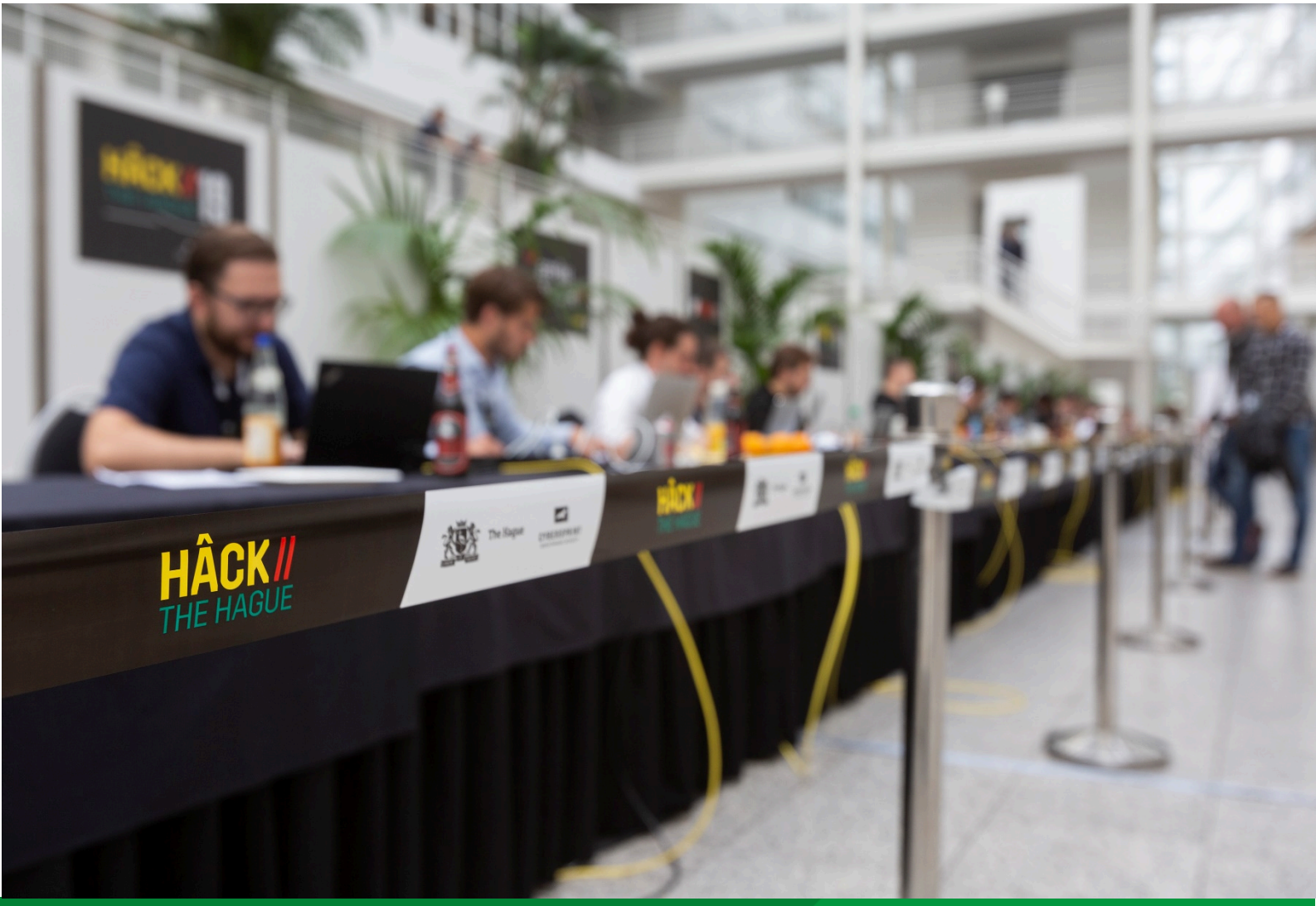
Den Haag

Strategisch Beleidskader Informatieveiligheid Gemeente Den Haag 2019-2022



Status Definitief
Organisatie Bestuursdienst, directie Informatie
Opsteller Jeroen Schipper (Chief Information Security Officer)

December 2019

Managementsamenvatting

Den Haag is de stad van Vrede, Recht, én Veiligheid. Voor de gemeente Den Haag betekent dat zowel de kans om op digitale veiligheid, cybersecurity en informatieveiligheid een belangrijke rol te spelen, als de verplichting om in een voorbeeldrol de gemeentelijke digitale omgeving goed te beschermen. Daarom investeert de gemeente op verschillende wijzen in informatieveiligheid. Informatieveiligheid leidt tot baten die tot uiting komen in een betrouwbare, transparantere en veiligere dienstverlening en uitvoering van gemeentelijke taken in de publieke ruimte. Informatieveiligheid is daarmee een randvoorwaarde voor het bereiken van de doelen die wij als gemeente stellen.

De speerpunten die voor informatieveiligheid de komende drie jaar hoog op de agenda van de gemeente staan zijn:

1. **Risicogebaseerd werken**: de gemeente organiseert informatieveiligheid zodanig dat steeds de afweging gemaakt wordt tussen enerzijds kans, dreiging, gevolgschade en anderzijds de kosten van de mitigerende maatregelen om deze schade te beperken.
2. **Bewust maken van verantwoordelijkheden**: de gemeente zorgt ervoor dat binnen de gehele gemeentelijke organisatie gehandeld wordt naar een verantwoordelijkheid voor informatieveiligheid van de lijn met duidelijk ingevuld eigenaarschap.
3. **Security by design**: de gemeente zorgt dat informatieveiligheid altijd vanaf het begin bij vernieuwingen en veranderingen, zowel bij systemen als beleid en processen, meegenomen wordt.
4. **Voorloper cybersecurity**: de gemeente zorgt dat Den Haag bekend staat als gemeentelijke voorloper op het gebied van cybersecurity. Dit betreft de inzet van in Den Haag aanwezige kennis en expertise en de wijze waarop de gemeente innovatief maatregelen neemt om zo veilig mogelijk te zijn. Uiteraard doen we dat op basis van het hierboven genoemde risicogebaseerd werken.

Ten behoeve van de bovenstaande speerpunten zijn goed opgeleide professionals in informatieveiligheidsfuncties cruciaal. Momenteel is er mondiaal sprake van tekort aan personeel op informatieveiligheid. Vandaar dat de gemeente zich blijft richten op het aantrekken van information security professionals binnen en buiten de Haagse regio.

Naast het opleiden van de medewerkers zijn gedrag, attitude en cultuur essentieel om de gewenste ambities te behalen. Gedrag en cultuur moeten in de gehele gemeentelijke organisatie versterkt worden om het gewenste niveau te bereiken. De komende jaren zal het onderwerp bewustwording of awareness dan ook prominent op de agenda staan. Hierbij werkt de gemeente aan een organisatiecultuur waarin het vanzelfsprekend is om open te zijn over risico's en de meldingsbereidheid hoog is. Het voorbeeldgedrag door het management is daarbij van wezenlijk belang, oftewel '*The Tone at the Top*'.

In het jaarlijks uit te brengen gemeentelijk informatieveiligheidsplan, vast te stellen door het Gemeentelijk Management Team (GMT), worden tactische en operationele aspecten van de informatieveiligheid verder uitgewerkt. Dit wordt gedaan op basis van input van de diensten, de informatieveiligheidsorganisatie van de gemeente, het dreigingsbeeld van de IBD, de uitkomsten van ENSIA en audits. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Van toepassing zijnde wet en regelgeving is toegankelijk op het gemeentelijke intranet.

Inhoudsopgave

1. Inleiding

Dit beleidskader beschrijft het strategisch informatieveiligheidsbeleid voor de jaren 2019 tot en met 2022 en vervangt het 'Beleidskader informatieveiligheid 2015-2018' (RIS 280309). Dit bestuurlijk beleidskader is richtinggevend en kaderstellend en wordt ambtelijk uitwerkt met specifieke interne beleidsdocumenten voor informatieveiligheid op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Beleidskader Informatieveiligheid 2019-2022' zet de gemeente Den Haag een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleidskader is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) die de Baseline Informatiebeveiliging Gemeenten (BIG) per 2020 vervangt. Per 1 januari 2020 wordt de BIO verplicht voor gemeenten als opvolger van de BIG. Voor de opzet van dit beleidskader heeft format van de Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG) als basis gediend.

1.1. Leeswijzer

Hoofdstuk 2 bevat de basisprincipes van informatieveiligheid binnen de gemeente. Hoofdstuk 3 zet de kern van het strategisch beleid uiteen, waarna in hoofdstuk 4 de landelijke context wordt geschetst. Hoofdstuk 5, tenslotte, beschrijft hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2. Wat is informatieveiligheid?

Onder informatieveiligheid wordt verstaan: het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie. Het informatieveiligheidsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele 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 bestuur, alle medewerkers, burgers, ondernemers, gasten, bezoekers en externe relaties.

1.3. Bestuurlijke ambitie informatieveiligheid

Binnen de door de gemeente gestelde doelen is nadrukkelijk aandacht voor de impact die de digitalisering op de samenleving heeft. De beschreven veranderingen spelen niet alleen in de stad maar ook binnen de gemeentelijke organisatie. De gemeente is het dan ook, als stad van vrede, recht en veiligheid, aan haar stand verplicht om haar eigen digitale omgeving goed te beschermen en op dit vlak een voorbeeldrol te vervullen:

"Digitalisering heeft een steeds grotere impact op de maatschappij en daarmee op iedereen die woont en werkt in Den Haag. Naast de fysieke stad, begint er een digitale stad te ontstaan met nieuwe kansen, vraagstukken en bedreigingen. Digitale mogelijkheden worden beter benut. Onze inzet op verdere digitalisering van de dienstverlening moet er voor zorgen dat diensten en producten sneller, eenvoudiger en toegankelijker worden geleverd aan burgers, bedrijven en organisaties in de stad. Gemeentelijke diensten en producten zullen daardoor steeds meer tijd en plaats onafhankelijk (digitaal) geleverd worden. Inwoners en bedrijven moeten daarbij optimale toegang hebben tot informatie. Dat is van belang voor de democratische controle, de keuzevrijheid, zeggenschap en betrokkenheid. De gemeente gaat voort met het verder en klantvriendelijk en zoveel mogelijk op basis van open data ontsluiten van openbare informatie.

Privacy speelt bij deze ontwikkelingen een cruciale rol. Zorgvuldige omgang van de gemeente met de data over iedereen die woont en werkt in Den Haag is uitgangspunt. Dat vergt dat onze systemen

goed beveiligd zijn en minimaal voldoen aan de geldende normen. Dataveiligheid is ook van belang voor onze partners in de stad."

1.4. Speerpunten

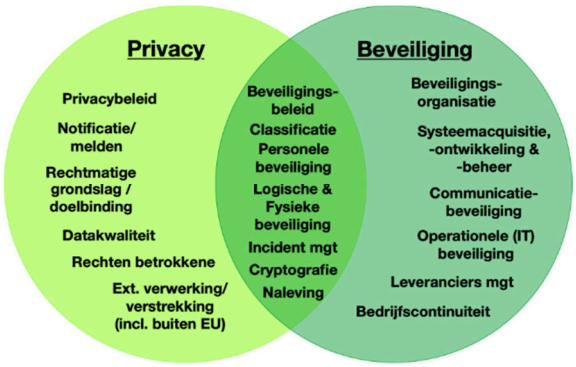
De gemeentelijke ambities vertalen zich naar de volgende vier speerpunten:

1. **Risicogebaseerd werken**: de gemeente organiseert informatieveiligheid zodanig dat steeds de afweging gemaakt wordt tussen enerzijds kans, dreiging, gevolgschade en anderzijds de kosten van de mitigerende maatregelen om deze schade te beperken.
2. **Bewust maken van verantwoordelijkheden**: de gemeente zorgt ervoor dat binnen de gehele gemeentelijke organisatie gehandeld wordt naar een verantwoordelijkheid voor informatieveiligheid van de lijn met duidelijk ingevuld eigenaarschap.
3. **Security by design**: de gemeente zorgt dat informatieveiligheid altijd vanaf het begin bij vernieuwingen en veranderingen, zowel bij systemen als beleid en processen, meegenomen wordt.
4. **Voorloper cybersecurity**: de gemeente zorgt dat Den Haag bekend staat als gemeentelijke voorloper op het gebied van cybersecurity. Dit betreft de inzet van in Den Haag aanwezige kennis en expertise en de wijze waarop de gemeente innovatief maatregelen neemt om zo veilig mogelijk te zijn. Uiteraard doen we dat op basis van het hierboven genoemde risicogebaseerd werken.

1.5. Reikwijdte van dit beleid

Dit beleidskader betreft de totale informatievoorziening van de gemeente Den Haag en dient door alle organisatieonderdelen en medewerkers te worden opgevolgd. Het beleid heeft betrekking op gemeentelijke informatie in alle vormen zoals papieren dossiers, mobiele apparaten, gegevensdragers, ongeacht of deze intern of extern worden beheerd. Dit beleid beschrijft voornamelijk de wijze waarop het management en de medewerkers van de gemeente Den Haag hun verantwoordelijkheid voor informatieveiligheid kunnen en moeten nemen. Het heeft naast alle informatie van de gemeente ook betrekking op informatie die aan de zorg van de gemeente is toevertrouwd. De geautomatiseerde gegevensuitwisseling met externe organisaties, informatiesystemen in beheer bij derde partijen en de ontwikkeling van informatiesystemen vallen ook binnen de scope van dit beleid.

Voor gegevensbescherming (privacy) en het naleven van de Algemene Verordening Gegevensbescherming (AVG) is binnen de gemeente in maart 2018 separaat een beleidskader vastgesteld (RIS 299392) en maakt daarom geen deel uit van de scope van dit beleidskader. Daar waar de onderwerpen van Gegevensbescherming en Informatieveiligheid overlappen, zijn deze onderdeel van de scope van Informatieveiligheid. Ten aanzien van het tactisch beleid zal de uitvoering in overleg plaatsvinden.



Dit strategisch gemeentelijke informatieveiligheidsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK), DigiD (Digitale Identiteit) en Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

1.6. Onderliggend beleid en richtlijnen

Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. De komende twee jaar zal het bestaande tactisch beleid worden geëvalueerd en waar mogelijk worden hergebruikt en opnieuw worden vastgesteld. De evaluatie zal zoveel mogelijk gebeuren aan de hand van bestaande normen en kaders die (inter)nationaal verkrijgbaar zijn zodat maatwerk zo min mogelijk nodig is. Tactisch beleid met betrekking tot informatieveiligheid zal voor iedere medewerker toegankelijk zijn op het gemeentelijke intranet en de structuur van de ISO27000 serie volgen. In het jaarlijks uit te brengen gemeentelijk informatieveiligheidsplan, vast te stellen door het Gemeentelijk Management Team (GMT), worden deze tactische en operationele aspecten van de informatieveiligheid verder uitgewerkt. Dit wordt gedaan op basis van input van de diensten, de informatieveiligheidsorganisatie van de gemeente, het dreigingsbeeld van de IBD, de uitkomsten van ENSIA en audits. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Van toepassing zijnde wet en regelgeving is toegankelijk op het gemeentelijke intranet.

1.7. Geldigheidsduur van het beleid en evaluatie

Dit beleid is door het College van B&W vastgesteld voor de periode van 2019-2022. Uiterlijk het laatste jaar zal het geëvalueerd, waar nodig aangepast en opnieuw vastgesteld worden. Indien een nieuw beleidskader binnen deze termijn nog niet is vastgesteld, dan blijft het huidige beleidskader tot dat moment van toepassing.

2. Basisprincipes

De Gemeente Den Haag hanteert de volgende basisprincipes voor haar informatieveiligheid en zijn van toepassing op de gehele gemeentelijke organisatie en op alle partijen waarmee de gemeente samenwerkt, inclusief ketenpartners en leveranciers. Deze principes fungeren als basis ten behoeve van de ambities van de gemeente Den Haag. Ze zijn gelijkwaardig en kunnen zelfstandig worden gebruikt, maar moeten steeds in hun onderlinge samenhang toegepast worden.

1. *Grondbeginsel:* Informatieveiligheid is een vast en onlosmakelijk onderdeel van beheer en vernieuwing. Daarbij mag informatieveiligheid de operatie in beginsel **niet hinderen** omdat de operatie de hartslag vormt van gemeente Den Haag. De term operatie is hier gebruikt voor iedere vorm van operationele en primaire processen. Enige vorm van hinder kan niet altijd worden vermeden.

2. *Doelmatigheid:* Maatregelen zijn **in balans** met de te beschermen waarde of het belang; er moeten **'doelmatige, zakelijke' argumenten** zijn om beveiligingsmaatregelen te treffen. Als er geen doelmatige argumenten zijn, worden er geen nieuwe maatregelen getroffen. Dit betekent dat een risicoanalyse uitgevoerd moet worden naar de noodzaak van maatregelen, d.w.z. de te nemen maatregelen voor informatieveiligheid zijn risico gedreven.

3. *Basisbeveiliging:* De gemeente Den Haag beschikt over een **basis beveiligingsvoorziening** die voor alle vormen van informatieverwerking een standaardniveau tegen beveiligingsincidenten biedt. Deze basis wordt vanuit vier functionele gebieden geregeld door 1. de technische voorzieningen, 2. facilitair, 3. inkoop en 4. personeelszaken.

4. *Eigenaarschap:* Alle processen, applicaties, informatieverzamelingen en generieke infrastructuur (fysiek en digitaal) hebben steeds elk **één formele eigenaar** in de lijnorganisatie. Het is dan ook belangrijk dat de lijnorganisatie voor ondersteuning kan beschikken over voldoende capaciteit en kwaliteit binnen de bedrijfsvoering.

5. *Continuïteit:* De formele eigenaren van processen, informatieverzamelingen en generieke infrastructuur (fysiek en virtueel) hebben **zelf de verantwoordelijkheid** om, daar waar nodig, te zorgen voor de **borging van de continuïteit** van de **functionaliteit van die voorziening**, dit geldt ook in geval van uitval of onbeschikbaarheid van applicaties, informatie-verzamelingen en generieke infrastructuur (fysiek en informatie).

6. *Gehele organisatie:* Informatieveiligheid is een **lijnverantwoordelijkheid** binnen elk onderdeel van de organisatie; de Chief Information Security Officer (CISO) en de ISO's adviseren daarbij.

7. *Attitude:* Iedere medewerker is **zelf verantwoordelijk** voor het **naleven** van beveiligings-maatregelen, waardoor zij er als individu op aangesproken kunnen worden. Afdelingsmanagers en teamleiders stellen medewerkers in staat die verantwoordelijkheid te nemen.

8. *Herleidbaarheid:* Iedere medewerker is **uniek identificeerbaar** en traceerbaar bij het gebruik van ICT-systemen of applicaties, waardoor monitoring en controle kunnen worden ingericht.

9. *Gedrag:* Aandacht voor **bewustwording en opleiding** zijn een onmisbaar onderdeel van de inrichting van informatieveiligheid. Centraal worden expertise en middelen aangeboden die lijnmanagers inzetten binnen hun afdeling en teams zodat zij deze verantwoordelijkheid effectief kunnen uitoefenen.

3. Strategisch beleid

3.1. Doel

De ambitie van de gemeente Den Haag is te zorgen dat de gemeente de informatieveiligheid van haar informatievoorziening zodanig inricht en exploiteert dat de vertrouwelijkheid, integriteit en beschikbaarheid effectief en duurzaam gewaarborgd is. Daarbij worden de risico's binnen de budgettaire kaders en voor bedrijfsvoering acceptabele grenzen beheerst. De gemeente Den Haag beschikt daartoe over een informatieveiligheidsorganisatie met voldoende goed opgeleide professionals. Deze bewuste en bekwame medewerkers voeren met eindverantwoordelijke proceseigenaren het door het college vastgestelde beleid binnen budget uit. Hierdoor verleent de gemeente Den Haag een ongestoorde dienstverlening aan burgers, bedrijven, organisaties, ketenpartners en bezoekers en geeft daarmee tevens continuïteit aan de uitvoering aan haar wettelijke taken.

3.2. Risicogebaseerde informatieveiligheid

Informatieveiligheid dient risico-gebaseerd te worden opgezet en is een speerpunt van dit beleidskader. Het richt zich op de bescherming van informatie tegen bedreigingen en gaat in principe over de beantwoording van drie vragen:

1. Wat zijn voor ons de meest waardevolle processen, informatiesystemen en informatie?
2. Welke gebeurtenissen kunnen schade toebrengen aan deze meest waardevolle informatiesystemen en informatie?
3. Wat doen we wel en vooral ook niet om deze informatiesystemen en informatie te beschermen tegen deze gebeurtenissen?

De gemeente Den Haag definieert informatieveiligheid als het proces van het beschermen van informatie en gerelateerde componenten (zoals geautomatiseerde informatiesystemen, personen en papieren documenten) tegen onbedoelde of vooropgezette inbreuken van de (BIV):

- **Beschikbaarheid**: de mate waarin informatie en informatiesystemen op de juiste momenten beschikbaar zijn voor geautoriseerde gebruikers.
- **Integriteit**: de mate waarin de juistheid en volledigheid van informatie is gewaarborgd.
- **Vertrouwelijkheid**: de mate waarin informatie alleen toegankelijk is of wordt gemaakt voor degenen die hiervoor gerechtigd zijn.

De gemeente neemt maatregelen om te voorkomen dat informatie bijvoorbeeld onbedoeld wordt gewijzigd of dat de informatieverwerking wordt verstoord. Om te zorgen dat dit op de meest effectieve en efficiënte manier gebeurt, is informatieveiligheid structureel onderdeel van de bedrijfsvoering. De gemeente Den Haag neemt maatregelen daarom risico-gebaseerd, op basis van zakelijke overwegingen (kosten versus baten) óf omdat er externe verplichtingen (wet- en regelgeving) zijn om bepaalde maatregelen te nemen of een bepaald beschermingsniveau te garanderen. Beveiligingsmaatregelen worden in verhouding tot de eisen aan de BIV van de bedrijfsprocessen genomen en geïmplementeerd. Dit beleid is daar het fundament van, terwijl de verdere details in onderliggend beleid en standaarden verder zijn uitgewerkt.

3.3. Strategische doelen

De strategische doelen van het informatieveiligheidsbeleid zijn:

- Het managen van de informatieveiligheid.
- 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.

3.4. Belangrijkste kaders

De belangrijkste kaders van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatieveiligheid.
- De uitvoering van de informatieveiligheid is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Den Haag 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.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatieveiligheidsbeleid vormt samen met het informatieveiligheidsplan het fundament onder een betrouwbare informatievoorziening. In het informatieveiligheidsplan 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.
- Informatieveiligheid is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatieveiligheid.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid. Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- 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.

3.5. Invulling van de kaders

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten en kaders:

- Het college van B en W stelt als eindverantwoordelijke het strategisch informatieveiligheidsbeleid vast.
- Het GMT stelt jaarlijks het informatieveiligheidsplan vast.
- De directies zijn verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directies zijn verantwoordelijk voor het vragen om informatie bij de afdelingsmanagers en ziet erop toe dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.

- De 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 viermaandelijks aan het GMT. Risicovolle onderwerpen die daarbij naar voren komen, kunnen worden opgenomen in het gemeentelijke auditplan.
- De gemeentelijke managers zijn verantwoordelijk voor de uitvoering van de informatieveiligheid voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatieveiligheid, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Afdelingsmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers voeren quickscans informatieveiligheid uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

3.6. Randvoorwaarden

Belangrijke randvoorwaarden voor een goede werking van het strategisch beleidskader zijn:

- De informatieveiligheid maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatieveiligheid en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatieveiligheidsplan opgesteld onder regie van de CISO, gebaseerd op:
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Het dreigingsbeeld gemeenten van de IBD;
    - De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3.7. Afwijkingen van bestaand beleid en regelgeving

De implementatie van maatregelen kost in veel gevallen geld en/of tijd van onze medewerkers en de organisatie. Omdat dit schaarse middelen zijn, kan het voorkomen dat bepaalde en dus benodigde maatregelen niet of onvoldoende (tijdig) kunnen worden geïmplementeerd. Deze afwijking wordt door een ISO met een advies ter beoordeling voorgelegd aan de desbetreffende algemeen directeur en de CISO. Bij verschil van inzicht wordt de afwijking ter goedkeuring en herbeoordeling aan de het GMT voorgelegd. De toegestane afwijkingen zullen aan een termijn van maximaal twee jaar zijn gebonden. Voor het verstrijken van deze termijn dient de herbeoordeling plaats te vinden.

De desbetreffende dienst zorgt ervoor dat de besluitvorming rond deze afwijkingen goed gedocumenteerd wordt en steeds voor audits toegankelijk is. De CISO bewaakt het totaaloverzicht en ziet er op toe dat de termijnen zorgvuldig bewaakt en gehandhaafd worden.

4. Landelijke context beleidskader

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

4.1. Baseline Informatiebeveiliging Overheid (BIO)

De BIO is het nieuwe normenkader informatieveiligheid voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan het oude normenkader (BIG). Dat wil zeggen dat de afdelingsmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

4.2. Tien bestuurlijke principes voor informatieveiligheid

De tien bestuurlijke principes voor informatieveiligheid zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatieveiligheid is van iedereen.
3. Informatieveiligheid is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatieveiligheid behoeft ook aandacht in (keten)samenwerking.
6. Informatieveiligheid is een proces.
7. Informatieveiligheid kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatieveiligheid in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatieveiligheid nadrukkelijk gewenst op de bestuurstafel.

4.3. Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld helpt daarmee om focus aan te brengen in het actualiseren van beleid en plannen voor informatieveiligheid.

4.4. Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

4.5. Standaarden informatieveiligheid

De basis voor de inrichting van het informatieveiligheidsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatieveiligheidsbeleid heeft de interbestuurlijke werkgroep Normatiek in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. 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 ISO en de BIO. Ook het informatieveiligheidsplan zal deze structuur volgen.

5. Organisatie, taken en verantwoordelijkheden

5.1. Leiderschap en betrokkenheid

Binnen de al eerdergenoemde gemeentelijke doelen is aangegeven dat zorgvuldige omgang met de informatie die de gemeente heeft een belangrijke randvoorwaarde is bij de inzet om dienstverlening verder te digitaliseren.

… Zorgvuldige omgang van de gemeente met de data over iedereen die woont en werkt in Den Haag is uitgangspunt. Dat vergt dat onze systemen goed beveiligd zijn en minimaal voldoen aan de geldende normen. …

Om dit te realiseren is voorbeeldgedrag en leiderschap noodzakelijk. Alleen als iedereen van hoog tot laag door hun eigen gedrag aangeven dat informatieveiligheid belangrijk is zullen collega's dat gedrag ook gaan vertonen.

Het GMT en de directies van de gemeentelijke diensten spelen een cruciale rol bij het uitvoeren van dit strategische informatieveiligheidsbeleid. Het gehele gemeentelijk management geeft een duidelijke richting aan informatieveiligheid en demonstreert dat zij informatieveiligheid ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatieveiligheidsbeleid van en voor de hele gemeente. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis worden acties op het gebied van informatieveiligheid bepaald en wordt de voortgang van de uitvoering bewaakt.

De organisatie van Informatieveiligheid moet op drie niveaus plaatsvinden en die niveaus moeten onderling naadloos op elkaar aansluiten: 1. Strategisch, 2. Tactisch en 3. Operationeel. De besturing is er op gericht om deze aansluiting te borgen en bovendien de aansluiting bij de overige processen binnen de gemeente zeker te stellen. We maken daarbij een onderscheid tussen bestuurlijke aansturing en lijn aansturing:

Binnen de gemeente berust de verantwoordelijkheid voor de bestuurlijke aansturing bij het college onder leiding van de burgemeester. De dagelijkse uitvoering hiervan berust bij de gemeentesecretaris, waarbij de verantwoordelijkheid voor de inrichting van informatieveiligheid door hem via de Chief Information Officer gedelegeerd is aan de Chief Information Security Officer (CISO). Het lijnmanagement binnen elke dienst heeft de verantwoordelijkheid om het informatieveiligheidsbeleid uit te voeren onder leiding van de algemeen directeur (AD). De aan de AD toegewezen information security officer (ISO) treedt hierbij op als adviseur van de AD en de sectordirecteuren op dit gebied.

Om informatieveiligheid binnen de organisatie in te bedden moet aandacht zijn voor:

- Processen
- Cultuur, attitude en gedrag
- Organisatie rollen, verantwoordelijkheden en bevoegdheden

5.2. Processen

Algemeen ten aanzien van de processen binnen de gemeente moet informatieveiligheid een integraal onderdeel zijn. Het is de verantwoordelijkheid van de proceseigenaar om te zorgen dat dit ook zo is. Het is de verantwoordelijkheid van de AD om erop toe te zien dat de proceseigenaren hier zorg voor dragen. Het is de verantwoordelijkheid van de CISO om richting te geven en erop toe te zien dat er een effectieve informatieveiligheidsorganisatie is die passend is voor de gemeente. De operationele inrichting van onderdelen hiervan zal in bijna alle gevallen de verantwoordelijkheid zijn van lijnmanagers binnen het BEC of IDC/A. In de gevallen waar het een dienst betreft is de desbetreffende AD verantwoordelijk. Daarnaast is iedere medewerker zelf verantwoordelijk voor het naleven van beveiligingsmaatregelen. Het helder en eenduidig beleggen van deze verantwoordelijkheden is een speerpunt binnen dit beleidskader.

5.3. Cultuur, attitude en gedrag

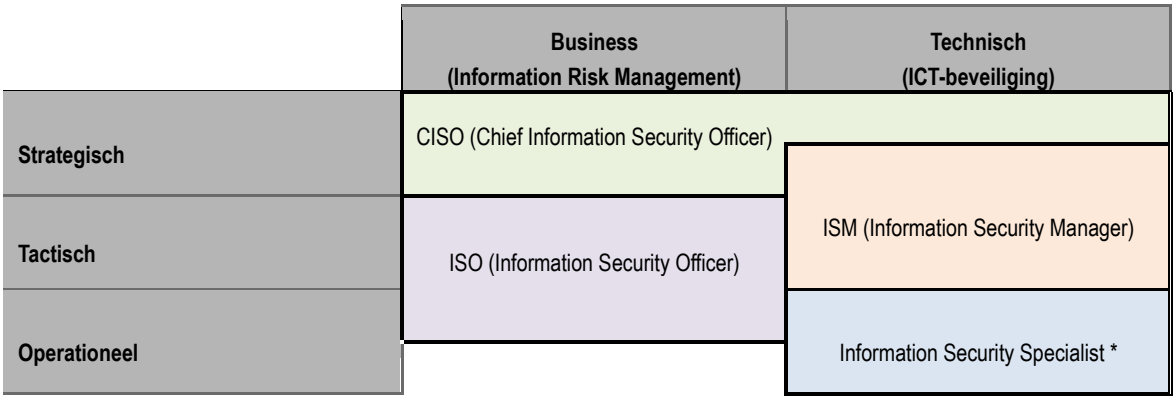
Naast de opleiding van de medewerkers waardoor zij, ondersteund door het management, in staat moeten zijn hun verantwoordelijkheid op het gebied van het beschermen van de informatie van de gemeente te nemen, zijn gedrag, attitude en cultuur essentieel om het gewenste resultaat te bereiken. Gedrag en cultuur zullen zowel over de gemeente als geheel, als vanuit de bestaande organisatiestructuur beïnvloed worden om het gewenste niveau te bereiken. Hierbij streven we naar een organisatiecultuur waarin het vanzelfsprekend is om open te zijn over risico's en de meldingsbereidheid hoog is. Het is een speerpunt om informatieveiligheid vanaf het begin mee te nemen bij vernieuwing of verandering. Het voorbeeldgedrag door het management is daarbij van wezenlijk belang, van boven naar beneden – *The Tone at the Top*.

5.4. Rollen, verantwoordelijkheden en bevoegdheden

<u>Organisatiestructuur informatieveiligheid</u>
De organisatie van informatieveiligheid binnen de gemeente wordt functioneel aangestuurd vanuit de hoofdstructuur op de verschillende niveaus:

- **Strategisch:** CIO-Office met daarin de CISO.
  Hier vindt ook de coördinatie en aansturing plaats in overleg met de Sr ISO (Information Security Officer - BEC-I) en ISM (Information Security Manager - IDC/A).
- **Tactisch:** BEC-I en IDC/A met daarin de ISO en ISM.
  De ISO's vullen de informatieveiligheidsrol voor de diensten in vanuit de business, waarbij een of meerdere ISO's als adviseur aan een dienst of bedrijfsproces toegewezen kunnen worden. Zij maken de risico's voor de business inzichtelijk, adviseren de business over toe te passen maatregelen en handhaven de IB-beleidskaders.
  De ISM (Information Security Manager) is binnen IDC/A verantwoordelijk voor informatieveiligheid ten aanzien van de geleverde ICT-diensten in samenspraak met de ISO's. In toenemende mate komen die diensten ook van buiten de gemeente (externe leveranciers). Daarnaast stuurt de ISM ook de information security specialisten binnen de afdeling IDC/A aan.
- **Operationeel:** IDC/A met de verschillende Information Security Specialisten en de ISO's van BEC-I.
  Vanuit IDC/A bestaat de inzet uit specialistische kennis op diverse vraagstukken zoals, cryptografie, netwerkbeveiliging, logging en monitoring, incidenten onderzoek en afhandeling als ook controle op naleving technische componenten. Ook valt hieronder het verrichten van ontwikkel-, beheer- of advieswerkzaamheden binnen IDC/A die vragen om diepgaande technische kennis van ICT en informatieveiligheid. Voor wat betreft de inzet vanuit BEC-I gaat het hier om de afhandeling van incidenten en de security aspecten van datalekken.

Schematisch kan de indeling van de belangrijkste functies weergegeven worden zoals in de tabel hieronder is aangegeven. Hierbij wordt de opzet gevolgd zoals die door het PvIB (Platform voor Informatiebeveiliging) in het QIS-framework is gemaakt en die binnen Nederland algemeen gebruikt wordt:



Verantwoordelijkheden

Binnen de informatieveiligheidsorganisatie is een aantal rollen benoemd. Onderstaande tabel geeft de rol aan, aan wie die is toegewezen en welke verantwoordelijkheid daarbij hoort.

Rol	Ingevuld door	Verantwoordelijk voor
Eindverantwoor-delijk voor informatie-veiligheid binnen de gemeente Den Haag	College van B&W, Gemeenteraad	Het College van B&W stelt formeel het strategisch beleidskader informatieveiligheid vast en delegeert de ambtelijke eindverantwoordelijkheid aan de gemeentesecretaris. Met ENSIA verantwoordt de gemeente zich vanaf 2017 ook horizontaal aan de gemeenteraad ten aanzien van alle registratiesystemen. Het college is verantwoordelijk voor het afgeven van de bijbehorende collegeverklaring inzake DigiD en Suwi-net en, voor zover van toepassing, het afleggen van verantwoordelijkheid daarover aan de raad.
Ambtelijk eind-verantwoordelijk voor informatie-veiligheid	Gemeentesecretaris	De gemeentesecretaris is binnen de gemeente ambtelijk eindverantwoordelijk voor de informatieveiligheid. Hij/zij heeft een aantal taken gedelegeerd om invulling te geven aan deze verantwoordelijkheid. De gemeentesecretaris stelt de CISO aan als formeel ENSIA-coördinator.
Stuurgroep Informatie Veiligheid	GMT	Het Gemeentelijk Management Team (GMT) is onder leiding van de gemeentesecretaris verantwoordelijk voor de bekrachtiging van het beleidskader informatieveiligheid en de daarin opgenomen richtlijnen.
Business Eigenaren	Algemeen directeur van de dienst (AD) en (sector)directeuren /managers binnen de diensten met eindverantwoordelijkheid voor een eigen domein	De algemeen directeuren zijn eindverantwoordelijk voor het vaststellen van specifieke informatieveiligheidsmaatregelen voor de diensten, afgeleid van het informatieveiligheidsbeleid, alsmede voor het toezien op de uitvoering van deze maatregelen en eventuele acceptatie van de restrisico's. De algemeen directeuren zijn als eigenaren verantwoordelijk voor de afhandeling van informatieveiligheidsincidenten in overleg met de ISO, alsmede voor het toezicht op de juiste werking van beveiligingsmaatregelen. Tevens zijn zij eindverantwoordelijk voor het bepalen van de waarde van informatie en het vaststellen van het noodzakelijke niveau van beveiliging, alsmede het uitvoeren van de vastgestelde beveiligingsmaatregelen.
Eindverantwoorde lijk voor IT-infrastructuur	Manager IDC-A	De manager IDC-A is binnen de gemeente eindverantwoordelijk voor de implementatie van de juiste informatieveiligheidsmaatregelen in de ICT-infrastructuur en bevoegd passende maatregelen te nemen indien systemen hier niet aan voldoen.
Chief Information Offcer Chief Information Security Officer (CISO)	CIO, CISO	De CIO is verantwoordelijk voor de kaderstelling ten aanzien van de gemeentelijke informatievoorziening en IT en het toezicht op de naleving van de vastgestelde kaders. De CISO is verantwoordelijk voor het aansturen van het strategische gedeelte van het ISMS (Information Security Management Systeem). De CISO functioneert als een adviseur, coördinator en algemeen aanspreekpunt voor informatieveiligheidsincidenten, de organisatie inzake informatieveiligheid en projecten op het gebied van

Rol	Ingevuld door	Verantwoordelijk voor
		informatieveiligheid. Tevens bewaakt deze functionaris de kwaliteit van dit proces. De CISO faciliteert de Information Security Officers (ISOs) met het beleid, de richtlijnen, procedures en voorschriften zoals beschreven in dit document.
Business Information Security Officers	Information Security officers bij het BEC (ISO's)	De Business Information Security Officer is een rol die per dienst wordt ingevuld door de toegewezen ISO's uit het BEC. Zij zijn verantwoordelijk voor het adviseren over en coördineren en communiceren van de activiteiten op het gebied van informatieveiligheid binnen de dienst namens de Algemeen Directeur. Zij werken in nauw overleg met de ISM.
Information Security Manager (ISM)	ISM	De Information Security Manager (IDC/ISM) is verantwoordelijk voor de technische vertaling van de kaders, analyses en architectuurbeelden in een informatieveiligheidsplan. Het plan bevat de organisatorische, procesmatige en technische maatregelen voor de Shared Service Centers (SSC's) HR, Automatisering, Facilitair (fysieke beveiliging) en het waarborgen van de uitvoering ervan. De ISM is adviserend bij inbedding van beveiliging in SLA's met de diensten en externe partijen en verantwoordelijk voor het implementeren van informatieveiligheid. De ISM controleert de output van de processen van de SSC's. Tevens waarborgt hij de samenwerking tussen de verschillende onderdelen, o.a. binnen het IDC. Met de diensten op het gebied van beveiliging geeft de ISM advies en initieert verbeterpunten. De ISM is verantwoordelijk voor aansturing van interne en externe audit op de technische infrastructuur.
Medewerkers	Alle vaste medewerkers, alle medewerkers in tijdelijke dienst en allen die ingehuurd zijn om onder aansturing van de gemeente werkzaamheden te verrichten	Medewerkers handelen conform richtlijnen en voorschriften. Signaleren en melden beveiligingsproblemen of -incidenten. Bevorderen actief een veilige cultuur. Spreken elkaar aan op naleving.
Onafhankelijk Auditor	Gemeentelijke Accountantsdienst (GAD)	De GAD is de externe Auditor die verantwoordelijk is voor audits op de uitvoering van informatieveiligheid en geven een onafhankelijk oordeel aan de ambtelijk top, College en Raad en diverse externe partijen.
ENSIA Coördinator	CISO	De ENSIA Coördinator is verantwoordelijk voor het organiseren van ENSIA-verantwoordingsproces zodanig dat deze juist, tijdig en volledig wordt ingediend. Daarbij hoort: • Het opstellen en het uploaden van de documenten zoals Collegeverklaring, Assurance Rapport, Bijlage B+C en de TPM's. • Externe communicatie en afstemming i.k.v. ENSIA met ondersteunende organisaties VNG en ICTU. • Organiseren opdrachtverlening voor IT-auditen en voor pentesten per DigiD-aansluiting. Faciliteren werkzaamheden van RE-Auditor en bewaken tijdige oplevering Assurance Rapport. • Nauw overleg met ISO's en ISM m.b.t. afstemmen procedures, maatregelen en controles die wel/niet worden uitgevoerd.
Cyber Crisis Management	Cyber Board - Manager IDC/A - Chief Information Security Officer - Hoofd Uitvoering en Beheer - Information Security Manager - - Sr Information Security Officer	Heeft tot taak in geval van een groot cyber incident de operationele coördinatie van de ICT uit te voeren.

5.5. Planning en risicomanagement

Het risicomanagement voor informatieveiligheid wordt op de verschillende niveaus in de organisatie ingevuld. Dat wil zeggen dat de gemeente-brede inrichting van risicomanagement voor informatieveiligheid is belegd bij de CISO. Het is de taak van de CISO om de gemeente-brede informatieveiligheidsrisico's in kaart te (laten) brengen en die kenbaar te maken aan de verantwoordelijke proces- en systeemeigenaren en erop toe te zien dat deze op een voor de gemeente aanvaardbare wijze worden afgehandeld. Dit in kaart brengen gebeurt op basis van de door de dienst ISO's en proceseigenaar uitgevoerde risicoanalyses binnen hun verantwoordelijkheidsgebied.

De risico's op niveau van de diensten worden door de ISO's afgehandeld. Zij zorgen ervoor dat er een risico-inventarisatie wordt uitgevoerd, zoals een Baseline toets of Business Impact Analyse (BIA) die wordt uitgevoerd en afgestemd met de verantwoordelijke van de dienst. Ook zien zij er op toe dat de risico's gemitigeerd worden en de risico's die daarna overblijven door een daartoe bevoegd persoon expliciet geaccepteerd worden. Indien dat grote risico's of risico's op gemeentelijk niveau betreft is altijd advies van de CISO nodig voordat een risico geaccepteerd mag worden, waarbij de GS als eindverantwoordelijke betrokken kan worden.

5.6. Awareness of bewustwording

Het is noodzakelijk dat alle medewerkers de juiste instelling hebben ten aanzien van informatieveiligheid. Attitude en gedrag zullen daarom op het niveau van de gehele organisatie periodiek door middel van 'Awareness'-campagnes en -trainingen beïnvloed moeten worden om medewerkers bewust te maken van het belang van informatieveiligheid en bekwaam te maken en hun eigen rol daarin te kunnen vervullen. Op deze manier wordt het juiste gedrag bevorderd en ontstaat een cultuur waarin met elkaar aanspreekt op fout en goed gedrag. Deze campagnes en trainingen zullen vanuit de CISO georganiseerd worden, maar het is de verantwoordelijkheid van elke manager om ervoor te zorgen en op toe te zien dat al zijn of haar medewerkers hier serieus aan mee doen. (N.B. Gezien de overlap met het onderwerp Privacy/gegevensbescherming dat onder verantwoordelijkheid staat van de Functionaris Gegevensbescherming, zal de awareness vaak in combinatie georganiseerd worden). Naast deze permanente en verplichte educatie zal vanuit de CISO en ISO's door middel van events en publicaties gezorgd worden voor continue aandacht voor het onderwerp.

5.7. Onafhankelijke toetsing

<u>Gemeentelijke Accountantsdienst (GAD)</u>
De GAD controleert en evalueert de naleving van wettelijke voorschriften en van het eigen informatieveiligheidsbeleid. De GAD beoordeelt minimaal eenmaal per jaar of alle informatieveiligheidsprocedures binnen elk verantwoordelijkheidsgebied correct worden uitgevoerd en of processen c.q. (informatie)systemen voldoen aan de eisen die voorkomen uit de relevante wet- en regelgeving, het informatieveiligheidsbeleid, de normen en andere verplichtingen. Daarnaast controleert de GAD minimaal eenmaal per jaar de naleving van technische normen door de productiesystemen te onderzoeken op de effectiviteit van de geïmplementeerde informatieveiligheidsmaatregelen, bijvoorbeeld door het (laten) uitvoeren van security scans.

Door de onafhankelijke positie die de GAD heeft, is ook geborgd dat de toetsing niet beïnvloed wordt door andere belangen en of overwegingen die binnen de gemeente een rol spelen bij de besluitvorming. Hierdoor bestaat een zuiver beeld van de informatieveiligheid binnen de gemeente en mag hierop gesteund worden in de verantwoording naar het college, de raad en naar externe partijen.

<u>Eenduidige Normatiek Single Information Audit (ENSIA)</u>
Gemeenten organiseren de verantwoording over informatieveiligheid op een uniforme manier. Dit gebeurt met behulp van ENSIA. De Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op de horizontale verantwoording: binnen de gemeente, met een belangrijke rol voor de gemeenteraad. ENSIA structureert ook de verticale verantwoording richting de rijksoverheid, over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie

(DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI). De ENSIA-coördinator organiseert de verantwoording over de informatieveiligheid van de gemeente, zowel horizontaal als verticaal. ENSIA toetst of de informatieveiligheid op orde is. Met vragenlijsten en een jaarlijkse rapportage over hoe het gesteld is met de informatieveiligheid krijgt de gemeente inzicht, waarmee ze haar beleid kan verbeteren en kan rapporteren.