Strategisch Gemeentelijk Informatiebeveiligingsbeleid Hilversum

2020-2024

Inhoudsopgave

1 Inleiding 3

1.1 Wat is informatiebeveiliging? 3

1.2 Ambitie en visie van de gemeente op het gebied van informatieveiligheid. 4

1.3 Plaats van het strategisch beleid 4

1.4 Leeswijzer 5

2 Strategisch beleid 6

2.1 Totstandkoming Strategisch beleid 6

2.1.1 De BIO 6

2.1.2 De tien principes voor informatiebeveiliging (zie bijlage 2) 6

2.1.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 7

2.1.4 Gemeentelijke registratie van beveiligingsincidenten- en datalekken 7

2.2 Doel 7

2.2.1 Standaarden informatiebeveiliging 7

2.3 Scope strategisch beleid 7

2.4 Uitgangspunten informatiebeveiliging 7

2.4.1 Doelen informatiebeveiliging 8

2.4.2 Belangrijkste uitgangspunten 8

2.4.3 Invulling van de uitgangspunten 9

2.4.4 Randvoorwaarden 9

3 Organisatie, taken & verantwoordelijkheden 10

3.1 Aansturing: directieteam 10

3.2 Uitvoering: lijnmanagers 10

3.3 Tweedelijns ondersteuning 11

3.4 Controle en verantwoording 11

3.4.1 ENSIA 11

1 Inleiding

Dit strategisch beleid is een kader voor de stappen die we de komen jaren willen uitvoeren. Na vaststelling van het strategisch beleid volgt tactisch beleid en een informatiebeveiligingsplan. Hierin wordt een nadere uitwerking gegeven aan de activiteiten van de komende jaren om het informatiebeveiligingsbeleid in de organisatie te borgen. De komende twee jaar wordt stapsgewijs verder invulling gegeven aan het inrichten van de PDCA (Plan-do-check-act) cyclus. Intussen zitten we niet stil en sluiten we aan bij de “Eenduidige Normatiek Single Information Audit” (ENSIA), een maatstaf in hoeverre de beveiliging op orde is. Met de uitvoering van het tactische beveiligingsplan sturen we op het in control komen van het informatiebeveiligingsproces. Hierbij wordt gestart met het uitvoeren van de Baselinetoets BIO. Deze toetsing helpt proceseigenaren met het in kaart brengen van de beveiligingsrisico’s.

Inwoners, ondernemers, partners en medewerkers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn, dat de informatie die de gemeente uitwisselt met andere overheden betrouwbaar is en dat de gemeente zorgt voor een veilige leefomgeving. Betrouwbare informatie is daarom een belangrijkste grondstof voor de gemeente om haar werk goed te kunnen doen. Hiervoor is informatiebeveiliging een randvoorwaarde.

Vanaf 1 januari 2020 is de “Baseline Informatiebeveiliging Overheid” (BIO) van kracht. De BIO is een doorontwikkeling, of te wel een ‘update’, van de nu bestaande “Baseline Informatieveiligheid voor Gemeenten” (BIG). Door de invoering van de BIO ontstaat er één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid.

Met dit ‘Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2024’ zet Hilversum een volgende stap om de beveiliging van persoonsgegevens en andere informatie te continueren en voort te gaan op de stappen die in de afgelopen jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017[1] en de daarvan afgeleide BIO (zie bijlage 1).
De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging, zoals uitgewerkt door de VNG (zie bijlage 2). Dit strategisch informatiebeveiligingsbeleid is richtinggevend en kader stellend. Dit wordt aangevuld met specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies en standaarden op operationeel niveau. Deze documenten en werkinstructies maken onlosmakelijk geheel van dit beleid uit. Dit beleid vervangt dan ook het in 2015 vastgestelde ‘informatiebeveiligingsbeleid 2015-2018’ en wordt opgenomen in het normenkader. Dit Strategisch gemeentelijk Informatiebeveiligingsbeleid geldt voor de duur van vier jaar (2020-2024) en wordt op doeltreffendheid tweejaarlijks geëvalueerd. Dat zal zijn eind 2021 en eind 2023.

1.1 Wat is informatiebeveiliging?

Onder informatiebeveiliging 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 (persoons)gegevens en andere informatie. Hierin ligt een belangrijke relatie met de Algemene Verordening Gegevensbescherming (AVG), aangezien dit ook één van de belangrijkste basisprincipes zijn voor de bescherming van persoonsgegevens.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de

[1] *International Organisation for Standardization (ISO): organisatie die belast is met het vaststellen van normen en protocollen, onder andere voor datacommunicatie en netwerken. Deze heeft normen uitgevaardigd, bekend als de (NEN)*

toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.2 Ambitie en visie van de gemeente op het gebied van informatieveiligheid.

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeentelijke organisatie. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Ernstige incidenten hebben mogelijk negatieve gevolgen voor inwoners, bedrijven, bezoekers en medewerkers met mogelijk ook politieke consequenties en imagoschade voor de gemeente. Informatieveiligheid is daarom van groot belang om deze risico's te verminderen.

De ontwikkelingen in de samenleving en technologie maken dat informatiebeveiliging en privacy steeds belangrijker worden. Toenemende digitalisering en samenwerking met andere partijen in dienstverleningsketens leidt tot meer en eenvoudiger uitwisselen van informatie. Onze inwoners en bedrijven willen snel en digitaal geholpen worden, maar willen dit doen met behoud van hun recht op privacy. Onze medewerkers willen en moeten steeds meer plaats en tijd onafhankelijk kunnen werken, maar dit mag niet leiden tot informatie die opeens 'op straat ligt'. Ook onze kantooromgeving is door het flexwerken, samenwerking met andere partijen en het openbare karakter van het raadhuis, steeds meer een ontmoetingsplek, waarin de gemeente gastheer is. Informatiebeveiliging gaat over meer dan alleen ICT. Het raakt bijvoorbeeld ook de toegang en de inrichting van gebouwen. Daarom zetten we de komende jaren in op het optimaliseren van informatieveiligheid, de bescherming van persoonsgegevens en het verder professionaliseren van de informatiebeveiligingsfunctie. Hierdoor blijven we aansluiten op de veranderende wetgeving op het gebied van informatisering, digitalisering, informatiebeveiliging en privacy.

Het gemeentelijk Informatieveiligheid zorgt ervoor dat onze informatievoorziening:

- beschikbaar is (voorkomen van uitval van systemen);
- integer en betrouwbaar is (gegevens zijn juist, actueel en volledig);
- vertrouwelijk en exclusief is (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn);
- controleerbaar en transparant is;
- bijdraagt aan een juiste uitvoering van onze (wettelijke) taken en dienstverlening.

Voor de gemeente Hilversum is het belangrijk dat informatie beschikbaar is wanneer medewerkers en (keten)partners deze nodig hebben voor de uitvoering van hun taken. Dat inwoners en bedrijven over informatie kunnen beschikken om diensten te verlenen of te benutten. Hiervoor moet beschikbare informatie juist, actueel en volledig zijn. Daarnaast moet vertrouwelijke informatie voldoende worden beschermd. Tenslotte moeten handelingen en besluiten aantoonbaar (zoals door verslaglegging en logging) controleerbaar zijn, zodat rapporteren en eventueel auditen mogelijk is.

Om dit te verwezenlijken wordt informatiebeveiliging vormgegeven door maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard. De daadwerkelijke aanpak staat niet in dit strategisch beleidsdocument. Wel de organisatie van informatiebeveiliging en de wijze van verantwoording hierover. Deze is in lijn met de organisatie en wijze van verantwoording vanuit het privacy beleid.

1.3 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op operationeel

niveau. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP). In dit plan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de CISO, het dreigingsbeeld van de Informatiebeveiligingsdienst (IBD), registratie van incidenten en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. De directie stelt deze documenten vast.

1.4 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Hierin komen onder andere totstandkoming, de BIO, de tien principes, uitgangspunten, doel en randvoorwaarden aan bod. Het derde hoofdstuk beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie zijn belegd.

2 Strategisch beleid

2.1 Totstandkoming Strategisch beleid

De totstandkoming en de invulling van dit strategisch beleid zijn afgeleid uit de volgende ontwikkelingen:

2.1.1 De BIO

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht. De BIO is het nieuwe normenkader voor de gehele overheid. De werkwijze van de BIO gaat, in tegenstelling tot de Baseline Informatiebeveiliging Gemeenten (BIG), uit van risicomanagement. Dat wil zeggen dat de afdelingsmanagers nu meer dan voorheen moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dat betekent dat het management op voorhand keuzes maakt en continu afweegt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.1.2 De tien principes voor informatiebeveiliging (zie bijlage 2)

De tien principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader[3] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes die wij hanteren zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging 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 informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen het bestuur bij het uitvoeren van goed risicomanagement. De risico's van een slechte informatiebeveiliging zijn talrijk: privacy-schendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte. 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, medewerkers, partners of de reputatie van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

[2] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

[3] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG).

2.1.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

De Informatie Beveiligingsdienst (IBD) geeft periodiek inzicht in de belangrijkste bedreigingen en ontwikkelingen en adviseert over de prioriteiten. Het dreigingsbeeld geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen bij de jaarlijkse actualisering van het informatiebeveiligingsplan. Het dreigingsbeeld biedt een handvat om de informatiebeveiliging verder te verbeteren en daarmee de digitale weerbaarheid te verhogen.

2.1.4 Gemeentelijke registratie van beveiligingsincidenten- en datalekken

Naast de informatie op basis van het hierboven genoemde dreigingsbeeld, is er binnen de gemeente een eigen registratie van beveiligingsincidenten en datalekken. Deze registraties geven ook waardevolle informatie om van te leren en helpend bij het actualiseren van het informatiebeveiligingsplan.

2.2 Doel

Het doel van het ‘Strategisch Informatiebeveiligingsbeleid voor de jaren ‘2020 tot 2024’ is om de organisatie een strategisch kader te geven voor de verdere invulling van tactische beleid en operationele richtlijnen en maatregelen.

2.2.1 Standaarden informatiebeveiliging

De BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Via de IBD worden praktische operationele handreikingen uitgebracht, zoals onder ander een handleiding voor het uitvoeren van een risicoanalyse. Daarnaast is de gemeente voor een aantal processen waarin persoonsgegevens worden verwerkt verplicht een Data Protection Impact Assessment (DPIA) uit te voeren.

2.3 Scope strategisch beleid

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), paspoorten en Nederlandse identiteitskaarten (PNIK) 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. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.4 Uitgangspunten informatiebeveiliging

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. 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 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, zoals de Algemene Verordening Gegevensbescherming (AVG).

2.4.1 Doelen informatiebeveiliging

De doelen van ons 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 inwoners, bedrijven, partners en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.4.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van informatiebeveiliging 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 informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Hilversum hebben of krijgen een interne eigenaar (lijnmanager) 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 informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- 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.
- Het strategische informatiebeveiligingsbeleid en de verantwoordelijkheden voor het beveiligingsbeleid wordt vastgesteld door het college.
- 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 bij de direct leidinggevende en de CISO.

2.4.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- Het college behandeld de informatiebeveiliging binnen de portefeuille ICT,
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is 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 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 controleplannen.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging van de (bedrijfs)processen.
- Hoewel de basiskernregistraties (zoals BRP, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, 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.
- Organisatie ziet er op toe dat medewerkers kennisnemen van de regels en richtlijnen die betrekking hebben op informatiebeveiliging.
- 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 informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.4.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Er zijn voldoende middelen en formatie beschikbaar voor de uitvoering.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CIO-office, gebaseerd op:
    - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - het dreigingsbeeld gemeenten van de IBD;
    - analyse van de geregistreerde beveiligingsincidenten en datalekken;

- de door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3 Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security- en privacy officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een lijnmanager. Voorts draagt zij zorg dat de lijnmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. In de BIO zijn verplichte- en niet verplichte maatregelen opgenomen. De verplichte maatregelen moeten altijd geïmplementeerd worden en zijn ook soms van toepassing op de hele gemeente. Op basis van een GAP-analyse wordt vastgesteld welke maatregelen al in de organisatie aanwezig en geïmplementeerd zijn en welke nog niet. Door de CISO en de eindverantwoordelijke(n) binnen de directie wordt op basis van een GAP analyse bepaald welke maatregelen uitgevoerd worden op concern. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. De tweede analyse wordt gedaan in aanvulling op de eerste door de verantwoordelijk lijnmanagers

Het onderwerp informatiebeveiliging wordt in de gemeente Hilversum gezien als een integraal onderdeel van risicomanagement. De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie is verantwoordelijk voor het (laten) uitwerken van tactische informatiebeveiligingsbeleid en laat zich hierin bijstaan door de CISO van de gemeente. Daarnaast zorgt de directie dat de eindverantwoordelijke portefeuillehouder ICT binnen het college, gevraagd en ongevraagd, geïnformeerd wordt over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Jaarlijks rapporteert de directie aan de wethouder ICT over de voorgang van de uitvoering. Dit gebeurd structureel jaarlijks met de ENSIA rapportage. Op die manier kan het college zich ook verantwoorden naar de raad.

3.2 Uitvoering: lijnmanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van gehele directie en management van de gemeente Hilversum. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar (lijnmanager) hebben; er moet dus altijd iemand verantwoordelijk zijn. Het lijnmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp Informatiebeveiliging te bespreken in de het bedrijfsvoeringsoverleg tussen directie en afdelingsmanagers.

Taken van de lijnmanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.

- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen. De voorbereiding en coördinatie van dit overleg ligt bij de CISO.

3.3 Tweedelijns ondersteuning

De tweede lijn wordt gevormd door ondersteunende professionals, waaronder de Privacy- en Security Officer en informatiemanager. Zij ondersteunen en faciliteren het lijnmanagement bij de risico-inventarisatie en de te nemen maatregelen, organiseren campagnes voor bewustwording en leveren ondersteunende beleidsproducten. Om uitvoering te geven aan het beleid wordt de organisatie bijgestaan door adviserende functionarissen die tezamen met de toezichthoudende functionarissen een Privacy en Informatieveiligheid Team (PIT) vormen. Op de specifieke onderwerpen wordt dit team aangevuld met specialisten vanuit HR, facilitair en ICT.

3.4 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur binnen de portefeuille ICT.
De bestuurders en directeuren van de gemeente Hilversum zullen volgens de tien principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.
Daarnaast rapporteert de Functionaris Gegevensbescherming (FG) jaarlijks rechtstreeks aan het bestuur over de informatiebeveiliging in relatie tot de bescherming van persoonsgegevens.

3.4.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijk managers. De managers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Rapportage van de ENSIA wordt in het college vastgesteld en leidt tot een verklaring in de jaarrekening

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording worden het bestuur en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel. Dat laat zien dat de gemeente informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.