegen verlies, diefstal en inzage door daartoe niet bevoegde personen. Dit dient te worden opgenomen in de bijbehorend op te stellen overeenkomst;
- de vereiste dat de leverancier in de overeenkomst aangeeft dat de gehanteerde beveiligingsmaatregelen, zowel technisch als organisatorisch up-to-date worden gehouden en voldoen aan de laatst bekende beveiligingsinzichten, beveiligingsnormen en –richtlijnen;
- de noodzakelijkheid om in geval van een webapplicatie er minimaal jaarlijks penetratietesten uit te laten voeren, waarbij als uitgangspunt genomen wordt dat de leverancier de gemeente in staat stelt om aan haar verplichtingen als verantwoordelijke te voldoen. Dit vloeit voort uit de aan de DigiD gekoppelde wet- en regelgeving en de Wet bescherming persoonsgegevens (Wbp).

9.5 Hardening van systemen
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 9. Verwerving, ontwikkeling en onderhoud van systemen

De hardening van alle systemen, maar met name de internet facing systemen, dient strak te worden georganiseerd. Voor de webapplicaties en systemen geldt: er moet een geldige reden bestaan voor het open staan van elke applicatie of elk systeem en daarnaast dient deze openstand secure te zijn. De hardening van interne systemen mag minder stringent. In het geval van interne systemen moeten management functies secure zijn, mogen er geen onveilige protocollen worden gebruikt, dienen de default wachtwoorden te zijn gewijzigd en moeten ongebruikte applicaties en services te worden verwijderd.
Systeem hardening is een proces dat expliciet per leverancier moet worden ingezet, aangezien de afzonderlijke leveranciers het systeem tijdens het standaard (default) installatieproces op verschillende manieren configureren en van diensten voorzien. Alle componenten van de ICT-infrastructuur moeten onderdeel uitmaken van het hardening-proces.
Voorbeelden van situaties waarin risico's door het proces van hardening teniet kunnen worden gedaan zijn:

- Indien (externe) systemen, zoals webservers en mailservers 'reclame' maken voor hun type en versie. In deze gevallen wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren.
- Indien systemen onnodige diensten draaien en poorten open hebben staan, zonder dat hier noodzaak voor bestaat, worden zij eerder blootgesteld aan kwaadwillende aanvallers, omdat deze overbodige diensten en poorten aanvullende mogelijkheden bieden om het systeem binnen te dringen.

9.6 Hardening van websites
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 9. Verwerving, ontwikkeling en onderhoud van systemen
De websites van de gemeente worden nadrukkelijk meegenomen in het proces van hardening van websites. Aangezien niet langer gebruikte websites of verouderde informatie (die toegankelijk is via het internet) een beveiligingsrisico op kan leveren, dient de gemeente deze informatie te (laten) verwijderen.
Andere risico's schuilen vooral in encryptieprotocollen en invoervelden. Een goede richtlijn voor de beveiliging van websites is te vinden binnen de OWASP community (Open Web Application Security Project).
De verantwoordelijkheid voor de beveiliging ligt bij de gemeente en in het bijzonder bij de eigenaar van de specifieke website.

Hoofdstuk 10: Beveiligingsincidenten (BIG hoofdstuk 13).

10.1 Definitie beveiligingsincident
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 10. Beveiligingsincidenten

Doelstelling
De bewerkstelliging van het in kaart brengen van informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen, zodat er tijdig corrigerende maatregelen kunnen worden getroffen.

Resultaat
De opstelling van formele procedures aangaande de rapportage van gebeurtenissen of escalaties. Alle medewerkers (dit betreft zowel internen als extern ingehuurde gebruikers) zijn op de hoogte van de te hanteren procedures tijdens rapportage over verschillende soorten gebeurtenissen en zwakke plekken, die invloed kunnen hebben op de beveiliging van bedrijfsmiddelen.

Definitie beveiligingsincident
Een beveiligingsincident is een gebeurtenis waarbij er een kans bestaat dat de beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatiesystemen gevaar loopt.
Beschikbaarheid staat in deze beschrijving voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. Integriteit staat hier voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking hier op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen krijgen tot informatie(systemen). Voorbeelden van beveiligingsincidenten zijn: besmettingen met virussen of malware, pogingen om ongeautoriseerd toegang te verkrijgen tot informatie of systemen (hacken), het niet beschikbaar zijn van de website waarin het dienstverleningsportaal zich bevindt, het verlies van USB-sticks waarop gevoelige informatie is opgeslagen, het gebruik van gecompromitteerde mailboxen en diefstal van data of hardware.

10.2 Melding en omgang beveiligingsincidenten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 10. Beveiligingsincidenten
Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelswijze is vastgelegd die moeten worden gevolgd na het ontvangen van een rapport aangaande een beveiligingsincident. Hierbij gelden de volgende uitgangspunten:

- Verantwoordelijke Informatiebeveiliging is formeel de beheerder van de registratie van beveiligingsincidenten.
- Een medewerker meldt geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct bij Verantwoordelijke Informatiebeveiliging van de gemeente.
- Beveiligingsincidenten die worden gemeld bij de Servicedesk, worden als zodanig geregistreerd en doorgegeven aan Verantwoordelijke Informatiebeveiliging.
- Vermissing of diefstal van apparatuur of media waarop mogelijk gegevens van de gemeente zijn opgeslagen, wordt in alle gevallen aangemerkt als een informatiebeveiligingsincident.
- Informatie omtrent handelingen die relevant zijn met betrekking tot informatiebeveiliging, zoals loggegevens of foutieve inlogpogingen van gebruikers worden regelmatig gecontroleerd. Verantwoordelijke Informatiebeveiliging bekijkt periodiek een samenvatting van de als relevant aangemerkte informatie.
- Afhankelijk van de ernst van een incident bestaat er een meldplicht aan de autoriteit persoonsgegevens.
- Indien er aansluiting bestaat met de Informatiebeveiligingsdienst (IBD) dient er ook een procedure omtrent communicatie naar de Informatiebeveiligingsdienst te worden opgesteld.
- De informatie die is verkregen uit de beoordeling van beveiligingsmeldingen wordt geëvalueerd, met als doel om verbetering van beheersmaatregelen te bewerkstelligen (PDCA cyclus).
- Indien er aanleiding is voor een bijzonder onderzoek zoals beschreven in paragraaf 5.7 dient de procedure bijzonder onderzoek te worden gevolgd.

Hoofdstuk 11: Continuïteitsbeheer (BIG hoofdstuk 14).

11.1 Proces van continuïteitsmanagement
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 11. Continuiteitsbeheer

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

Resultaat
Een beheerst proces voor het waarborgen van de continuïteit 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 beheerst proces vastgesteld om de continuïteit van de organisatie als geheel te waarborgen. Het proces kent de volgende onderdelen:

- Bedrijfsprocessen worden geanalyseerd. In deze analyse wordt getracht gebeurtenissen te identificeren die kunnen leiden tot discontinuïteit. Aan de hand van een risicoanalyse is de waarschijnlijkheid en het mogelijke gevolg van een discontinuïteit in termen van tijd, schade en benodigde herstelperiode in kaart gebracht.
- Er wordt een eenduidig kader voor continuïteitsplannen opgesteld om ervoor te zorgen dat alle plannen consistent zijn. Er worden minimaal jaarlijks oefeningen of testen gehouden, waarbij de interne of externe uitwijk ook wordt meegenomen in de beoordeling. Op deze manier worden continuïteitsplannen evenals het niveau van alertheid van de organisatie getoetst. Aan de hand van de hieruit voortvloeiende resultaten worden plannen, indien dit nodig blijkt bijgesteld en wordt de organisatie op deze wijze bijgeschoold.

11.2 Relatie met nood- en ontruimingsplan
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 11. Continuiteitsbeheer
De vaststelling van een ontruimingsregeling voor de computerruimte(n) valt onder de verantwoordelijkheid van het team Services. Dit sluit aan op het algemene nood- en ontruimingsplan. Hierin wordt aangegeven op welke wijze computerfaciliteiten in geval van calamiteiten worden uitgeschakeld. Dit is eventueel van buitenaf (op afstand) te regelen. Voorts is vastgesteld hoe het team ICT de afgesproken regeling zal testen en met welke frequentie dit zal gebeuren.

11.3 Veiligstelling programmatuur
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 11. Continuiteitsbeheer
Voor alle systeemsoftware en informatiesystemen moet worden bepaald of de broncodes, al dan niet via bijvoorbeeld een escrow-contract bij derden moeten worden ondergebracht.

11.4 Monitoring capaciteit
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 11. Continuiteitsbeheer
Voor alle relevante ICT-middelen wordt het capaciteitsbeslag dusdanig gepland, dat er continu kan worden 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.

Hoofdstuk 12: Naleving (BIG hoofdstuk 14).

12.1 Organisatorische uitgangspunten
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 12. Naleving

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

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

Organisatorische uitgangspunten
Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarbij met gevoelige informatie wordt gewerkt. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan de hand van:

- de mate waarin een volledige set aan maatregelen geïmplementeerd is, gebaseerd op het vastgestelde beleid;
- efficiency en effectiviteit van de geïmplementeerde maatregelen;
- de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

Verantwoordelijke Informatiebeveiliging coördineert namens de gemeentesecretaris de uitvoering van het informatiebeveiligingsbeleid.

ICT-providers en externe hosting-providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatiebeveiligingsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI en BRP en waardedocumenten. Aanvullend op dit organisatiebrede informatiebeveiligingsbeleid kunnen daarom specifieke normen gelden.
Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van Controleur Informatiebeveiliging onderzocht via gemeentelijke auditors en door onafhankelijke externen (bijvoorbeeld door middel van penetratietesten). Jaarlijks worden meerdere audits/onderzoeken uitgevoerd. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
In de P&C-cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het 'in control' statement.
Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of waardoor kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

12.2 Naleving van informatiebeveiligingsbeleid en -plan
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 12. Naleving
Om de naleving van de beveiligingseisen uit het informatiebeveiligingsbeleid en het Informatiebeveiligingsplan te bewaken, legt de procesverantwoordelijke adequate organisatorische en procedurele afspraken vast. Kernelementen binnen het controle- en evaluatieproces zijn:
- Minimaal eenmaal per jaar voert de procesverantwoordelijke een zelfevaluatie of een audit uit.
- Managementrapportages worden minimaal eenmaal per jaar door de controleur informatiebeveiliging op inhoud en vorm getoetst en ingebed in de bestaande P&C-cyclus.

12.3 Naleving van wettelijke voorschriften
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 12. Naleving
Relevante eisen uit wet- en regelgeving evenals contractuele eisen moeten voor ieder (informatie)systeem zijn vastgelegd. Er wordt deskundig advies over specifieke juridische eisen ingewonnen bij de juridische adviseur(s) van de gemeente. Conform de Archiefwet beschikt de Gemeente Beverwijk over een systeem waarin opslag, bewaartermijnen en de vernietiging van gegevens en informatie, in analoge en digitale vorm is geregeld.
Aan de bescherming van persoonsgegevens stelt de Wet bescherming persoonsgegevens (Wbp) duidelijke eisen. De Gemeente Beverwijk stelt een privacy beheerder aan, die de uitvoering en de naleving van de Wbp bewaakt.
12.4 Beoordeling van de naleving
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » 12. Naleving
Het MT en de procesverantwoordelijken (managers) zorgen voor de controle en evaluatie op de naleving van wettelijke voorschriften van het informatiebeveiligingsbeleid. Zij beoordelen of alle beveiligingsprocedures binnen hun verantwoordelijkheidsgebied correct worden uitgevoerd en of hun processen en (informatie)systemen voldoen aan relevante wet- en regelgeving, het beveiligingsbeleid, geldende 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 (bijv. via BRP-zelfevaluatie steekproeven, SUWI- en BAG- en DigiD audits en externe accountants).

Begrippenlijst
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » Bijlagen

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

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

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

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

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

Back-up
Reservekopie van een computerbestand of programmatuur.

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen.

Beschikbaarheid
zie Continuïteit.

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

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

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

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

Clear desk (ook wel clean desk)
Een opgeruimde werkplek waar geen vertrouwelijke of privacygevoelige documenten of andere informatiebronnen rondslingeren.

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

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

Configuratie management
Beheer en beheersing van de samenstelling en de status van de 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.

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

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

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

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

Gegevens
Feiten en begrippen, weergegeven in een vorm die geschikt is voor het communiceren, interpreteren en verwerken tot informatie, hetzij door de mens, hetzij door automatische middelen, dan wel beide.

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

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens.

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

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

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

Incident
Onverwachte of ongewone gebeurtenis.

Incident management
Beheer en beheersing van de afhandeling van incidenten.

Informatie
Informatie bestaat uit gegevens verzameld en uitgewerkt om te dienen als communicatie tussen personen. Informatie behoeft echter niet te zijn vastgelegd. De vormen van informatie kunnen zijn, digitaal, papier, beeld, geluid. De informatie kan opgeslagen worden digitaal en dossiers (papier).

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

Informatiebeveiligingsbeleid
Strategie van een organisatie met betrekking tot informatiebeveiliging.

Informatiebeveiligingscoördinator / CISO / Verantwoordelijke Informatiebeveiliging
Medewerker die gemeentebreed adviseert over informatiebeveiligingsvraagstukken in brede zin en activiteiten op het gebied van informatiebeveiliging coördineert.

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

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

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

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

Internet Protocol (IP)
Veel gebruikt protocol voor netwerkverkeer.

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

Local Area Network (LAN)
Zie Lokaal netwerk.

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

Lokaal netwerk (LAN)
Fysiek afgegrensd, instellingsgebonden netwerk.

Maatwerkprogrammatuur
Op specifiek (deel)proces toegesneden programmatuur.

MARAP
Management Rapportage.

Medium (opslag-)
Fysieke gegevensdrager.

Netwerk

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

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

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

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

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

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

Personal Digital Assistant (PDA)
Kleine computer, formaat "binnenzak".

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

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

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

Programmatuur
Het geprogrammeerde deel van (informatie)systemen.

Recovery
Herstel van een computerbestand of programmatuur.

Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen.

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

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

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

SNMP

Simple Network Management Protocol: zie diagnoseprotocol.

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

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem.

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

Systeemklok
Interne klok in een computersysteem.

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

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

Technisch beheer
Opslag en onderhoud van digitale informatie door middel van technische maatregelen.

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

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

Utility
Zie Systeemhulpmiddel.

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

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden.

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

Rollen en namen informatiebeveiligingsorganisatie
Informatiebeveiliging Gemeenten » Hst 5 Beveiligingsbeleid » Gemeentebreed Informatiebeveiligingsbeleid » Bijlagen
In verband met de namen van betrokken medewerkers wordt deze niet gepubliceerd maar alleen intern verstrekt.