Gemeentelijk Informatiebeveiligings-Beleid 2014-2018

Haarlem

---

gemeente Haarlem

Versie: 1.0
Status: Definitief
Auteur: W. Mevissen
Datum: november 2014

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1		Willy Mevissen	1e ruwe versie
0.11	11-6-2013	Willy Mevissen	Verwerken opmerkingen Jeroen vd Klaauw
0.2	27-6-2013	Willy Mevissen	Wijzigingen nav bespreking met Patrick Spigt Brede verspreiding door organisatie
0.3	9-7-2013	Willy Mevissen	Na commentaar uit de organisatie.
0.4	16-9-2013	Willy Mevissen	Bijstelling structuur, verwerken commentaar CS en OR.
0.5	26-9-2013	Willy Mevissen	Afronding op basis van BIG
0.6	16-10-2013	Willy Mevissen	Na commentaar MT/MenS en stuurgroep digitalisering
0.61	30-10-2013	Jeroen van der Klaauw	Na commentaar directie
0.62	27-11-2013	Jeroen van der Klaauw/Willy Mevissen	Na aanvullend commentaar controller
0.7	30-7-2014	Willy Mevissen	Na overleg met OR par. 5.1. verwijderd en beheersmaatregel toegevoegd.
1.0	5-9-2014	Willy Mevissen	Na aanstelling CISO en ISO

Inhoud

0 Managementsamenvatting

Deze beleidsnota beschrijft het informatiebeveiligingsbeleid voor de jaren 2014 tot 2018 en vervangt het in 2011 vastgestelde “Gemeentelijk InformatiebeveiligingsBeleid”.
Deze nota is normstellend en zal worden uitgewerkt met concrete actiepunten in het jaarlijks bij te stellen informatiebeveiligingsplan.

Met dit “Gemeentelijk Informatiebeveiligingsbeleid 2014-2018” zet de gemeente de eerste stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente meer op orde te krijgen. Door in alle geledingen van de organisatie aandacht aan informatiebeveiliging te blijven schenken, kan de gemeente beter de veilige verwerking van gegevens van haar burgers en bedrijven gaan waarborgen.

Wat is informatiebeveiliging?
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politiek bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

Hoe gaan we dit realiseren?
De belangrijkste uitgangspunten bij het informatiebeveiligingsbeleid zijn:
- Het college van B&W is eindverantwoordelijk voor de informatiebeveiliging en stelt het informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast op basis van een risicoanalyse.
- De Chief Information Security Officer (CISO) heeft een onafhankelijke rol en rapporteert rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken. De onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in de auditplannen.
  De Information Security Officer (ISO) is geplaatst binnen M&S/IV en is verantwoordelijk voor de tactische en operationele aspecten van de informatiebeveiliging. De positie van de CISO en de ISO binnen de organisatie zal de komende periode nader worden bepaald.
- Het lijnmanagement is verantwoordelijk voor de uitvoering van de informatiebeveiliging.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement.

Belangrijke randvoorwaarden zijn:
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld, gebaseerd op een risicoanalyse.

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

De hoofdstukken 3 tot en met 12 geven een nadere invulling van het gemeentelijk informatiebeveiligingsbeleid, gebundeld in de onderstaande groepen:
H3. De organisatie van de informatiebeveiliging.
H4. Beheer van bedrijfsmiddelen.
H5. Beveiligingseisen ten aanzien van personeel.
H6. Fysieke beveiliging en beveiliging van de omgeving.
H7. Beheer van communicatie- en bedieningsprocessen
H8. Logische toegangsbeveiliging
H9. Verwerving, ontwikkeling en onderhoud van informatiesystemen.
H10. Beheer van informatiebeveiligingsincidenten.
H11. Bedrijfscontinuïteitsbeheer.
H12. Naleving.

1 Inleiding

1.1 Leeswijzer: de indeling van deze nota

Het doel van deze beleidsnota is het presenteren van het normstellend Informatie Beveiligings Beleid voor de jaren 2014 tot 2018. Deze nota vervangt de nota 'Gemeentelijk Informatiebeveiligingsbeleid' die in 2011 is vastgesteld.
De uitwerking in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan.

Na de inleiding in hoofdstuk 1 wordt in hoofdstuk 2 de kern van het beleid weergegeven. De daarop volgende hoofdstukken vormen een onlosmakelijk geheel met het informatiebeveiligingsbeleid van de gemeente. Deze hoofdstukken corresponderen met de hoofdstukken 5 tot en met 15 geven een nadere invulling van het gemeentelijk informatiebeveiligingsbeleid.
Op een aantal terreinen wordt nog niet aan de beleidseisen voldaan.
In het jaarlijks uit te brengen gemeentelijk Informatie Beveiligings Plan wordt worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.

1.1.1 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN/ISO 27001[1]. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN/ISO 27002[2] genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatie beveiligings beleid heeft de Informatie Beveiligings Dienst (IBD)[3] begin 2013 de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) uitgebracht, gebaseerd op NEN/ISO 27001 en 27002. Deze BIG bestaat uit een strategische en een tactische baseline. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.
De inhoud en structuur van deze nota zijn afgestemd op die van de BIG. Ook het Informatie Beveiligings Plan zal deze structuur volgen.

1.2 Wat is informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Het gaat hierbij over:

- Beschikbaarheid: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers:

[1] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor Informatiebeveiliging
[2] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[3] De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013.

Gegevens en functionaliteit dienen voor gebruikers zodanig beschikbaar te zijn dat zij hun taken optimaal kunnen uitvoeren.

- Integriteit: de mate waarin gegevens of functionaliteit juist ingevuld zijn:
  De juistheid van gegevens en functionaliteit dient te voldoen aan de daarvoor gestelde normen, wet- en regelgeving.
- Vertrouwelijkheid: de mate waarin de toegang tot (persoons)gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn:
  Toegang tot (persoons)gegevens en functionaliteit is beperkt tot degenen die daartoe door de eigenaar hiervan is vastgesteld.

Belangrijk hierbij is de controleerbaarheid van de maatregelen die genomen zijn om de betrouwbaarheid te borgen.

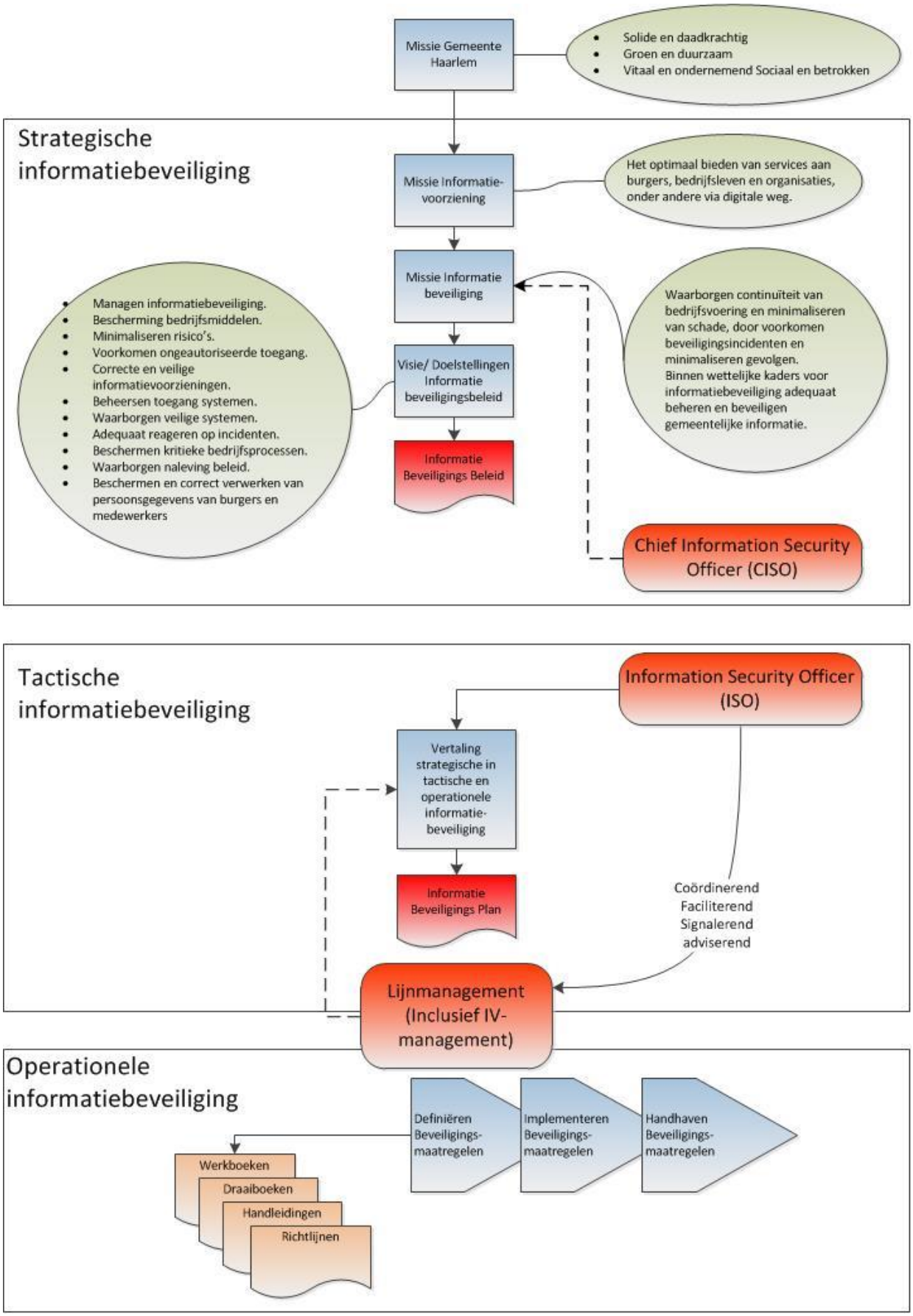
1.3 Waarom informatiebeveiliging?

Informatie, waaronder privacygevoelige gegevens, is één van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van vertrouwelijke en waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe vertrouwelijker of waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

1.4 De plaats van het Informatiebeveiligingsbeleid

Het beleid wordt gebruikt om middels informatiebeveiligingsplannen de vertaling te kunnen maken naar tactische en operationele richtlijnen en maatregelen, die zijn toegesneden op de taken en verantwoordelijkheden van de betrokken medewerkers.
Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. Deze worden uitgewerkt in het ‘Gemeentelijk Informatiebeveiligingsplan’.

De relatie tussen strategisch, tactisch en operationeel niveau wordt weergegeven in de volgende figuur.
Belangrijk daarin is het onderscheid tussen het Informatiebeveiligingsbeleid en het Informatiebeveiligingsplan.
De Chief Information Security Officer (CISO) ten aanzien van het strategische niveau en de Information Security Officer (ISO) ten aanzien van het tactische en operationele niveau zijn hierin centraal.


Missie Gemeente Haarlem
Solide en daadkrachtig
Groen en duurzaam
Vitaal en ondernemend Sociaal en betrokken
Strategische informatiebeveiliging
Missie Informatie-voorziening
Het optimaal bieden van services aan burgers, bedrijfsleven en organisaties, onder andere via digitale weg.
Missie Informatie beveiliging
Waarborgen continuïteit van bedrijfsvoering en minimaliseren van schade, door voorkomen beveiligingsincidenten en minimaliseren gevolgen. Binnen wettelijke kaders voor informatiebeveiliging adequaat beheren en beveiligen gemeentelijke informatie.
Managen informatiebeveiliging.
Bescherming bedrijfsmiddelen.
Minimaliseren risico's.
Voorkomen ongeautoriseerde toegang.
Correcte en veilige informatievoorzieningen.
Beheersen toegang systemen.
Waarborgen veilige systemen.
Adequaat reageren op incidenten.
Beschermen kritieke bedrijfsprocessen.
Waarborgen naleving beleid.
Beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers
Visie/ Doelstellingen Informatie beveiligingsbeleid
Informatie Beveiligings Beleid
Chief Information Security Officer (CISO)
Tactische informatiebeveiliging
Information Security Officer (ISO)
Vertaling strategische in tactische en operationele informatie-beveiliging
Informatie Beveiligings Plan
Coördinerend
Faciliterend
Signalerend
adviserend
Lijnmanagement (Inclusief IV-management)
Operationele informatiebeveiliging
Definiëren Beveiligings-maatregelen
Implementeren Beveiligings-maatregelen
Handhaven Beveiligings-maatregelen
Werkboeken
Draaiboeken
Handleidingen
Richtlijnen

1.5 De Scope van het informatiebeveiligingsbeleid

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit gemeentelijke IB-beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen (Bijvoorbeeld SUWI en gemeentelijke basisregistraties.).

1.6 Ontwikkelingen.

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

1.6.1 Management letter 2012

In de management letter 2012 van de accountant worden ten aanzien van de beveiliging van de IT-omgeving een aantal aanbevelingen gedaan:

- Het op orde brengen van (het proces rond) de gebruikersautorisaties.
- Het actualiseren van het beveiligingsbeleid.
- Het verhogen van het beveiligingsbewustzijn binnen de organisatie.
- Het integreren van de testprocedure in het wijzigingsbeheer.
- Het opstellen van een continuïteits- of herstelplan, met name voor kritieke systemen.

In het beleid, en vervolgens in de planning, zullen deze zaken een hoge prioriteit krijgen.

1.6.2 Informatiebeveiliging bij Regievoering, Regiovorming, Ketensamenwerking en basisregistraties.

In toenemende mate is sprake van informatiedeling met derden zoals uitvoeringsorganisaties en organisaties in een keten met hetzelfde kennisdomein. Bij het werken in regievorm, in regioverband en "in de keten" worden gemeentelijke gegevens verstrekt aan derden. Onder meer worden de gegevens uit de basisregistraties op een geautomatiseerde wijze verstrekt aan zowel interne afdelingen als aan derden.

1.6.3 Cloud computing

Cloud computing is het afnemen van IT services via het internet (zoals netwerken, servers, opslag, applicaties en diensten) Het afnemen van diensten uit de cloud vindt al plaats, zoals het gebruik van SUWI en RIS/BIS, en zal in de toekomst verder toenemen. Het gebruik van de cloud zal altijd weloverwogen moeten plaatsvinden. Met name voor wat betreft de vertrouwelijkheid van (persoons)gegevens is het op eigen initiatief opslaan hiervan in de cloud (zoals bijvoorbeeld in Dropbox) niet toegestaan.

1.6.4 Sociale media

Het gebruik van sociale media wordt steeds uitgebreider. Het gebruik door medewerkers van de gemeente Haarlem is toegestaan. De medewerkers dienen zich ervan bewust te zijn dat ze online gezien worden als vertegenwoordigers van de organisatie. Uitingen op het internet worden daarom beschouwd als gedaan door de organisatie, worden permanent opgeslagen en kunnen eventueel via andere media opnieuw worden gepubliceerd. Hiervoor bestaat een richtlijn ‘Gedragsregels Social Media gemeente Haarlem’.

1.6.5 Open data.

Open Data is overheidsinformatie die verzameld is in het kader van de uitvoering van een publieke taak en die openbaar beschikbaar wordt gesteld voor gebruik en bewerking. Zowel op

Europees, landelijk en gemeentelijk niveau zijn organisaties bezig data beschikbaar te stellen. Zo ook de gemeente Haarlem. Bij het beschikbaar stellen van deze informatie zal toetsing dienen plaats te vinden aan het informatiebeveiligingsbeleid.

1.6.6 Bedreigingen

ICT raakt steeds meer verweven in maatschappelijke processen en is daarmee een belangrijk deel van het maatschappelijke leven. Ook steeds meer apparatuur is verbonden met internet, van computers tot koelkasten en thermostaten. Dat er risico's kleven aan deze ontwikkelingen wordt steeds duidelijker, mede door diverse incidenten in het afgelopen jaar. ICT is vaak kwetsbaar.
Het Nationaal Cyber Security Centrum (NCSC) publiceert jaarlijks het Cybersecuritybeeld Nederland (CSBN). Het is bedoeld voor beleidsmakers van de overheid en vitale sectoren om inzicht te bieden in ontwikkelingen, ter beoordeling van mogelijke bedreigingen.

Een overzicht van de belangrijkste bedreigingen is weergegeven in het schema in Bijlage 3, afkomstig uit het CSBN-3 (april 2012 tot maart 2013).
Voor overheden is de grootste dreiging momenteel gericht op het belang van de vertrouwelijkheid van informatie (met name tegen spionage) en continuïteit van onlinedienstverlening (inclusief generieke voorzieningen) en eigen ICT. Deze dreiging komt uit verschillende hoeken: staten, beroepscriminelen, hacktivisten en cybervandalen/scriptkiddies.

2 Het informatiebeveiligingsbeleid

2.1 Uitgangspunten

Het bestuur en management speelt een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
Bij het opstellen, uitvoeren en/of handhaven van het beleid geldt:

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

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

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. **Het College van B&W is eindverantwoordelijke voor de informatiebeveiliging.**
2. De uitvoering van de informatiebeveiliging is een **verantwoordelijkheid van het lijnmanagement.** Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Haarlem hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
3. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
4. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.
5. De **Centrale informatiebeveiligingsfunctionaris/** Chief Information Security Officer (CISO) ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
   Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de

rapportage van de CISO.
De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
De **Information Security Officer** (ISO) vervult een centrale rol op tactisch en operationeel niveau.
De positie van CISO en ISO binnen de organisatie zal de komende periode nader worden bepaald.

6. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
7. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
8. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.2 Het informatiebeveiligingsbeleid in detail

De gemeentelijke missie ten aanzien van de informatievoorziening is het optimaal bieden van services aan burgers, bedrijfsleven en organisaties, onder andere via digitale weg.
Dit laatste om een groene en duurzame bedrijfsvoering te bevorderen.

De daarvan afgeleide missie ten aanzien van de informatiebeveiliging is het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade, door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen. Binnen de wettelijke kaders voor informatiebeveiliging zorgt de organisatie ervoor dat alle gemeentelijke informatie (van burger, bedrijfsleven en organisatie) adequaat wordt beheerd en beveiligd.

Het informatiebeveiligingsbeleid van de gemeente Haarlem heeft daarom als doel het realiseren van een optimaal beveiligde opslag en bewerking van informatie, en de daarvoor vereiste functionaliteit, die bij gemeentelijke processen betrokken is.

Dit resulteert in de volgende doelstellingen met specifieke aandachtspunten. Deze worden uitgewerkt in de hierna volgende hoofdstukken. Het informatiebeveiligingsbeleid van de gemeente Haarlem is gericht op:

- Het managen van de informatiebeveiliging (H3).
- Adequate bescherming van bedrijfsmiddelen (H4).
- Het minimaliseren van risico's van menselijke fouten, diefstal, fraude of misbruik (H5).
- Het voorkomen van ongeautoriseerde toegang tot de gebouwen en informatie(systemen) van de organisatie, die tot schade of verstoring kan leiden (H6).
- Het garanderen van correcte en veilige voorzieningen voor beheer en verstrekking van informatie (H7).
- Het beheersen van de toegang tot informatie en informatiesystemen (H8).
- Het waarborgen van veilige informatiesystemen (H9).
- Het adequaat kunnen reageren op (en het leren van) incidenten, bijna incidenten en gebreken (H10).

- Het reageren op verstoringen van bedrijfsactiviteiten en het beschermen van kritieke bedrijfsprocessen tegen de effecten van grootschalige storingen en calamiteiten (H11).
- Het waarborgen dat het informatiebeveiligingsbeleid wordt nageleefd, inclusief de hierop betrekking hebbende wetgeving (H12).

De uitwerking van dit beleid naar specifieke doelstellingen en tactische en operationele aspecten is te vinden in de volgende hoofdstukken.

2.3 Privacy en informatiebeveiliging

Gebruik van persoonsgegevens betekent: rekening houden met privacy.
In veel informatiesystemen, waaronder basisregistraties, beheert en verwerkt de gemeente persoonsgegevens. Dit zijn alle gegevens die te herleiden zijn tot een specifieke persoon. Deze specifieke persoon kan een burger zijn, maar ook een medewerker.
Maar de betreffende persoon heeft recht op privacy. Zorgvuldig gebruik van gegevens waarborgt de privacy van de burger of medewerker.
Deze moet de gemeente kunnen vertrouwen en heeft er recht op dat zijn/haar persoonsgegevens voldoende worden beveiligd tegen oneigenlijk of onrechtmatig gebruik.
Mede in het belang van de privacy van haar burgers en medewerkers dient de gemeente de informatiebeveiliging dan ook op orde te hebben.

Binnen de gemeente zijn de lijnmanagers (eind)verantwoordelijk voor:

- Behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de Wet Bescherming Persoonsgegevens (WBP).
- Adequate beveiliging van de beheerde en verwerkte persoonsgegevens.
  Deze beveiliging dient te worden getoetst aan de bepalingen, zoals deze zijn opgenomen in het gemeentelijk informatiebeveiligingsplan.
- Melding van verwerking van persoonsgegevens, indien nodig, bij het College Bescherming Persoonsgegevens.
- Afsluiten van een bewerkersovereenkomst met de bewerker, indien de verantwoordelijke persoonsgegevens laat verwerken door een bewerker
  (definitie bewerker volgens WBP: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen).

2.4 Planning en uitwerking informatiebeveiligingsbeleid

Het geactualiseerde informatiebeveiligingsbeleid is normstellend en zal worden uitgewerkt met concrete actiepunten in het jaarlijks bij te stellen informatiebeveiligingsplan.

Jaarlijks zullen de volgende zaken worden uitgevoerd:

- Bepalen waar de gemeente wel en waar de gemeente nog niet voldoet aan het nieuwe informatiebeveiligingsbeleid (een zogenaamde GAP-analyse).
- Aan de hand van deze analyse de risico's bepalen welke de gemeente loopt op het gebied van de informatiebeveiliging, bepalen waar extra beveiligingsmaatregelen nodig zijn en met welke prioriteit deze geïmplementeerd moeten worden.
- Al gerealiseerde en nog te nemen maatregelen uitwerken in een informatiebeveiligingsplan wat zal worden voorgelegd aan de directie.
- Ontbrekende beveiligingsmaatregelen op basis van prioriteit implementeren.

- Het actueel houden van het meldingenregister van het College Bescherming Persoonsgegevens ten aanzien van de verwerking van de persoonsgegevens.

3 De organisatie van de informatiebeveiliging

Risico's

- Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, verhindert het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.

Doelstelling:

Beheren van de informatiebeveiliging (IB) binnen de organisatie.

Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.

3.1 Afstemming met aanpalende beleidsterreinen

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij de gemeente Haarlem op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging, als aan fysieke beveiliging, ARBO-veiligheid en bedrijfscontinuïteit. Immers, samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor goed governance.

3.2 Organisatie van de informatiebeveiliging.

De verantwoordelijkheden in de informatiebeveiliging zijn als volgt verdeeld:

Wie	Verantwoordelijkheid	Toelichting
College van B en W (strategisch)	- Het vaststellen van het informatiebeveiligingsbeleid.	1 x in de vier jaar, tenzij noodzaak eerder.
Directie (strategisch en tactisch)	- Het vaststellen van de richtlijnen en maatregelen. Het vaststellen van het informatiebeveiligingsplan.	1 x per jaar
Chief Information Officer (CIO) (strategisch en tactisch)	- Geeft primair opdracht voor het Informatiebeveiligingsbeleid. - Geeft primair opdracht voor het Informatiebeveiligingsplan.	
Chief Information Security Officer (CISO) (strategisch)	- Het adviseren van de directie op het gebied van informatiebeveiliging. - Het opstellen van het informatiebeveiligingsbeleid. - Het toezien op naleving van het beleid. - Rechtstreeks rapporteren aan directie, voorafgaand aan P&C gesprekken.	Coördinerend, faciliterend, signalerend en adviserend. De rol van CISO is essentieel en centraal in de uitvoering van het informatiebeveiligingsbeleid

Wie	Verantwoordelijkheid	Toelichting
Information Security Officer (ISO) (tactisch en operationeel)	- Het adviseren van de directie op het gebied van informatiebeveiliging. - Opstellen informatiebeveiligingsplan. - De implementatie van het informatiebeveiligingsplan . - Het ondersteunen van het management. - Het opstellen van richtlijnen en maatregelen. - Het afhandelen van incidentmeldingen. - Het informeren van de directie over incidentmeldingen. -	De ISO is het dagelijkse aanspreekpunt voor de organisatie ten aanzien van de informatiebeveiliging.
Lijnmanagement (hoofdafdelings-manager, afdelingshoofd, bureauhoofd) (tactisch en operationeel)	- De leidinggevenden zijn verantwoordelijk voor de informatiebeveiliging binnen hun organisatie onderdeel. Zij dragen het beleid actief uit en zien er op toe dat het beleid wordt nageleefd. - Zij zijn verantwoordelijk voor de handhaving van de benodigde beveiliging van de informatiesystemen waarvan zij eigenaar zijn. Hieronder valt het opstellen en handhaven gedragscodes en richtlijnen hiervoor.	Ook de afdeling IV wordt hierbij gezien als lijnafdeling met eigen systemen en verantwoordelijkheden.
Medewerker/Gebruiker (operationeel)	- ledere medewerker is verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.	
Computer Security Incident Responce Team (CSIRT) (tactisch en operationeel)	- Het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij); - Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;	Samenstelling op ad hoc basis uit voorgeselecteerde groep.

3.3 De Security Officer

Centraal in de organisatorische opzet van de informatiebeveiliging staat de Chief Information Security Officer (CISO). Deze formuleert het informatiebeveiligingsbeleid in opdracht van de gemeentesecretaris. Ook stelt deze jaarlijks het informatiebeveiligingsplan op.
Deze functionaris coördineert de te treffen beveiligingsmaatregelen en het incidentproces, en adviseert de organisatie onafhankelijk op het gebied van de informatiebeveiliging. Daarnaast vervult deze een faciliterende en signalerende rol.

De Security Officer rapporteert rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de Security Officer.

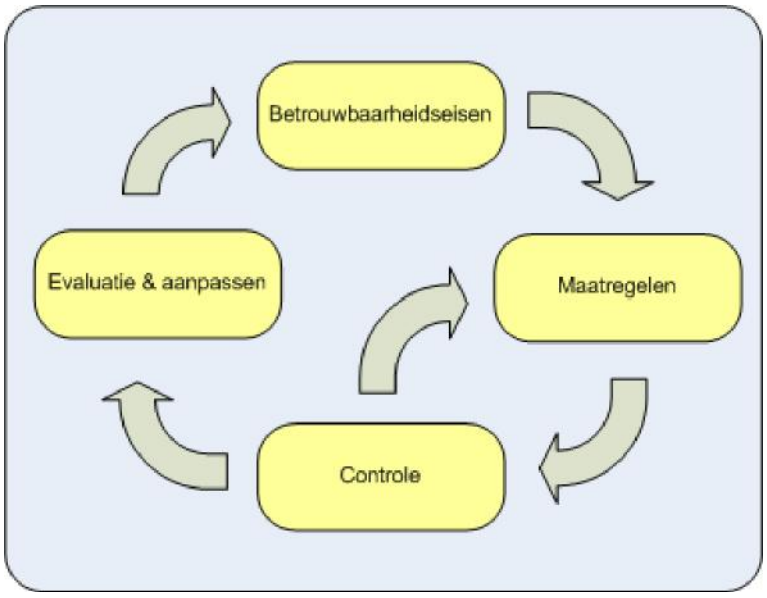
De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.

3.4 Verantwoordelijkheden lijnmanagement

Het lijnmanagement is verantwoordelijk voor de kwaliteit van de bedrijfsvoering en daardoor voor de beveiliging van informatiesystemen. Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot teamleider. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook verantwoordelijk voor informatiebeveiliging. Het begrip lijnmanagement wordt hierbij ruim opgevat. Ook het management van de afdeling IV valt hier onder en wordt dus verantwoordelijk wordt gesteld voor de beveiliging van de door de afdeling beheerde ICT-middelen. In voorkomende gevallen kan ook een afdelingshoofd of een manager van een stafafdeling onder het lijnmanagement worden verstaan.
Het lijnmanagement:

1. stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast.
2. is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
3. controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze maatregelen worden nageleefd.
4. evalueert periodiek de betrouwbaarheidseisen en stelt deze waar nodig bij.
5. rapporteert over de implementatie van de maatregelen in de management rapportages.

Er kan besloten worden om (delen van) de ontwikkeling, exploitatie of het onderhoud van informatiesystemen uit te besteden. Ook in deze gevallen blijft het lijnmanagement verantwoordelijk voor de beveiliging van het individuele systeem. Het lijnmanagement communiceert de betrouwbaarheidseisen van het systeem aan de derde partij. Via een schriftelijke overeenkomst, bijvoorbeeld een bewerkersovereenkomst of een Service Level Agreement wordt vastgelegd hoe de derde partij aan deze eisen gaat voldoen en tevens worden er consequenties verbonden aan het niet naleven van deze afspraken. Vanuit zijn hoedanigheid als verantwoordelijke partij, controleert het lijnmanagement of de werkzaamheden van de derde partij het vereiste betrouwbaarheidsniveau realiseren.



Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus (zie figuur). Na het vaststellen wat nodig is, worden maatregelen getroffen en gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau.

Door het beveiligingsbeleid op te nemen in de planning- en controlcyclus en hierover door de organisatieonderdelen verantwoording af te laten leggen door reguliere voortgangsrapportages, heeft beveiliging een duidelijke rol in de verticale sturingskolom van de gemeente. Over het functioneren van de informatiebeveiliging, de kwaliteitscirkel, wordt ook conform de planning- en controlcyclus binnen de gemeente en naar het college verantwoording afgelegd door het management.

Voor het ontwikkelen, bevorderen en onderhouden van kennis en verantwoordelijkheden ten aanzien van de informatiebeveiliging zullen voorlichtings- en scholingstrajecten worden aangeboden.

3.5 Financiën

Voor de realisatie van beveiligingsmaatregelen, ook bij vakafdelingen, zal in het informatiebeveiligingsplan jaarlijks een budget worden opgenomen. Voor 2014 is hiervoor € 50.000 beschikbaar.
Binnen ieder project zal een security check moeten worden uitgevoerd. Deze maakt onderdeel uit van de projectopzet en wordt van daar uit ook bekostigd. Er zijn in dit kader geen aanvullende (onderzoeks)budgetten beschikbaar.

3.6 Overleg

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen wordt in de gemeentelijke organisatie gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op vele niveaus.
Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt in het overleg tussen CISO, directie en concerncontroller.
Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg is per hoofdafdeling georganiseerd, met regelmatig centraal overleg.
Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan.
Voor alle drie de typen overleg geldt dat het zoveel mogelijk ingepast moet worden in bestaande overlegvormen met hetzelfde karakter. Zo zal op ieder niveau niet alleen over informatiebeveiliging gesproken worden, maar ook over andere risico's en maatregelen waarmee de organisatie te maken kan krijgen, zoals bijvoorbeeld financieel, juridisch en personeel.
Voor de opvang en bestrijding van calamiteiten wordt een Computer Security Incident Response Team (CSIRT) ingericht.

4 Beheer van bedrijfsmiddelen

4.1 Verantwoordelijkheid voor bedrijfsmiddelen

Risico's:

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

Doelstellingen

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

Beheersmaatregelen

- Alle bedrijfsmiddelen moeten geïdentificeerd zijn er moet een inventaris van worden bijgehouden.
- Alle informatie en bedrijfsmiddelen, die verband houden met ICT-voorzieningen aan een 'eigenaar' (een deel van de organisatie) toewijzen.
- Regels vaststellen, documenteren implementeren voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en gemeentelijke informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken gemeentelijke informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan.
- Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:
    - Illegale software mag niet worden gebruikt voor de uitvoering van het werk.
    - Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel.
    - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.
- De medewerker neemt passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
    - de beveiligingsclassificatie van de informatie (zie hieronder);

- de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
- aan de werkplek verbonden risico's;
- het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

4.2 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt.17 Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid.

Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

Risico's:

- Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de primaire processen.
- Onjuiste classificatie draagt bij aan het onjuist beschermen van informatie en bedrijfsmiddelen met als risico, dat deze verloren kunnen gaan of openbaar worden gemaakt terwijl dat niet de bedoeling is.

Doelstellingen

Informatie heeft een geschikt niveau van bescherming.

Classificatie van informatie om bij verwerking de noodzaak en bescherming te kunnen aangeven.

Adequate niveaus van bescherming van informatie zijn gedefinieerd en de noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.

Beheersmaatregelen:

- Informatie classificeren met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Opstellen en uitdragen classificatiebeleid binnen de gemeente.
- Er dienen geschikte samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de classificering en verwerking van informatie overeenkomstig het classificatiesysteem dat is vastgesteld.

De classificatie van informatie is weergegeven in onderstaande tabel:

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

Uitgangspunten

- De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.
- Het object van classificatie is informatie. We classificeren op het niveau van informatiesystemen (of informatieservices). Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de CISO en dienen jaarlijks gecontroleerd te worden door de eigenaren.
- Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn.
- De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen, wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt tevens wie toegang krijgt tot welke gegevens.
- Er wordt gestreefd naar een zo ‘laag’ mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar te zijn (transparante overheid).
- Er wordt gestreefd naar een balans tussen het te lopen risico en de kosten van tegenmaatregelen én daarnaast verdient een technische oplossing altijd de voorkeur boven gedragsverandering.

Toelichting
De te nemen maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Dit is vaak situatie afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het mitigeren van de risico's disproportioneel hoog zijn. Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

5 Beveiligingseisen ten aanzien van personeel

Risico's

- Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.

Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder voor vertrouwensfuncties.

Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

De gemeente Haarlem onderkent de belangrijke rol die de mens speelt in de informatiebeveiliging en treft daarom maatregelen bij het in dienst treden van de medewerker, tijdens het dienstverband en wanneer de medewerker uit dienst treedt. De gemeente onderscheidt hierbij de volgende groepen van medewerkers:
Interne medewerkers zijn alle personen die in tijdelijke of vaste dienst zijn bij de gemeente, of een daarmee vergelijkbare status hebben.
Externe medewerkers zijn niet in dienst van de gemeente, zij verrichten op regelmatige basis diensten voor de gemeente binnen de terreinen en gebouwen van de gemeente
Aangesloten derden zijn personen zoals ketenpartners of medewerkers van leveranciers, niet zijnde interne of externe medewerkers, die door middel van informatietechnologie toegang hebben tot de systemen van de gemeente. Ook medewerkers van uitvoerders van uitbestede gemeentelijke taken, zoals Cocensus, vallen hier onder, evenals die van een leverancier die een conversie uitvoert of een fout analyseert in een bestand.
Thuis-/Telewerkers zijn personen die de beschikking hebben over faciliteiten om het werk thuis, of elders, uit te voeren. Deze faciliteiten worden niet standaard aangeboden. Alleen wanneer dit voor de werkzaamheden absoluut noodzakelijk is wordt dit mogelijk gemaakt. Deze medewerkers worden beschouwd als interne medewerkers.

Soort medewerker	Moet zich houden aan het Informatie-beveiligingsbeleid, richtlijnen en maatregelen	Tekent integriteits-verklaring	Opmerkingen
Interne medewerker en thuis/telewerkers	Ja	Ja	Bij opzettelijk foutief handelen kunnen disciplinaire maatregelen worden genomen (zie ook ambtenarenreglement).

Externe medewerker	Ja	Ja	Geheimhouding wordt opgenomen in het contract met de leverancier.
Aangesloten derde	Ja	Nee	Geheimhouding wordt geregeld in de SLA.

Beheersmaatregelen:

- Meldingsplicht: Alle medewerkers zijn verplicht alle beveiligingsincidenten en waargenomen of vermoede zwakke plekken in de beveiliging zo snel mogelijk te melden (richtlijn incidentmelding).
- Adequate functiescheiding: Door middel van adequate functiescheiding worden risico's van menselijke fouten en eventueel opzettelijk misbruik van systemen verminderd.
- Verklaring omtrent gedrag: Er wordt standaard een verklaring omtrent gedrag gevraagd voor alle nieuwe medewerkers, ook die tijdelijk in dienst komen. Omdat stagiaires geen arbeidsrechtelijke dienstbetrekking hebben, geen werknemer zijn, en niet onder het ambtenarenrecht vallen, wordt van hen geen VOG gevraagd. Zij ondertekenen wel altijd een gedrags/integriteitsverklaring.
- Externe medewerkers: Externe medewerkers die toegang krijgen op onze technische infrastructuur moeten bekend zijn bij de gemeente Haarlem. Hun gegevens worden geregistreerd (in het personeelssysteem) zodat de controleerbaarheid van hun in- en uitstroom op onze technische infrastructuur gewaarborgd is. Zij dienen te voldoen aan de door ons gestelde beveiligingseisen.
- Controle, naleving en sancties: Bij de gemeente Haarlem initieert de Security Officer in samenwerking met de interne auditor de controle op de uitvoering van het informatiebeveiligingsjaarplan.
  De externe controle wordt uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.
  Steeds vaker is er ook sprake van branche audits, zoals die voor GBA, SUWI en BAG. De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen.
  De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat lijnmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wet Bescherming Persoonsgegevens (in het kader van de privacy) wordt een periodieke signalering uitgevoerd in overleg tussen de Security Officer en hoofd Juridische Zaken.
  Mocht de naleving ernstig tekort schieten, dan kan de organisatie de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
- Bewustwording en training: Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk is de mens altijd de belangrijkste speler. Daarom wordt binnen de organisatie kennis en bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn opleidingen voor degenen die daadwerkelijk met gegevensbeheer bezig zijn en regelmatig terugkerende bewustwordingscampagnes voor medewerkers en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en fysiek. Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van het management als de Security Officer; uiteindelijk is ook hiervoor het College van Burgemeester en Wethouders eindverantwoordelijk.
- Beveiligingsbewustzijn zal een standaard onderdeel van P-gesprekken worden.

- Indien een medewerker verplichtingen of voorschriften niet nakomt wordt gehandeld conform:
    - CAR hoofdstuk 15.
    - De “Nota Integriteit”.
    - De regeling “Bedrijfsrecherche: Richtlijnen inschakeling bedrijfsrecherche” (B&W besluit d.d. 11 mei 2004, gewijzigd bij B&W besluit d.d. 25-09-2007).

6 Fysieke beveiliging en beveiliging van de omgeving

Risico's

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet-medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
- Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico m.b.t. de vertrouwelijkheid.
- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

Doelstelling

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

ICT-voorzieningen,die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.

Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Beheersmaatregelen

- Alle objecten (gebouwen) van de gemeente krijgen op basis van generieke profielen een risicoprofiel toegewezen. Dit is het generieke risicoprofiel dat het beste aansluit bij het object.
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijgehouden.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).

- In diverse panden van de gemeente wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is beperkt door de Wet Bescherming Persoonsgegevens en nadere regels.
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel. Registratie van de verleende toegang ondersteunt de uitvoering van de toegangsregeling.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.
- (Data)verbindingen worden beschermd tegen interceptie of beschadiging.
- Reserve apparatuur en back-ups zijn gescheiden in twee locaties of datacenters, om de gevolgen van een calamiteit te minimaliseren.
- Gegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd. Informatie wordt bewaard en vernietigd conform de Archiefwet 1995 en de daaruit voortvloeiende archiefbesluiten.

7 Beheer van communicatie- en bedieningsprocessen

Risico's

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- De gemeente gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

Doelstelling

Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.

Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

Zowel het verkeerd gebruik van ICT-middelen als het niet goed oplossen van verstoringen kunnen grote gevolgen hebben voor de bedrijfsvoering en de dienstverlening. Daarom worden de verantwoordelijkheden voor het beheer van informatiesystemen en de verwerking van de informatie duidelijk beschreven. De gemeente Haarlem werkt conform de ITIL standaarden. Om de beschikbaarheid te waarborgen verloopt de invoering, of wijziging, van informatiesystemen volgens een vast proces.
Binnen de gemeentelijke organisatie zijn nog veel papieren informatiedragers in gebruik. Daarom dient ook het beheer van deze 'analoge' informatiedragers goed te zijn ingericht. Waar sprake is van informatie-uitwisseling dient ook met deze informatiedragers rekening te worden gehouden.
Ten aanzien van (documentair) informatiebeheer zijn de Archiefverordening en het Besluit Informatiebeheer bepalend.

7.1 Beheer

De verantwoordelijkheid voor het dagelijks beheer is als volgt belegd:

- De afdeling IV is verantwoordelijk voor het beheer van de technische infrastructuur (centrale computers, netwerken, PC's, patchkasten, telecommunicatie en bekabeling en communicatie met printers en MFC's).
- De afdeling FaZa is verantwoordelijk voor printers en MFC's.
- De afdeling IV is verantwoordelijk voor capaciteitsplanning, en speelt hierop in, zodat het risico van overbelasting wordt gereduceerd.
- De afdeling IV is verantwoordelijk voor het technisch applicatiebeheer voor alle systemen.
- De lijnafdelingen beheren, op functioneel niveau, hun eigen informatiesystemen (functioneel applicatiebeheer).
- De afdeling Facilitaire Zaken is verantwoordelijk voor het beheer van het toegangssysteem voor de gebouwen en het inbraakalarmsysteem.
- De afdeling Facilitaire Zaken/DIV is verantwoordelijk voor het beheer van analoge en digitale documenten en archiefbescheiden.

Hierbij geldt:

- De beheerwerkzaamheden worden gedocumenteerd.
- Kennis en ervaring worden gedeeld met collega's, daar waar nodig kan men een collega vervangen (m.n. bij kritieke processen bemensd door één persoon).
- Installaties van applicaties worden gedocumenteerd.
- IT-componenten (Configuratie items) worden vastgelegd in de Configuration Management DataBase (CMDB.)

7.2 Bestrijding malware

Haarlem neemt de volgende maatregelen om te voorkomen dat programma's en/of gegevens worden geïnfecteerd door malware:

- Alle ICT-apparatuur is voorzien van actuele anti-malware software.
- Alle gegevensdragers worden bij gebruik gecontroleerd op virussen.
- Indien een gebruiker een actief virus vermoedt dan geeft de gebruiker dit onverwijld door aan de servicedesk ICT.
- Waarschuwingen (het communiceren) over virussen, richting de organisatie, worden uitsluitend door afdeling IV en/of het Computer Security Incident Response Team (CSIRT) uitgebracht.

7.3 Beperking gegevensverlies

De beschikbaarheid van informatiesystemen en gegevens wordt geborgd door een adequate back-up strategie (dagelijkse aanmaak van reservekopieën van gegevens). Daarnaast dienen medewerkers adequate maatregelen te treffen om te voorkomen dat gegevens verloren gaan door menselijke fouten, storingen of opzettelijk handelen. Gegevens worden in principe niet opgeslagen op apparaten van eindgebruikers. In gevallen waarin dit nodig is, maken gebruikers een reservekopie.

7.4 Logging

Activiteiten van gebruikers en beheerders kunnen worden gelogd om problemen te kunnen oplossen, eventueel misbruik te kunnen detecteren en het gebruik van de systemen te analyseren (hiervoor dient de nota 'privacy reglement, gebruik e-mail en internet' te worden geactualiseerd).

7.5 Gegevensdragers

Gegevensdragers worden gebruikt voor het opslaan, bewaren of uitwisselen van software of gegevens. Voor een zorgvuldig gebruik hiervan, dient de richtlijn "Gebruik en Vernietiging Gegevensdragers" te worden uitgewerkt.

7.6 Beveiliging van mobiele apparatuur

Informatieverwerkende mobiele apparatuur moet zowel binnen als buiten het gebouw zo mogelijk fysiek beschermd worden. Voor het gebruik van deze apparatuur worden richtlijnen vastgesteld:

- Mobiele apparatuur en bijbehorende media mogen niet onbeheerd worden achtergelaten.
- Mobiele apparatuur moet worden beveiligd met toegangscodes en anti-malware software.
- Bij het verwerken van vertrouwelijke, privacygevoelige en/of kritische gegevens zijn aanvullende maatregelen getroffen passend bij het classificatieniveau, zoals encryptie.

7.7 Uitwisseling van informatie met externe partijen.

Bij Regievoering, Regiovorming, Ketensamenwerking en basisregistraties, maar ook incidenteel, worden over en weer gegevens verstrekt. Voor het uitwisselen van gegevens met externe partijen geldt:

- Het verstrekken van vertrouwelijke gegevens vindt plaats op grond van formele overeenkomsten. Hierbij worden afspraken gemaakt over informatiebeveiliging (de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van de systemen en gegevens) en de Wet Bescherming Persoonsgegevens WBP.
- Het niveau van beveiliging dient bij de externe partij minimaal gelijk te zijn aan het niveau dat de gemeente Haarlem hanteert.
- Het doel waarvoor gegevens door externe partijen mogen worden gebruik wordt vastgelegd.
- Als sprake is van structurele uitwisseling van gegevens, worden hiervoor procedures en richtlijnen opgesteld door de betreffende lijnmanager en de externe partij.
- Bij regiepartners wordt periodiek een informatiebeveiligings-audit uitgevoerd.
- Bij het transport (via internet of op externe gegevensdrager) vindt versleuteling van de gegevens plaats.

7.8 Internet (digitale dienstverlening en e-mail)

Haarlem neemt adequate technische en organisatorische maatregelen om risico's bij het gebruik van internet te ondervangen. De gemeente Haarlem zorgt onder andere voor:

- Afdoende afscherming van het netwerk.
- Het gebruik, bij vertrouwelijke informatie, van certificaten voor de identificatie van een partij waarmee op internet gecommuniceerd wordt en voor de versleuteling van de informatie.
- Een e-mail protocol voor de eigen medewerkers.
- Een internet protocol voor de eigen medewerkers.
- Een periodieke beveiligingstoets van de website door een externe partij.
- Adequate beveiliging van vertrouwelijke gegevens die over internet worden getransporteerd door het versleutelen van de gegevens.
- Het treffen van adequate beveiligingsmaatregelen bij het aanbieden van online diensten en de inzet van de meest actuele en passende voorzieningen.

7.9 Certificaten

Certificaten worden gebruikt voor de identificatie van een partij waarmee gecommuniceerd wordt en voor de versleuteling van gegevens.
De gemeente Haarlem hanteert twee soorten certificaten: de PKI-overheid certificaten (Public Key Infrastructure-overheid) en reguliere ssl certificaten. Hierbij geldt:

- Bij het uitwisselen van vertrouwelijke gegevens/informatie op internet kiest de gemeente voor certificaten die gebruik maken van technieken die op dat moment door de markt geadviseerd worden.

- Waar technisch mogelijk en relevant streven we naar het hoogste betrouwbaarheidsniveau.

7.10 Cloudcomputing

Met cloud computing wordt hardware en software via het internet aangeboden. Opslag in de cloud is een relatief nieuwe methode en brengt nieuwe risico's met zich mee, vooral wat betreft vertrouwelijkheid. Bij cloudcomputing dient aanvullend te worden voldaan aan de volgende informatiebeveiligingseisen:

- Met de aanbieder moet een overeenkomst worden afgesloten waarin
    - beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van de gegevens zijn gewaarborgd;
    - afspraken zijn opgenomen over de manier waarop bij contractbeëindiging de gegevens weer terug gaan naar de gemeente Haarlem, waarbij moet worden vastgelegd:
        - in welke vorm de gegevens worden teruggeleverd;
        - dat ook de relevante meta-gegevens worden teruggeleverd;
    - wordt gewaarborgd dat het eigenaarschap van en de zeggenschap over de gegevens altijd bij de gemeente Haarlem blijven.
- De gegevens in de cloudopslag zijn versleuteld.
- Gegevens worden bij transport over het internet versleuteld.
- Er wordt alleen gebruik gemaakt van diensten die voldoen aan en vallen onder de Nederlandse en/of Europese wetgeving, vooral ten behoeve van de privacy.

8 Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient te worden vastgesteld.[4] Logische ('digitale') toegang is gebaseerd op de classificatie van de informatie.

Risico's:
- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en/of een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

Doelstelling

Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.

Beleid ten aanzien van informatieverspreiding en autorisatie is van toepassing.

Uitgangspunten
- De eigenaar van de data is bevoegd toegang te verlenen.
- Er worden in de regel geen 'algemene' identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts.
- De gemeente maakt ,waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals DigiD, eHerkenning en toekomstig e-ID).

Logische toegangsbeveiliging voor systemen omvat het inrichten van de toegang tot informatiesystemen en onderdelen van de technische infrastructuur op zodanige wijze dat slechts geautoriseerde personen toegang tot deze systemen kunnen krijgen. De eigenaar van een informatiesysteem bepaalt wie toegang krijgt tot het informatiesysteem, gebaseerd op de functie of rol van de medewerker. Het toekennen en intrekken van toegangspermissies is onderdeel van de standaard procedure bij in-, uit- en doorstroming.

Gebruikers krijgen toegang tot gemeentelijke informatiesystemen door een authenticatie die is gebaseerd op een gebruikersnaam en wachtwoord. Toegang tot informatiesystemen van de Gemeente Haarlem vereist minimaal een gebruikersnaam en een wachtwoord. Iedereen die toegang krijgt tot de technische infrastructuur wordt geregistreerd (in het personeelsregistratiesysteem). Op basis van de gebruikersnaam moeten alle activiteiten op de IT-infrastructuur kunnen worden herleid naar die persoon. Activiteiten van de gebruikers kunnen worden gelogd om problemen te kunnen oplossen en eventueel misbruik te kunnen detecteren. Voor het gebruik van niet- persoonsgebonden gebruikersnamen zijn richtlijnen vastgesteld door het MT-IV. Deze uitzonderingen op de regel kunnen alleen met toestemming van de ISO worden toegestaan en moeten worden onderbouwd.

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

De gemeente hanteert richtlijnen voor:

- Authenticatie.
- auditing, logging en monitoring.
- beheer en gebruik wachtwoord.
- werkplekbeveiliging (clear screen en clear desk).
- thuis-/telewerkers.

9 Verwerving, ontwikkeling en onderhoud van informatiesystemen

Risico's:

- Wanneer bij verwerving, ontwikkeling en onderhoud van een informatiesysteem geen of onvoldoende rekening wordt gehouden met beveiligingsmaatregelen, is de kans groot dat het systeem onvoldoende beveiligd is.

Doelstelling

Het waarborgen van het in gebruik krijgen en houden van voldoende beveiligde informatiesystemen.

Bij verwerving, ontwikkeling en onderhoud van informatiesystemen wordt altijd rekening gehouden met een afdoende beveiliging. Alle beveiligingsaspecten (beleid, maatregelen en richtlijnen) inclusief uitwijkvoorzieningen worden nageleefd en goedgekeurd als onderdeel van het project. Er worden adequate maatregelen getroffen om de beschikbaarheid, de betrouwbaarheid en de vertrouwelijkheid te kunnen garanderen. Hiervoor zal een normenkader worden opgesteld. Vooruitlopend daarop is het document 'Algemene eisen aan applicaties' van kracht.
Verwerving, ontwikkeling en onderhoud worden op een veilige manier uitgevoerd. Om schade aan de bedrijfsvoering tot een minimum te beperken is strenge controle vereist bij implementatie. Er wordt in voldoende mate en zorgvuldig getest (adequaat testproces met professionele testomgevingen). Ook bij gebruik van testgegevens worden regels voor informatiebeveiliging gehanteerd. De eigenaar van het informatiesysteem is verantwoordelijk voor de acceptatie van het informatiesysteem en de handhaving van de betrouwbaarheid en de vertrouwelijkheid van de gegevens.

10 Beheer van informatiebeveiligingsincidenten

Risico's

- Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

Doelstelling

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

Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.

Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

10.1 Melding en afhandeling

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door de medewerkers en andere betrokkenen gemeld worden en de wijze waarop deze worden afgehandeld.
Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. De sevicedesk ICT functioneert als meldpunt voor incidenten. Indien een incident zeer vertrouwelijk is, dient rechtstreeks contact te worden gezocht met de ISO.
Elke medewerker is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De medewerker dient de incidenten en inbreuken direct te melden aan het de servicedesk ICT, waarna de ISO wordt ingeschakeld.
De incidenten worden op een dusdanige manier geregistreerd dat een objectieve vergelijking met andere incidenten mogelijk wordt. Omdat deze potentieel gevoelige informatie bevat, is het incidentenregister slechts toegankelijk voor een beperkte groep medewerkers.
De incidenten worden afgehandeld en dienen als input voor de incident-rapportages. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne. In dit kader levert de ISO managementrapportages aan directieteam over de beveiligingsincidenten en doet voorstellen tot betere preventie of het verhelpen van incidenten.

10.2 Computer Security Incident Response Team (CSIRT)

Het doel van het CERT bij gemeente Haarlem is organisatiebrede preventie en verhelpen van informatiebeveiligingsincidenten.

Het gemeentelijk CSIRT bestaat uit een groep medewerkers die kennis hebben van de gemeentelijke organisatie, de informatievoorziening en/of informatiebeveiliging. Afhankelijk van de aard van een incident stelt de security officer hieruit een ad-hoc team samen.
Het team analyseert het incident en zorgt voor een adequate oplossing. De security officer is verantwoordelijk voor het functioneren van dit team. In het kader hiervan is het CSIRT gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.
Na signalering van een beveiligingsincident kan de ISO een CSIRT bij elkaar roepen. Dit team coördineert de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij). Dit escalatieproces zal door CISO, ISO en CIO worden ingericht.
Leden van het CSIRT kunnen ook ingeschakeld worden bij het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers.

11 Bedrijfscontinuïteitsbeheer

Risico's

- Wanneer er niet of nauwelijks invulling gegeven wordt aan de continuïteitsplanning is er naast een vals gevoel van veiligheid, ook grote kans op ad hoc maatregelen als een calamiteit zich voordoet.
- Het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

Doelstelling

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

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

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

- De organisatie heeft voor elke afdeling heeft een eigen plan voor bedrijfscontinuïteitsbeheer. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
    - Risico's;
    - (Wettelijke) regels ten aanzien van het herstel van het bedrijfsproces.
    - Identificatie van essentiële procedures voor bedrijfscontinuïteit;
    - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
    - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
    - Prioriteiten en volgorde van herstel en reconstructie;
    - Documentatie van systemen en processen;
    - Kennis en kundigheid van personeel om de processen weer op te starten.
- Er worden minimaal jaarlijks oefeningen of testen gehouden om de plannen voor bedrijfscontinuïteitsbeheer te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

12 Naleving

Risico's

- Het schenden van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen.

Doelstelling

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen.

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de Wet Bescherming Persoonsgegevens (WBP), die een belangrijke rol speelt in de bescherming van de persoonlijke levenssfeer (privacy). De gemeente dient zich aan al deze wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging.
Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De WBP regelt in artikel 13 welke maatregelen organisaties moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft de gemeente is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 16 van de WBP. Vooral aan de uitvoering van de WBP zal veel aandacht moeten worden besteed.
Deze maatregelen maken deel uit van het informatiebeveiligingsbeleid van een gemeente.
Wetten en regelingen die van belang zijn voor de informatiebeveiliging zijn (niet limitatief):

- Wet Bescherming Persoonsregistratie en Vrijstellingsbesluit (WBP)
- Wet Openbaarheid van Bestuur (WOB)
- Wet Computercriminaliteit
- Comptabiliteitswet
- Archiefwet
- Wet Veiligheidsonderzoeken (WVO)
- Ambtenarenwet en regelgeving (CAR-UWO)
- Beveiligingsvoorschrift 2005 (BVR)
- PUN (Paspoort Uitvoeringsregeling Nederland)
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2O1O)
- Programma van Eisen PKI Overheid
- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Wet SUWI
- Wet op de identificatieplicht
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet GBA en wet BRP
- Wet Werk en Bijstand
- Algemene wet bestuursrecht
- Richtlijnen van het NCSC (Nationaal Cyber Security Centrum) en IBD (Informatie Beveiligings Dienst)

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

controle op de naleving van wet en regelgeving is belegd bij het lijnmanagement en bij in- en externe auditors.
Aanvullend worden maatregelen geënt op de Strategische en Tactische Baselines van de Informatie Beveiligings Dienst (IBD).

Bijlage 1. Interne documenten informatiebeveiliging

In het kader van informatiebeveiliging zijn voor de organisatie de volgende documenten van belang:

12.1.1 Het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de organisatie. In het informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie er naar handelt wordt het uitgedragen door (of namens) het College van Burgemeester en Wethouders. Het informatiebeveiligingsbeleid wordt opgesteld door de CISO en vastgesteld door het College.

12.1.2 Informatiebeveiligingsplan met basisniveau van maatregelen

Dit plan beschrijft de maatregelen die minimaal nodig zijn om organisatiebreed een adequaat niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn. Deze zijn gebaseerd op een GAP- en risicoanalyse die voor de organisatie is uitgevoerd, overeenkomstig de BIG[5]. Deze basismaatregelen dienen dus overal in de organisatie genomen te worden. De baseline wordt door de CISO ter goedkeuring aangeboden aan de directie.
Wanneer er systemen zijn die na een risicoanalyse hogere beveiligingseisen nodig hebben, dan worden deze bovenop de basismaatregelen genomen.
Voor een aantal informatiesystemen is een eigen aanvullend beveiligingsplan vereist, bijvoorbeeld op wettelijke gronden.
Onderdeel van het informatiebeveiligingsplan is het Jaarplan en –verslag.
Ieder jaar levert de ISO een jaarverslag en een jaarplan voor het volgende jaar op. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles en audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan decentrale systemen.

12.1.3 Continuïteits- en Uitwijkplan

Voor het uitvoeren van de gemeentelijke taken is de organisatie steeds meer afhankelijk van digitale informatiesystemen. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Voor een doeltreffende uitwijkvoorziening is het nodig vooraf de beschikking te hebben over een draaiboek voor de uitwijkoperatie.
Het uitwijkplan wordt opgesteld door het hoofd IV in samenwerking met de systeemeigenaren en het hoofd Facilitaire Zaken.

12.1.4 Diensten niveau overeenkomsten (SLA's)

Een service level agreement is een overeenkomst tussen een leverancier en een afnemer. Bijvoorbeeld de afdeling IV sluit met interne afnemers (en externe leveranciers) een SLA af t.b.v. de ondersteuning van informatiesystemen. Dat zijn contracten met afspraken en randvoorwaarden over geleverde diensten. In deze contracten zit standaard een

[5] Baseline Informatiebeveiliging Nederlandse Gemeenten

informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier en afnemer zijn opgenomen. Een leverancier dient akkoord te gaan met het informatiebeveiligingsbeleid van de gemeente.

12.1.5 Inhuur- en uitbestedingscontracten

Bij de inhuur van diensten en personeel van derde partijen zal ook aandacht aan informatiebeveiliging besteed moeten worden, bijvoorbeeld door te stellen dat het gemeentelijk beleid ook van toepassing is voor hen. Hetzelfde is van belang bij uitbestedingen.

12.1.6 Gedragscodes en richtlijnen

Gedragscodes en richtlijnen voor medewerkers en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Deze richtlijnen sturen direct het operationele niveau aan en zullen daarom steeds actueel gehouden moeten worden. In het informatiebeveiligingsplan zal worden aangegeven wanneer welke richtlijn moet worden gepresenteerd. De richtlijnen zijn gericht op de totale informatiebeveiliging en niet alleen op de digitale kant daarvan.
De belangrijkste richtlijnen zijn:

- Gedragscode voor veilig e-mail en internetgebruik.
- Gebruik sociale media.
- Veilig gebruik mobiele devices.
- Wachtwoordbeleid.
- Classificatierichtlijnen voor gevoeligheid van gegevens
- Clear screen en clear desk-policy

Bijlage 2. Gebruikte documenten

Bij het opstellen van deze nota zijn de volgende documenten geraadpleegd:

1) NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor Informatiebeveiliging
2) NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
3) Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten; mei 2013; versie 1.0; IBD/KING
4) Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten; mei 2013; versie1.0; IBD/KING
5) Voorbeeld Informatie Beveiligings Beleid Gemeenten; 2013; IBD/KING
6) Cybersecuritybeeld Nederland; CSBN-3; uitgave van het Nationaal Cyber Cecurity Centrum.
7) Gemeentelijk InformatiebeveiligingsBeleid 2011
8) Directienota: ‘Acties naar aanleiding van de management letter 2012 van Pwc en de uitkomsten uit de financial audit op de hard close per 30 september.’, Concerncontrol.
9) Model Informatiebeveiligingsbeleid van het Hoger Onderwijs.
10) Gemeente Amersfoort: Informatiebeveiligingsbeleid 2012-2015

Bijlage 3. Bedreigingen.

Dreigingen vanuit verschillende actoren ten aanzien van verschillende doelwitten.

Doelwitten			
Actoren (dreigers)	**Overheden**	**Private organisaties**	**Burgers**
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Verstoring ICT (inzet offensieve capaciteiten) ★	Verstoring ICT (inzet offensieve capaciteiten) ★	
Terroristen	Verstoring ICT	Verstoring ICT	
(Beroeps)criminelen	Diefstal en verkoop van informatie ★	Diefstal en verkoop van informatie ★	Diefstal en verkoop van informatie ★
	Manipulatie van informatie ★	Manipulatie van informatie ★	Manipulatie van informatie ★
	Verstoring ICT	Verstoring ICT ⇧	
	Overname ICT	Overname ICT	Overname ICT
Cybervandalen en Scriptkiddies	Diefstal en publicatie van informatie ★	Diefstal en publicatie van informatie ★	Diefstal en publicatie van informatie ★
	Verstoring ICT	Verstoring ICT	
		Overname ICT ★	
Hacktivisten	Diefstal en publicatie van informatie ⇩	Diefstal en publicatie van informatie ⇩	Diefstal en publicatie van informatie ⇩
	Verstoring ICT	Verstoring ICT	Verstoring ICT ⇩
		Overname ICT ★	
	Digitale bekladding ★	Digitale bekladding ★	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie (chantage)	
	Verstoring ICT ★	Verstoring ICT ★	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private organisaties		Diefstal van informatie (bedrijfsspionage) ⇧	
Geen actor	Uitval ICT ⇩	Uitval ICT ⇩	Uitval ICT ⇩

Tabel 4. Overzicht dreigingen en doelwitten

Legenda relevantie		
Laag	**Midden**	**Hoog**
Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat. **OF** Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. **OF** Er hebben zich geen noemenswaardige incidenten van de dreiging voorgedaan in de rapportageperiode	Er worden nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat. **OF** Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. **OF** Incidenten hebben zich voorgedaan buiten Nederland, enkele kleine in Nederland.	Er zijn duideljke ontwikkelingen die de dreiging opportuun maken. **OF** Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. **OF** Incidenten hebben zich voorgedaan in Nederland.

Legenda wijzigingen: ⇧ dreiging is toegenomen ⇩ dreiging is afgenomen ★ dreiging/regel is nieuw

Uit: “Cybersecuritybeeld Nederland”; CSBN-3; uitgave van het Nationaal Cyber Cecurity Centrum.

Voor overheden is de grootste dreiging momenteel gericht op het belang van de vertrouwelijkheid van informatie (met name tegen spionage) en continuïteit van onlinedienstverlening (inclusief generieke voorzieningen) en eigen ICT. Deze dreiging komt uit verschillende hoeken: staten, beroepscriminelen, hacktivisten en cybervandalen/scriptkiddies.