gemeente Hoeksche Waard

GEMEENTEBLAD

Officiële uitgave van de gemeente Hoeksche Waard

Nr. 74886

29 maart 2019

Besluit van het college van burgemeester en wethouders houdende regels omtrent Strategisch Informatiebeveiligingsbeleid Hoeksche Waard 2019-2020

1 Samenvatting

1.1 Inleiding

Het document "Strategisch Informatiebeveiligingsbeleid gemeente Hoeksche Waard 2019-2020" en het document "Tactische Richtlijnen Informatiebeveiliging Hoeksche Waard", vormen gezamenlijk het nieuwe gemeentelijk beleid voor informatiebeveiliging. Het is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), conform de VNG resolutie (nov 2013) “Informatieveiligheid, randvoorwaarde voor de professionele gemeente”. De periode 2019-2020 is bewust gekozen in verband met de invoering van de Baseline Informatieveiligheid Overheid (BIO) in 2020.

1.2 Werking

- In dit document "Strategisch Informatiebeveiligingsbeleid Hoeksche Waard 2019-2020" worden de strategische uitgangspunten en verantwoordelijkheden ten aanzien van de gemeente op het gebied van informatiebeveiliging en gegevensbescherming benoemd, welke als basis dienen voor Tactische Richtlijnen (zie onder).
- Dit Strategisch Informatiebeveiligingsbeleid treedt in werking na vaststelling door het College van B&W, en is geldig tot eind 2020.

Figuur 1. Relatie Strategisch Informatiebeveiligingsbeleid en Tactische Richtlijnen

- In een separaat document "Tactische Richtlijnen Informatiebeveiliging Hoeksche Waard", wordt volgens internationale standaarden (NEN/ISO 27002:2005/7 en BIG) het inhoudelijke normenkader beschreven. Hierin staan de normen en maatregelen ten behoeve van risicomanagement en controle die op basis van “Compy-or-Explain” gelden voor alle organisatieonderdelen van de gemeente Hoeksche Waard.
- De "Tactische Richtlijnen Informatiebeveiliging Hoeksche Waard" treedt in werking na vaststelling door de Directie.

2 Uitgangspunten Informatiebeveiliging

2.1 Het belang van informatie

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente Hoeksche Waard voor het voldoen aan wetgeving en realiseren van primaire bedrijfsdoelstellingen zoals:

- klantgericht werken;
- efficiënte interne- en ketensamenwerking;
- integrale sturing op bedrijfsvoering;
- zaak en procesgericht werken;
- eenmalige opslag en uitvraag;
- openstelling van informatie;
- kostenreductie.

De betrouwbaarheid (beschikbaarheid, integriteit) van informatiesystemen en vertrouwen in informatie (privacy, controleerbaarheid) zijn dan ook van groot belang. Ook burgers, bedrijven en ketenpartners verwachten betrouwbare informatie.

2.2 Risico's

Door digitalisering van informatie wordt de gemeente steeds meer afhankelijk van betrouwbaarheid van informatiesystemen en vertrouwelijkheid van informatie. Door schaalvergroting en samenwerking in ketenautomatisering neemt de kans op, en de impact van incidenten toe.
De gemeente en ketenpartners lopen bedrijfsrisico's bij verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie. Dat kan ernstige gevolgen hebben voor burgers, bedrijven, partners en de eigen organisatie met eventueel politieke consequenties:

- het imago van de gemeente als betrouwbare leverancier wordt aangetast;
- maatschappelijke consequenties rond decentralisaties en verzelfstandigingen;
- kosten en werkzaamheden voor herstel;
- juridische en wettelijke consequenties, zoals aansprakelijkheid voor schade door fouten in verwerking en beheer van privacygevoelige informatie;
- fraude als gevolg onvoldoende beveiliging;
- managementbeslissingen worden beïnvloed door onbetrouwbare gegevens.

2.3 Doel

Dit Strategisch Informatiebeveiligingsbeleid is het kader voor passende organisatorische en technische maatregelen om gemeentelijke informatie te beschermen en te waarborgen dat de gemeente haar bedrijfsdoelstellingen met digitalisering kan realiseren, en voldoet aan relevante wet- en regelgeving. Om de risico's voor de bedrijfsvoering te verminderen worden deze voorafgaande aan veranderingen in informatiesystemen beoordeeld, en waar nodig met maatregelen beheerst.
De gemeente Hoeksche Waard streeft er naar om op preventieve wijze 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen aan College en Raad.

2.4 Doelgroepen

Het Strategisch Informatiebeveiligingsbeleid is bedoeld voor alle medewerkers en ketenpartners van de gemeente:

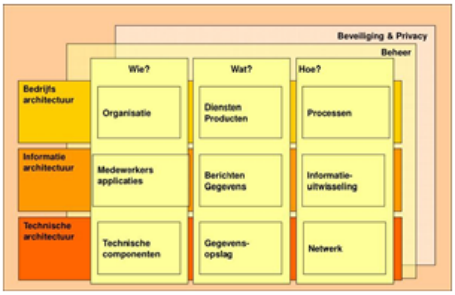
Doelgroep gemeente Hoeksche Waard	**Relevantie voor Informatiebeveiliging**
College van B&W	Integrale verantwoordelijkheid
Directie	Kaderstelling Strategisch IB beleid
Lijnmanagement en proceseigenaren	Sturing op risico's van informatie en controle op naleving van Tactische Richtlijnen
Beleidmakers	Planvorming binnen Strategisch kaders
Gegevenseigenaren	Via classificatie bepalen van beschermingseisen van informative
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT dienstverlening	Technische en Applicatie beveiliging
Medewerkers	Gedrag en naleving
Informatiebeveiligingsfunctionarissen	Dagelijkse coördinatie van Informatiebeveiliging

Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Aantoonbaar voldoen aan eisen en richtlijnen

Tabel 1: Doelgroepen

2.5 Scope

- De scope van dit Informatiebeveiligingsbeleid betreft genoemde doelgroepen die voor een bepaald doel informatie verwerken door middel van informatiesystemen in een gemeentelijke context.



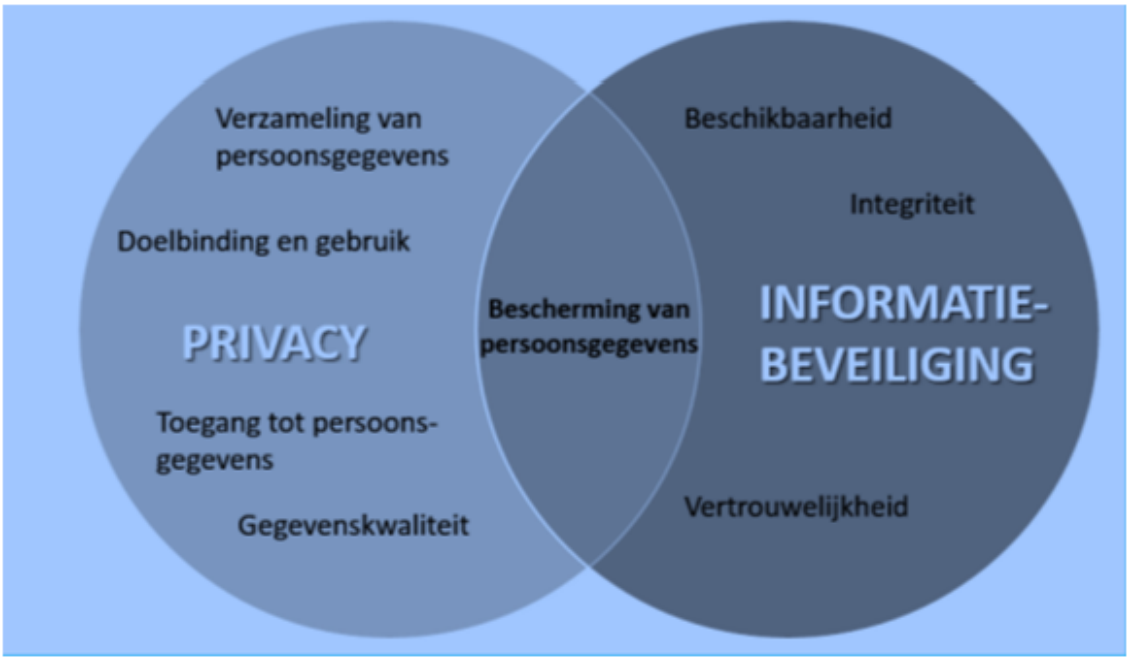
(Figuur 2: Scope op NORA raamwerk)

- In de "Tactische Richtlijnen Informatiebeveiliging Hoeksche Waard " zijn de volgende onderwerpen uitgewerkt:
  1. Beheer van bedrijfsmiddelen en classificatie;
  2. Beveiliging van personeel;
  3. Fysieke beveiliging en beveiliging van de omgeving;
  4. Beheer van communicatie- en bedieningsprocessen;
  5. Logische Toegangsbeveiliging;
  6. Verwerving, ontwikkeling en onderhoud van informatiesystemen;
  7. Beheer van informatiebeveiligingsincidenten;
  8. Bedrijfscontinuïteitsbeheer;
  9. Naleving en auditing.

- Dit Strategisch Informatiebeveiligingsbeleid is een basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.
- Het Strategisch Informatiebeveiligingsbeleid biedt geen afdoende bescherming tegen terrorisme, gericht hacktivisme of spionage van (vreemde) mogendheden. Risico's van dergelijke dreigingen kunnen indien van toepassing met een KWAS (Kwetsbaarheid Analyse Spionage) worden beoordeeld.

2.6 Samenhang Informatiebeveiligingsbeleid met Privacybeleid

Er is een nauwe samenhang tussen de bescherming van persoonsgegevens en informatiebeveiliging. De Functionaris Gegevensbescherming (FG) heeft onder meer als taken het toezien op naleving van privacywetgeving en adviseren over het beschermen en het borgen van een juiste verwerking van persoonsgegevens in werkprocessen conform de wetgeving.
De CISO (Chief Information Security Officer) bevordert en adviseert gevraagd en ongevraagd over Informatiebeveiliging aan de directie en rapporteert volgens de gebruikelijke P&C cyclus concernbreed aan de directie over de risico’s, veranderingen in controlemaatregelen en planning.



2.7 Uitgangspunten

- Het Hoeksche Waardse Informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en relevante landelijke en Europese wet en regelgeving.
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de daaruit afgeleide Strategische en Tactische Richtlijnen Informatiebeveiliging (KING, VNG).
- De aanpak van informatiebeveiliging in Hoeksche Waard is 'risk based', dat houdt in dat beveiligingsmaatregelen worden getroffen op basis van een risicoanalyse en informatieclassificatie.
- Dit Strategisch Informatiebeveiligingsbeleid is vastgesteld door het College van B&W. Het definieert uitgangspunten, verantwoordelijkheden en proces voor Informatiebeveiliging.
- Het College van B&W is eindverantwoordelijk voor informatiebeveiliging.
- Elke lijnmanager beoordeelt met behulp van bedrijfsrisicoanalyses welke mensen en middelen nodig zijn om zijn werkprocessen en eigendommen aantoonbaar te kunnen beveiligen volgens dit beleid met behulp van de Tactische Richtlijnen Informatiebeveiliging, advies en coördinatie van CISO.

- Iedere medewerker, zowel vast als tijdelijk, intern of extern gaat zorgvuldig om met gemeentelijke informatie en beschermt gegevens en informatiesystemen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en wordt gestimuleerd bij vermeende inbreuken hiervan melding te maken.
- Kennis en expertise zijn essentieel voor een toekomstvaste Informatiebeveiliging en moeten geborgd worden. Alle medewerkers van de gemeente worden getraind in bewustwording voor informatiebeveiliging en het gebruik van beveiligingsprocedures.
- Kwaliteit van de informatievoorziening wordt verankerd binnen de organisatie door jaarlijkse controle volgens het ENSIA principe (Eenvoudige Normatiek Single Informatie Audit), organisatie brede planning én coördinatie. De plannen worden periodiek geëvalueerd en zo nodig bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.
- Efficiëntie wordt bereikt door standaardisatie. Informatiebeveiliging voor generieke informatiesystemen gaat uit van een basisniveau zoals beschreven in de "Tactische Richtlijnen Informatiebeveiliging" en voegt beveiliging in meerdere lagen toe al naar gelang van de geïdentificeerde bedrijfsrisico's.

3 Visie op informatiebeveiliging

Een **betrouwbare** informatievoorziening is noodzakelijk voor het goed functioneren van de bedrijfsprocessen van de gemeente en de basis voor het verwerken van **vertrouwelijke gegevens** ter bescherming van **privacy** en rechten van burgers. Dit vereist een **integrale aanpak**, goed opdrachtgeverschap en **risicobewustzijn**.
Ieder organisatieonderdeel is hierbij betrokken. De komende jaren zet de gemeente Hoeksche Waard in op verbeteren van informatiebeveiliging en verdere professionalisering van de Informatie beveiligingsfunctie in de organisatie.

Betrouwbaar: Vitale maatschappelijke functies worden ondersteund door informatie en ICT. Risicoanalyses en normstelling rond betrouwbaarheid van gemeentelijke informatiesystemen verankeren de gewenste kwaliteit in bedrijfsprocessen en producten door toepassen van de best passende maatregelen. Het datacenter van gemeente Hoeksche Waard maakt elektronische dienstverlening op hoog niveau mogelijk door innovatieve manieren van werken zoals virtueel werken via Citrix en BYOD (Bring Your Own Device).

Vertrouwelijke gegevens en Privacy: Informatiebeveiliging gaat ook over vertrouwen in de bescherming van informatie in de persoonlijke levenssfeer (privacy) zoals vastgelegd in het Privacybeleid. Privacygevoeligheid van gegevensverzamelingen wordt door de eigenaar op de bedrijfslaag vastgesteld door middel van informatie classificatie en zo nodig getoetst met een Privacy Impact Analyses (PIA) en een beschrijving van doelbinding. Dit geeft richting en inhoud aan maatregelen op de informatielaag zoals persoonlijk gedefinieerde toegangsbeveiliging. De resultaten worden aantoonbaar gemaakt via reguliere audits en transparant gerapporteerd aan betrokkenen.

Integrale aanpak en samenwerking: Informatiebeveiliging vereist een integrale aanpak, zowel binnen de gemeente als voor overheidsbrede gemeenschappelijke voorzieningen (inclusief ketenpartners). Intern vindt overleg plaats met vertegenwoordigers van het Privacy & Informatieveiligheidsteam (PIV), Architecten, Directie, Interne Controle, Juridische Zaken, OOV, HRM, Teammanagers en Privacy Officers. Tevens is de gemeente Hoeksche Waard aangesloten bij de landelijke Informatie Beveiligingsdienst (IBD).

Risicobewustzijn
Informatiebeveiliging vereist goed opdrachtgeverschap, coördinatie en 'bewustzijn'.
Verantwoord en bewust gedrag van directie, medewerkers, ketenpartners en leveranciers is essentieel voor een goede informatiebeveiliging.

3.1 Visie op ontwikkelingen
De volgende ontwikkelingen zijn van invloed op Informatiebeveiliging:

3.1.1 Interne uitgangspunten op veiligheid
Risicobeheersing:
- risico's worden onderkend en waar nodig beheerst, zonder aan bedrijfsdoelstellingen tekort te doen. Beveiliging wordt mede geborgd door processclassificatie, detectie van afwijkingen en incident-en changemanagement.

Privacy:
- Hoeksche Waard beschermt de privacy van haar inwoners, en medewerkers.
- privacy aspecten moeten in digitale diensten en ontwikkelingen expliciet worden meegewogen en aan de wet getoetst via een Privacy Impact Analyse (PIA) en controle op de doelbinding.

Publieksdienstverlening en Digitalisering:
- waarmee burgers eenvoudig op digitale wijze hun aanvragen en vergunningen indienen en Hoeksche Waard deze digitaal verwerkt via "Papierarm en Zaakgericht werken".
- kernwaarden (betrouwbaarheid en vertrouwen) van informatie en systemen moeten zijn afgestemd op de vraag en behoefte van klanten en bedrijfsprocessen.

Proces optimalisatie:
- generiek beleid waar het kan, specifiek beleid waar het moet. Dit helpt de auditlast verminderen.
- organisatieonderdelen maken maximaal gebruik van de Tactische Richtlijnen, en wijken af als de wet dat voorschrijft.

Informatie is Open, tenzij…:
- het gaat over Vertrouwelijkheid (mate van toegang) tot informatie.
- de wet, classificatie of de eigenaar anders bepalen;
- classificatie onderscheid maakt tussen “Intern Open” en “Publiek Open” informatie;
- betrouwbaarheid (Beschikbaarheid en Integriteit -kans op onjuistheden) beschermd moet worden om ongeautoriseerde modificatie te voorkomen.

100% veiligheid bestaat niet:
- Bedrijfs Impact Analyse (BIA) en risicoanalyse zijn leidend om de benodigde beveiligingsmaatregelen expliciet vast te stellen.

3.1.2 Externe ontwikkelingen

Ketensamenwerking en decentralisaties van bedrijfsonderdelen vragen om steeds intensievere samenwerking tussen keten- en netwerkpartners. Hierdoor is er een toenemende uitwisseling van gegevens en informatie.
- externe en samenwerkende diensten voldoen meetbaar aan gemeentelijke standaarden, wat de gehele keten versterkt.
- informatie wordt zoveel mogelijk aan de bron beschermd, oa. d.m.v. classificatie en daarbij passende maatregelen bij opslag en transport van gegevens.
- koppelingen met informatiesystemen worden onder Architectuur gedefinieerd en beveiligd om een toenemend aantal koppelingen met leveranciers en ketenpartners te beheersen
- Hoeksche Waard zet in op verbetering van beheer van interne en externe identiteiten.

Cloud computing is via het internet op aanvraag beschikbaar stellen van hardware, software en gegevens. In Hoeksche Waard zijn voor medewerkers virtuele werkplekken ingericht, Webmail, Beveiligde koppelingen en voor burgers en bedrijven een Digitaal Loket met DIGID authenticatie.
- hosting volgens “Intern tenzij” principe voor interne afnemers en dienstverlening aan externe partijen om investeringen, beheerkosten en de enkelvoudige opslag van basisregistraties maximaal te benutten.
- externe hosting systemen worden onder architectuur ontwikkeld om de continuïteit van bedrijfsprocessen te borgen. Dit vermindert contractkosten, verbetert beheer van informatiekoppelingen en persoonlijke identiteiten en borgt informatieclassificaties volgens wettelijke kaders en afgesproken richtlijnen.

Participatiesamenleving vraagt onder andere toegang en beheer door burgers tot hun persoonlijke informatie.
- om fraude te voorkomen wordt het vaststellen van de identiteit van een burger en ambtenaar en toegangscontrole belangrijker (Identity management);
- het herkennen van identiteitsfraude is belangrijk en moet in digitale diensten en ontwikkelingen expliciet worden meegewogen en aan de wet getoetst.

ICT technische ontwikkelingen, met name de opkomst van sociale media, cloud computing, en Open Data en Data Gedreven Sturing. Ook Het Nieuwe Werken (en gebruik van eigen apparatuur BYOD) vergt aanvullende beveiligingsmaatregelen en veilige dienstverlening;
- beleid, richtlijnen en passende controles vaststellen en inrichten op basis van risicoanalyses
- doelbinding, privacy impact assessments (PIA), Privacy verordening, juridische controles en toezicht op juiste, volledige en tijdige verwerking worden belangrijker dan technische beperkingen

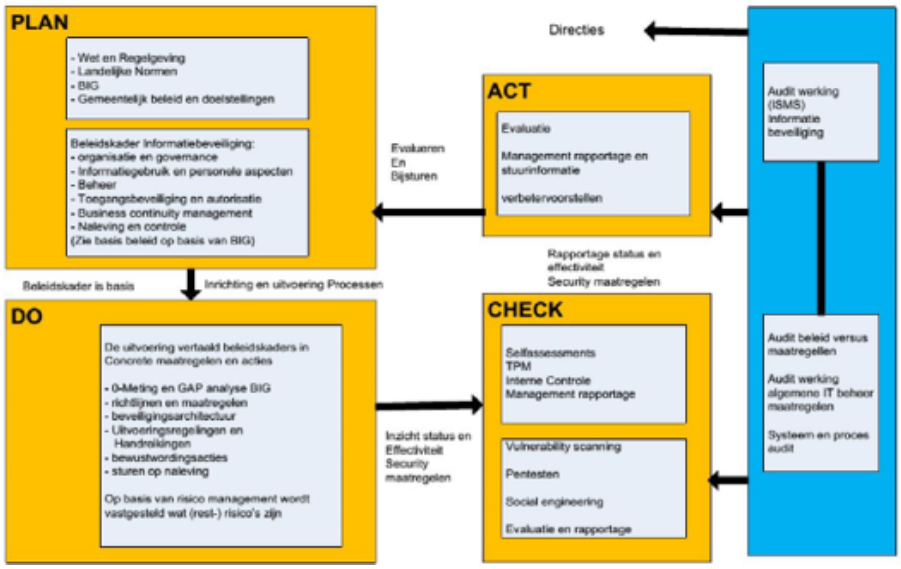
Bedreigingen zijn toegenomen zoals cybervandalisme, cybercriminaliteit en cyberterrorisme. Externe dreigingen stellen het vertrouwen in de overheid ter discussie, zoals hacken (DIGINOTAR affaire), fishing, botnets en virussen
- preventie tegen Malware, SPAM, DDOS e.d. is geoptimaliseerd

Ontwikkeling landelijke standaarden: Baseline Informatiebeveiliging Overheid (BIO); Informatiebeveiliging: Processturing en optimaal gebruik van landelijke richtlijnen (BIG, BIO Webrichtlijnen NCSC, GEMMA, NORA e.d)

4 Proces van informatiebeveiliging

4.1 Methodiek PDCA

Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het management systeem van informatiebeveiliging.



Figuur 3: PDCA Cyclus Proces Informatiebeveiliging

- Plan: De cyclus start met Informatiebeveiligingsbeleid, gebaseerd op wet-en regelgeving, landelijke normen en 'best practices', uitgewerkt in Tactische Richtlijnen voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning en rapportage sluiten aan op de reguliere P&C cyclus. De planning is mede onderdeel van het ontwikkelpad (roadmap) van de Architectuur.
- Do: Het beleidskader is de basis voor risicomanagement, uitvoering van maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT en voldoen aan wet- en regelgeving.
    - Externe controle: betreft controle buiten het primaire proces door een auditor. Dit heeft het karakter van een steekproef. De CISO is opdrachtgever. Bevindingen worden gerapporteerd aan de CISO, en via de CISO aan de directie.
    - Interne controle vindt steekproefsgewijs plaats zoals beschreven in de IC planning.
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning. De bevindingen worden in beginsel gerapporteerd aan de directie. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

4.2 Risicobenadering

De aanpak van informatiebeveiliging in Hoeksche Waard is 'risk based'. Een integrale risicobenadering maakt besturing van informatiebeveiliging vanuit de bedrijfslaag richting de applicatie laag en de technische laag mogelijk.

> Een gemeente werkt samen mét **mensen** vóór mensen, met behulp van **informatie** en **middelen**. De bedrijfsdoelstellingen benadrukken **betrouwbaarheid** en **vertrouwen** in de samenwerking om een optimale participatie en bedrijfsefficiency te behalen.

De kwaliteit van samenwerking is mede afhankelijk van de kwaliteit van informatie en middelen, en daarop zijn dezelfde kernwaarden **betrouwbaarheid** en **vertrouwen** van toepassing. Zodoende ligt er een relatie tussen de principes voor de gemeenten en informatiebeveiliging.

	Principe	**Principe**
Bedrijfsdoelstelling	**Betrouwbaarheid**: "Afnemers kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt"	**Vertrouwen**: "Afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt"

Informatie- en technische laag (Nora, ISO, BIG)	**Betrouwbaarheid** bestaat uit - Beschikbaarheid - Integriteit	**Vertrouwen** bestaat uit - Vertrouwelijkheid (Privacy) - Controleerbaarheid - Onweerlegbaarheid

Tabel 1: Relatie kernwaarden principes voor de gemeente en informatiebeveiliging

De kwaliteit van informatie is onderhevig aan talloze bedreigingen en wordt enerzijds verminderd door bijv. systeemuitval, virussen of ongeautoriseerde toegang. Anderzijds wordt de kwaliteit versterkt door relevante bedreigingen te onderkennen en met maatregelen te beheersen. Het gewenste niveau kan worden bepaald met een bedrijfsimpactanalyse (BIA). De uitkomst hiervan bepaalt welke controles en maatregelen toegepast moeten worden om relevante dreigingen te beheersen op het gebied van mensen, apparatuur, programmatuur, gegevens, omgeving, organisatie en diensten (MAPGOOD).

- Indien een proces of informatiesysteem gevoelige gegevens bevat, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar:**risico = kans x impact**.
- De beveiligingsmaatregelen dienen minimaal hetzelfde kwaliteitsniveau te hebben als het informatiesysteem wat ermee beschermd wordt.
- Organisatie en medewerkers dienen geen risico's te nemen die de beveiliging van de gemeenschappelijke voorzieningen of privacy schaden of besluiten te nemen tot het uitvoeren of nalaten van acties indien daarmee een wet overtreden wordt.

5 Organisatie van de informatiebeveiliging

Er is een kader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen. Goedkeuring door de directie van het Informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

5.1 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.

5.2 Verantwoordelijkheden

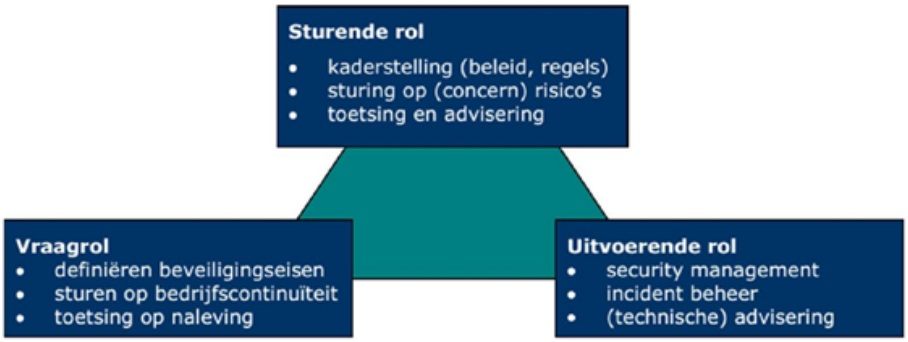
- **Het college van Burgemeester en Wethouders** is politiek verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente.

- **De Gemeentesecretaris** (in sturende rol) is verantwoordelijk voor kaderstelling en sturing.
- De directie:
  - stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet en regelgeving en landelijke normenkaders;
  - stuurt op concern- en cumulatieve risico's;
  - controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij.

- **De Teammanagers van organisatieonderdelen** (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.
  De Teammanager van organisatieonderdelen:

- stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie).
- is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- rapporteert over voldoen aan wet en regelgeving en algemeen beleid van de gemeente in de management rapportages.
- is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit betrouwbaarheidseisen (classificaties).
- is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging van functioneel en technisch beheer, zoals ICT security management,

De verdeling van verantwoordelijkheden is onderstaand weergegeven volgens het concernsturingsmodel voor de bedrijfsvoering.



Figuur 4: Concernsturingsmodel voor Informatiebeveiliging

5.3 Taken en rollen

- Het College van B&W stelt formeel het Informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het College als de Raad (controle functie) kunnen hiervoor opdracht geven. De gemeentedirectie adviseert B&W formeel over vast te stellen beleid.
- De **CISO** (Chief Information Security Officer) geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan. De CISO bevordert en adviseert gevraagd en ongevraagd over Informatiebeveiliging aan de directie en rapporteert volgens de gebruikelijke P&C cyclus concernbreed aan de directie over de risico's, veranderingen in controlemaatregelen en planning.
- Binnen organisatieonderdelen is, al naar gelang de risico's en aard van werkzaamheden (bv verwerking van gevoelige gegevens), de coördinatie van informatiebeveiliging in de lijn belegd bij beveiligingsfunctionarissen. Denk hierbij aan rollen zoals de beveiligingsfunctionaris van BRP, SUWI en DigiD. Deze rapporteren gesignaleerde risico's onmiddellijk aan zijn/haar directie en aan de CISO.
- Het onderwerp Informatiebeveiliging dient een vast onderdeel te zijn op de agenda van het lijnoverleg zodat er sturing plaatsvindt op risico's en de uitgevoerde activiteiten.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Sturen: Directie **Dagelijkse uitvoering: CISO**	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit (IC), pentesten.	Bijsturen: Opdrachtverstrekking voor verbeteracties. Rapportage aan directie / B&W
Vragen: Alle afdelingen:	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door lijnmanagement en Medewerkers (gedrag), compliancy.	Verbeteren bedrijfscontinuïteit. Rapportage aan CISO.

Uitvoeren: interne rollen en functies	Beleidsvoorbereiding, onderzoeken (marktverkenningen).	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies.	Kwetsbaarheden en risicoscanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de CISO over aanpassingen aan de informatievoorziening

Tabel 2: Taken en rollen

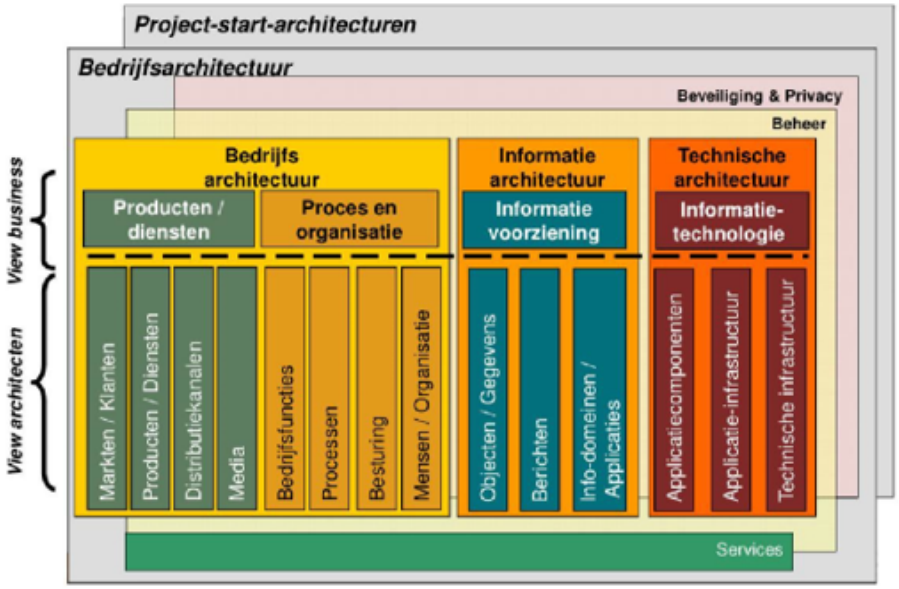
5.4 Rapportage over Informatiebeveiliging

- De beveiligingsfunctionarissen rapporteren per kwartaal tactisch/operationeel aan lijnmanagement en de CISO over risico's, maatregelen en beheersactiviteiten en het functioneren van informatiebeveiliging, of incidenteel indien nodig;
- De CISO rapporteert via een kwartaal rapportage aan lijnmanagement, en aan de directie over het functioneren van informatiebeveiliging en strategische doelen conform de P&C cyclus, of incidenteel indien nodig;
- Escalatielijn: Beveiligingsfunctionaris -> CISO -> Directie.

5.5 Samenwerking

5.5.1 Interne samenwerking

- Informatiebeveiliging is financieel en planmatig verankerd in de P&C cyclus, i-Visie, Informatieplannen van organisatieonderdelen en ontwikkelpad (roadmap) Architectuur.
- Informatiebeveiliging maakt onderdeel uit van de Hoeksche Waardse Informatiearchitectuur en moet worden uitgewerkt in de Informatiebeveiliging Architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie).
- Intern vindt overleg plaats met (Strategisch) adviseurs, Architecten, Interne Controle, Juridische Zaken, OOVd, HRM.
- De CISO overlegt maandelijks met de FG en decentrale beveiligingsfunctionarissen binnen de diverse Organisatieonderdelen. De CISO is voorzitter. Het Privacy&Informatieveiligheidsoverleg (PIV-overleg) heeft binnen de gemeente een adviesfunctie richting de Directie en richt zich met name op beleid en adviseert over tactisch/strategische informatiebeveiliging kwesties.
- Beveiligingsmaatregelen zoals zonering, filtering, authenticatie, Single Sign On, transacties e.d volgen de architectuur methodieken (Novius, DYA, GEMMA, NORA, TOGAF).
- Beveiligingsmaatregelen volgen het meerlaags beveiligingsmodel, en vullen elkaar aan op de bedrijfslaag, informatie laag en technische laag.



Figuur 5: Informatiebeveiliging onder Enterprise Architectuur

5.5.2 ICT crisisbeheersing

- Voor interne crisisbeheersing is een kernteam Informatiebeveiliging geïnstalleerd bestaande uit.
- Coördinator informatieveiligheid/CISO .
- Controller informatiebeveiliging.
- (Beveiligings)beheerder(s) ICT.
- (Security) Architect ICT.
- De manager verantwoordelijk voor de afdeling waar de crisis heeft plaatsgevonden.
- Indien nodig: relevante experts, medewerkers, directielid en/of bestuurlijk verantwoordelijke.
- Communicatie adviseur.

5.6 Externe partijen

- Overheden organiseren hun eigen informatiebeveiliging en toetsen elkaar om de informatieketens te versterken. Daardoor beschouwen ze elkaar als vertrouwde partner.
- Informatiebeveiligingsbeleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente Hoeksche Waard samenwerkt en informatie mee uitwisselt.
- Bij contractuele afspraken gelden in beginsel altijd de Algemene Inkoop Voorwaarden, waarin ten minste geheimhouding en aansprakelijkheid is geregeld. Informatiebeveiligingsbeleid maakt onderdeel uit van de AIV. Wijzigingen op de AIV dienen te worden getoetst aan Informatiebeveiligingsbeleid.
- Bij het (laten) vervaardigen en installeren van programmatuur wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.
- Alle hosting van systemen, data en/of services wordt onder architectuur en governance ontwikkeld om de continuïteit van bedrijfsprocessen te borgen. Dit vermindert contractkosten, verbetert beheer van informatiekoppelingen en persoonlijke identiteiten en borgt informatieclassificaties volgens wettelijke kaders en afgesproken richtlijnen.
- Voor hosting van systemen, data en/of services gelden naast generiek Informatiebeveiligingsbeleid de webrichtlijnen Informatiebeveiliging van NCSC en richtlijnen voor cloud computing.
- Vereiste beveiligingsmaatregelen worden bepaald via risicoanalyse in het governance proces, en aanvullend vastgelegd in contracten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente Hoeksche Waard het recht heeft afspraken te (laten) controleren.
- Voor het tot stand brengen van datakoppelingen met externe partijen geldt naast generiek Informatiebeveiligingsbeleid de procedure “Aanvragen externe toegang”.
- De gemeente is in alle gevallen gehouden aan:
    - de hoogste beveiligingseisen voor bijzondere categorieën gegevens en bij wet voorgeschreven nummers (BSN).
    - toezicht op naleving van regels door de externe partij(en); governance van externe partijen. Deze moet expliciet (centraal) in de organisatie zijn belegd om de contracten en inkoopvoorwaarden, licentie- en beheerkosten, maar ook de beveiligingseisen, rapportages en incidenten te bewaken.
    - regels omtrent grensoverschrijdend dataverkeer;
    - het verzorgen van een overzicht van maatregelen volgens de Tactische Richtlijnen Informatiebeveiliging en Operational Guidelines. Dit ten behoeven van de Comply en Explain status.

Bijlage 1: Wettelijke kaders

Wet en regelgeving

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de Algemene Verordening Gegevensbescherming (AVG). Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De AVG regelt 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. Deze maatregelen maken deel uit van het informatiebeveiligingsbeleid van een gemeente. De gemeente dient zich aan diverse wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging. Wetten en regelingen die van toepassing zijn (niet limitatief):

- Algemene Verordening Gegevensbescherming (AVG)
- Wet Openbaarheid Bestuur (WOB)
- Wet SUWI
- Wet GBA en wet BRP
- Patricipatiewet
- Wet Computercriminaliteit II
- Databanken wet
- Wet op de identificatieplicht
- Besluit Elektronische handtekening
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Politiegegevens (WPG)
- CAR – UWO (bepaalt de rechten en plichten van gemeenteambtenaren)
- Ambtenarenwet
- Registratiewet
- Kader Rijkstoegangsbeleid
- Archiefwet (en ED3 (Eisen Duurzaam Digitaal Depot (2008)))
- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007) aka BIG
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI2012)
- Beveiligingsvoorschrift 2005 (BVR)
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2010)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)

Bijlage 2: Relevante documenten en bronnen

Intern
- Tactische richtlijnen d Hoeksche Waard
- Operational Guidelines
- Statuut CISO
- Beschrijving architectuur Hoeksche Waard
- Algemene Inkoop Voorwaarden

Extern
- NEN/ISO 27001 en 27002 (Code voor Informatiebeveiliging), 2005/7
- Baseline Informatiebeveiliging Gemeenten (BIG), KING, 2013
- Wetgeving, wetten.overheid.nl
- NCSC: http://www.ncsc.nl
- IBD: http://www.ibdgemeenten.nl

Bijlage 3: Relevante begrippen

Audit: Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
Bedrijfsmiddel: Elk middel waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT- voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid: De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen
Beveiliging: Het brede begrip van informatiebeveiliging, inclusief fysieke beveiliging, Business Continuïty Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en integriteit.
Beveiligingsincident: Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICTvoorzieningen.
Controleerbaarheid: De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere ‘werkelijkheden of representaties daarvan’ zodat objectieve oordeelsvorming mogelijk wordt.
DDOS: Denial-of-service-aanvallen (DoS-aanvallen) en distributed-denial-of-service-aanvallen (DDoS-aanvallen) zijn pogingen om een computer, computernetwerk of dienst niet of moeilijker bereikbaar te maken voor de bedoelde klanten.
ICT-voorzieningen: Applicaties en technische infrastructuur, het geheel van ICT-voorzieningen.
Informatiebeveiliging: Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van maatregelen.
Informatiesysteem: Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur en de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
In Control: kan gedefinieerd worden als 'de wijze van sturen, beheersen en toezicht houden, gericht op een effectieve en efficiënte realisatie van strategische en operationele doelstellingen alsmede het hierover op een open wijze communiceren en verantwoording afleggen ten behoeve van belanghebbenden'.
Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de gemeenten: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging.
Integriteit: Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Malware: Is een verzamelnaam voor kwaadaardige en-of schadelijke software. Het woord is een samenvoeging van het Engelse malicious software (kwaadwillende software)
Onweerlegbaarheid: Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
SPAM: Is een verzamelnaam voor ongewenste berichten en is ook bekend als Unsolicited Commercial E-mail en Unsolicited Bulk E-mail. Onder deze term vallen ongewenste e-mails en reclameboodschappen op websites (onder andere fora).
Technische infrastructuur: Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Vertrouwd: In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken.
Vertrouwelijkheid: Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie: Informatie die niet algemeen bekend mag worden (bron: van Dale). In het kader van de BIG worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijke en persoonsvertrouwelijke informatie, zoals bedoeld in Artikel 9 van de AVG.