Hulst GEMEENTEBLAD
Officiële uitgave van de gemeente Hulst
Nr. 139900
4 april
2023

Strategisch informatiebeveiligingsbeleid 2023-2026

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid van de gemeente Hulst voor de jaren 2023 tot en met 2026 en vervangt het in 2019 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2019 - 2022'.
Deze nota is richtinggevend, kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2023 – 2026' zet de gemeente Hulst 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 beleid is de NEN-ISO/IEC 27002:2020 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels. In het gemeentelijk Informatiebeveiligingsjaarplan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingshoofden, de CISO, het dreigingsbeeld van de IBD, de uitkomsten van ENSIA, de Agenda Digitale Veiligheid 2020-2024 en het bijbehorende programmaplan 2022-2026. Daarin staan de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 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 persoonsgegevens en andere informatie. Het informatiebeveiligingsbeleid 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 politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de gemeente op het gebied van informatieveiligheid

De ambitie van de gemeente Hulst is om te zorgen dat de informatievoorziening van de gemeente zodanig is ingericht dat de vertrouwelijkheid, integriteit en beschikbaarheid gewaarborgd is. Dit moet leiden tot een ongestoorde dienstverlening aan burgers, bedrijven, organisaties, ketenpartners en bezoekers en geeft daarmee tevens continuïteit aan de uitvoering van haar wettelijke taken. Onze organisatie heeft zich akkoord verklaard met het implementeren van de BIO. Dit heeft als doel de gegevens van de burger en de organisatie conform deze kwaliteitseisen te beschermen.

Informatieveiligheid vraagt continue om aandacht. Om op een adequaat niveau te komen hebben we een systeem nodig wat ons daarbij helpt. We gaan hier uit van een plan-do-check-act cyclus. Hierdoor krijgen we een systeem wat gericht is op het continue verbeteren. In het vakgebied informatiebeveiliging noemen we dat ook wel een Information Security Management System (ISMS).

Een belangrijke fase in dit model is de fase van risicomanagement waarin verbetermogelijkheden worden gesignaleerd. Deze verbetermogelijkheden zijn een kans voor de organisatie om zich verder te ontwikkelen. Ook in de check-fase kunnen controles en audits gezien worden als een belangrijke kans om verdere verbeteringen door te voeren.

In de strategische richtlijn van dit informatieveiligheidsbeleid worden een aantal beleidsuitgangspunten beschreven welke betrekking hebben op aandachtsgebieden. Deze worden pas actueel op het moment dat de organisatie voor een dergelijke keuze of gelijksoortig vraagstuk staat. Hierbij valt te denken aan het al dan niet inzetten van cloud computing, gezamenlijke uitbesteding van softwareontwikkeling of de aanschaf van een nieuw informatiesysteem. In deze specifieke gevallen hanteert de organisatie de beleidsuitgangspunten uit dit document of de nadere richtlijnen, om de veiligheid van informatie bij deze keuze te vergroten.

Waar binnen de organisatie persoonsgegevens verwerkt worden, is privacywetgeving van toepassing. In het privacy-beleid worden aanvullende bepalingen nader uitgewerkt om te voldoen aan de vereisten van privacywetgeving via een privacy management systeem (PMS). Daar waar gevraagd wordt om beveiligingsmaatregelen wordt ook hier geput uit het beleid en de nadere richtlijnen.

Met de opstelling van dit document is bepaald dat de organisatie bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen, de beleidsregels uit dit document en de aanvullende richtlijnen als uitgangspunt hanteert.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het bieden van ondersteuning aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid. Deze beleidsnota presenteert het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2023 - 2026' van de gemeente Hulst. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsjaarplan (IBP).

2.2 Ontwikkelingen

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

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de afdelingshoofden 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.

2.2.2 De 10 principes voor informatiebeveiliging (zie bijlage C)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader[1] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes 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 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 informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.3 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 is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd (TOPdesk). 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.

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

2.2.5 Agenda Digitale Veiligheid 2020 – 2024 & Programmaplan 2022-2026

De Agenda Digitale Veiligheid beoogt een handelingsperspectief voor de lokale bestuurder bij vraagstukken rondom digitale veiligheid te bieden. Daarnaast bevat de agenda de ambities om te komen tot een digitaal veilige gemeente en de daarbij behorende onderwerpen. 10 actielijnen zijn gepresenteerd waarin concrete acties benoemd zijn. De van toepassing zijnde concrete acties voor gemeente Hulst zijn opgenomen in het informatiebeveiligingsjaarplan (IBP).

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2020. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2020 genomen. 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, 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 Informatiebeveiligingsjaarplan zal deze structuur volgen. Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Hiermee worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Binnen het beveiligingsbeleid van de gemeente is ook ruimte voor de bescherming van PA en dit beleid betreft dan ook afdelingen die zich met PA bezighouden zoals Realisatie & Beheer.

2.4 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 tactisch en operationeel niveau. Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven ‘jaarplan informatiebeveiliging gemeente Hulst’.

2.4.1 Gemeentelijke informatiebeveiligingsjaarplan

De BIO kan niet in één keer volledig worden geïmplementeerd. Een dergelijke implementatie zou een onevenredige inspanning van de organisatie verlangen. Daarnaast zijn er voor toekomstige technische en organisatorische veranderingen aanpassingen nodig.

Om deze redenen gaat het jaarplan informatiebeveiliging dan ook (zoals beschreven bij het ambitieniveau) uit van een systeem van continue plannen, uitvoeren, monitoren en verbeteren. We sluiten hiermee aan op de planning en control cyclus die is ingericht conform het plan-do-check-act-principe van Deming. Aan de hand van het beleid kunnen maatregelen worden geïmplementeerd en kan gemonitord worden op de naleving van de maatregelen. Met het bijstellen van de maatregelen of het corrigeren van de uitvoering worden verbeteringen doorgevoerd.
Voor een efficiënte en effectieve benadering gaat een jaarplanning minimaal uit van:

- Het inventariseren van veranderingen in de organisatie (nieuwe taken, veranderingen in wetgeving enz);
- Het periodiek uitvoeren van controles;
- Het periodiek uitvoeren van risicoanalyses (nieuwe of bij veranderingen);
- Het dreigingsbeeld gemeenten van de Informatiebeveiligingsdienst (IBD);
- Het periodiek communiceren over beveiliging;
- Het periodiek opstellen van rapportages;
- Het voorbereiden en uitvoeren van audits.

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI. Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen

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

(bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten
Het bestuur, de directie, de afdelingshoofden en de teamleiders 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, procesautomatisering en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

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

Artikel 2.6.2 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten 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 informatiebeveiliging.
- Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen, vallen onder dit informatiebeveiligingsbeleid.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Hulst 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 informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsjaarplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsjaarplan 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.
- 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.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgesteld en vastgelegd.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering,

openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid en het informatiebeveiligingsjaarplan 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 afdelingshoofden en ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de informatie, informatiesystemen en procesautomatiseringssystemen 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 rechtstreeks aan het management.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingshoofden zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, 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.
- Afdelingshoofden dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbenden de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. De procesbeheerder (vaak in samenwerking met de functioneel beheerder en de CISO) voeren quickscan Baselinetoets informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging maakt deel uit van de functionerings-/beoordelingssystematiek en wordt besproken tussen teamleider respectievelijk afdelingshoofd en de medewerker.

2.6.4 Risicomanagement

Binnen de BIO wordt uitgegaan van een risicogerichte benadering van informatieveiligheid. Deze benadering is gericht op het in kaart brengen van invloeden waar we geen of onvoldoende invloed op hebben. Daar waar onvoldoende maatregelen zijn getroffen kan de organisatie kwetsbaar zijn. Een kwetsbaarheid levert automatisch ook een mate van onzekerheid op voor de bedrijfsprocessen en daarmee de doelstellingen van de organisatie.

Hoewel overheidsorganisaties in hoge mate dezelfde diensten leveren, wil dat niet zeggen dat de omstandigheden ook overal hetzelfde zijn. De wijze van organiseren, de gebruikte techniek en de kennis en vaardigheden van het personeel kunnen per organisatie verschillen. De BIO gaat uit van een basisbeveiligingsniveau (BBN). Bovenop de basis kunnen aanvullende maatregelen nodig zijn. Er kunnen ondanks de implementatie van de BIO nog kwetsbaarheden bestaan. Door organisatorische en technische veranderingen kunnen daarnaast steeds weer nieuwe kwetsbaarheden ontstaan. Het Basisbeveiligingsniveau wordt bij gemeente Hulst bepaald door het uitvoeren van een Baselinetoets (BLT). De BLT wordt uitgevoerd bij de aanschaf van nieuwe applicaties/systemen of wijzigingen in functionaliteiten van systemen/applicaties. De Baselinetoetsen worden jaarlijks herzien totdat alle verbetermaatregelen zijn doorgevoerd.

De overheidsmaatregelen in de BIO hebben een verplicht karakter en dienen daardoor geïmplementeerd te worden. Voor het deel van de controls met overheidsmaatregelen zullen we een GAP-analyse uitvoeren. Op deze manier kunnen we bepalen in welke mate we wel of niet voldoen aan deze verplichte overheidsmaatregelen. De resultaten van de GAP-analyse zijn terug te vinden in het jaarplan informatiebeveiliging gemeente Hulst.

2.6.5 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een jaarplan informatiebeveiliging opgesteld onder leiding 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 afdelingshoofden of teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse;
  - Programmaplan Agenda Digitale Veiligheid 2022-2026;
  - Resultaten van de GAP-analyse.

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 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: directie

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De directie zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Hulst gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: afdelingshoofden en teamleiders

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingshoofden. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid voor informatiebeveiliging kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teamleiders kunnen een bijdrage leveren en/of de taken overnemen als het gaat om de uitvoerende werkzaamheden. Bij gemeente Hulst zijn de teamleiders verantwoordelijk voor het op orde zijn van hun eigen (werk)processen in het team en de uitvoering hiervan door de medewerkers.

Afdelingshoofden rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in een overleg met de CIO en CISO.

Taken van de afdelingshoofden in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures;
- Het voldoen aan wetgeving die op hun afdeling van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is;
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures;
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Taken van de teamleiders in het kader van informatiebeveiliging zijn:
- Preventie, herkennen en signaleren van beveiligingsincidenten
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld;
- Signaleren en oppakken van knelpunten in het team op het gebied van privacy en informatiebeveiliging;
- Monitoren van de uit te voeren verplichtingen bij nieuwe applicaties of proceswijzigingen;
- Contactpersoon tussen de CISO, PO en het team.

3.2.1 Uitvoering: Functioneel beheer
Geheel in lijn met de BIO is het eigenaarschap van applicaties belegd in de lijnorganisatie en is het betreffende afdelingshoofd eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen. Per applicatie is door het afdelingshoofd een functioneel beheerder aangewezen die de dagelijkse zorg draagt voor het functioneren van de applicatie. Dit bevat ook het implementeren van de van toepassing zijnde beveiligingsnormen zoals beschreven in de BIO. Via dataclassificatie door middel van het uitvoeren van een Baselinetoets, wordt bepaald welke beveiligingsnormen van toepassing zijn. Daarnaast draagt de functioneel beheerder in samenwerking met de procesbeheerder en de CISO, zorg voor de eventuele verplichte audits.

3.2.2 Controle en verantwoording
Dit Strategisch Beleid is een verantwoordelijkheid van het college van B en W van de gemeente Hulst. Het college van B en W, de directeur en het management van de gemeente Hulst zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het management is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het management rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.2.3 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingshoofden. De afdelingshoofden leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

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

4. Tactische uitgangspunten BIO

De tactische uitgangspunten van het informatieveiligheidsbeleid gaan in op de beheersdoelstellingen per onderdeel van de BIO. De BIO kent naast het ISMS een aantal inhoudelijke onderwerpen. Deze onderwerpen staan veelal niet op zich omdat onderwerpen vaak samen zorgen voor een niveau van veiligheid. Zo is er samenhang tussen de HRM processen instroom, doorstroom en uitstroom en het beheer van autorisaties. Op het gebied van communicatie op het internet is er samenhang met het beheer van encryptiesleutels. Wanneer een organisatie excelleert op één gebied kan een ander gebied weer voor onveiligheid zorgen. We zeggen dan ook wel dat de beveiliging zo goed is als de zwakste schakel in de keten. Per onderwerp zullen we op tactisch niveau aangeven wat het doel is van dit beheersaspect.

Veilig personeel
Doelstelling
Medewerkers dienen geschikt te zijn en geschikt te blijven voor hun functie. De belangrijkste waarborg is het aantrekken van betrouwbaar en geschikt personeel en de zorg dat de medewerkers geschikt

blijven voor hun functie, zodat ze op een goede wijze met de informatie van de organisatie om kunnen gaan tijdens en na afloop van hun contract.

Toelichting
Informatieveiligheid valt en staat met de kennis, houding en gedrag van de medewerkers. Om de juiste medewerkers in de organisatie te krijgen, deze gedurende hun loopbaan te trainen en te coachen zodat zij over de kennis en vaardigheden beschikken die nodig zijn om hun functie naar behoren uit te voeren.

Beheer van bedrijfsmiddelen
Doelstelling
De organisatie gebruikt een groot aantal systemen (apparatuur, devices en software) om de informatievoorziening te faciliteren. Het doel van dit beheeraspect is het identificeren van alle hard- en software zodat deze op een adequate wijze beheerd en beveiligd kunnen worden.

Toelichting
Om informatie adequaat te kunnen beheren is het van belang om inzicht te hebben in diverse ICT-componenten die gebruikt worden om informatie te verwerken. Er kan pas adequaat beheer gevoerd worden wanneer je in het zicht hebt wat je moet beheren. De administratie waarin de ICT- componenten worden beschreven (ook wel configuratie management database CMDB) genoemd dient als basis van diverse beheerprocessen zoals patchmanagement, incidentmanagement evenals het informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging door de verantwoordelijk manager kan worden bepaald.

Toegangsbeveiliging
Doelstelling
Toegang tot informatie en informatie op een passende wijze beveiligen zodat onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie wordt voorkomen.

Toelichting
Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen invoeren en onderhouden wordt er een toegangsrichtlijn opgesteld. Naast deze toegangsrichtlijn heeft ieder informatiesysteem nog een specifiek gedefinieerde uitwerking omtrent toegang, dat is afgestemd in samenspraak met de applicatiebeheerder en de CISO op het beveiligingsniveau van de informatie.

Cryptografie
Doelstelling
Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Toelichting
Een effectieve manier om informatie te beveiligen tegen onbevoegde inzage is het versleutelen van deze informatie. Dit gebeurt bij voorkeur zowel bij de opslag als het transport. Belangrijk beheeraspect is dat versleuteling wordt toegepast met behulp van sleutels die veilig genoeg zijn conform de actuele standaarden. Om verlies van data te voorkomen is het van belang dat er ten aanzien van het beheer van de sleutels goede maatregelen zijn getroffen.

Fysieke beveiliging
Doelstelling
Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Toelichting
Een belangrijk aspect van informatieveiligheid is het voorkomen dat onbevoegden fysiek toegang hebben tot informatie. Ondanks de snelle ontwikkeling van digitale informatieverwerking is veel informatie ook nog analoog beschikbaar. Daarnaast dienen de informatie verwerkende computers en apparaten beschermd te worden tegen onbevoegde toegang. Fysieke beveiliging wordt ingezet om onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Beveiliging bedrijfsvoering
Doelstelling
Correcte en veilige bediening van informatie verwerkende faciliteiten ter voorkoming van ongewenste aanpassingen, verlies en diefstal van gegevens.

Toelichting

Informatie wordt door de gehele organisatie heen gebruikt en daarnaast wordt informatie ook gedeeld met andere organisaties. Doordat informatie wordt hergebruikt is het van belang dat informatie goed wordt beheerd. Uitgangspunt hierbij is dat iedere brok aan informatie wordt beheerd vanuit een aangewezen organisatieonderdeel die daarvoor eenduidige processen en controlemaatregelen heeft ingericht om de kwaliteit van de informatie te kunnen waarborgen.

Communicatiebeveiliging
Doelstelling
Informatie van de organisatie die via het interne netwerk intern dan wel extern wordt getransporteerd dient afdoende te worden beveiligd om onderschepping en/of ongewenste aanpassing van informatie te voorkomen.

Toelichting
Bij het beheer van netwerken moet onderscheid worden gemaakt tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via netwerken dienen extra maatregelen ter waarborging van de veiligheid te worden getroffen om te zorgen dat de data-integriteit en de vertrouwelijkheid bij transport is gewaarborgd. Zeker nu we steeds meer met externe partijen samenwerking is het van groot belang te kunnen vertrouwen op de communicatiekanalen.

Aankoop, ontwikkeling en onderhoud van informatiesystemen
Doelstelling
Waarborgen dat informatieveiligheid integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus en bij het testen van systemen. Dit zowel bij interne systemen als bij gebruik van een cloud leverancier.

Toelichting
Bij de ontwikkeling van (informatie)systemen moeten beveiliging en privacy vanaf aanvang in het ontwerpproces of in het pakket van eisen worden meegenomen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd en of aan de eisen vanuit de AVG en de BIO wordt voldaan. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn. Bij de toepassing van nieuwe technologieën (zoals bijvoorbeeld Artificial Intelligence) dient extra aandacht te worden besteed aan ethiek, eventuele risico's voor de burger en de transparantie hierover.

Leveranciers
Doelstelling
Er dienen met leveranciers overeenkomsten te worden gesloten die ervoor zorgen dat de dienstverlening in overeenstemming is met het informatieveiligheidsbeleid en de wettelijke bepalingen.

Toelichting
Organisatie zijn ten aanzien van de verwerking van informatie sterk afhankelijk van diverse leveranciers. Dit niet alleen vanwege de aanschaf en de primaire werking maar vanwege de dienstverlening die verbonden is aan de primaire dienstverlening. Het is van belang om met de leveranciers goede afspraken te maken over de aard van de dienstverlening. Daarnaast dient te worden gecontroleerd of ook aan deze eisen wordt voldaan door de leverancier.

Incidenten- en kwetsbaarhedenbeheer
Doelstelling
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheidsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

Toelichting
Het beheer van incidenten kent twee gezichtspunten. Ten eerste dienen incidenten snel en adequaat te worden afgehandeld maar daarnaast zijn incidenten ook een signaal dat bestaande maatregelen wellicht niet voldoen. Het is dus van belang dat een incident zowel goed en snel wordt afgehandeld. En dat daarnaast een analyse plaatsvind zodat duidelijk is wat de oorzaak is geweest en hoe we er structureel voor kunnen zorgen dat een dergelijk voorval niet meer plaats kan vinden.

Continuïteitsbeheer
Doelstelling
Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

Toelichting

Continuïteitsbeheer heeft als doel om ervoor te zorgen dat de dienstverlening intern en extern ongestoord kan plaatsvinden. Om de dienstverlening ongestoord doorgang te laten vinden dienen we zowel te kijken naar de systemen die nodig zijn als naar de facilitaire voorzieningen.

Naleving
Doelstelling
Verzekeren dat informatieveiligheid wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie ter voorkoming van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatieveiligheid en beveiligingseisen.

Toelichting
Het uitdragen van beleid en het opstellen van procedures moeten een waarborg bieden voor de kwaliteit. Het controleren van het beleid en de naleving van de procedures zijn erop gericht om te beoordelen of beleid en procedures ook werkbaar zijn in de praktijk. Daarnaast kunnen controles ook gebruikt worden om verdere sturing te geven aan de organisatie en zijn daarmee een essentieel onderdeel van de governance.