GEMEENTEBLAD
Officiële uitgave van de gemeente Hulst
Nr. 293499
4 december 2019

Strategisch Informatiebeveiligingsbeleid 2019 – 2022 gemeente Hulst

Het college van burgemeester en wethouders van de gemeente Hulst;

besluit

vast te stellen:

het 'Strategisch Informatiebeveiligingsbeleid 2019 – 2022 gemeente Hulst'

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2019 tot 2022 en vervangt het in 2016 vastgestelde 'Informatiebeveiligingsbeleid 2016–2019'. Dit beleid is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.
Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2019–2022' zet de gemeente 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 strategische beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO - zie bijlage 1). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG (zie bijlage 2).

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 die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door directie) 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 en de uitvoering van risico-analyses. Daarin staan dan ook 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.

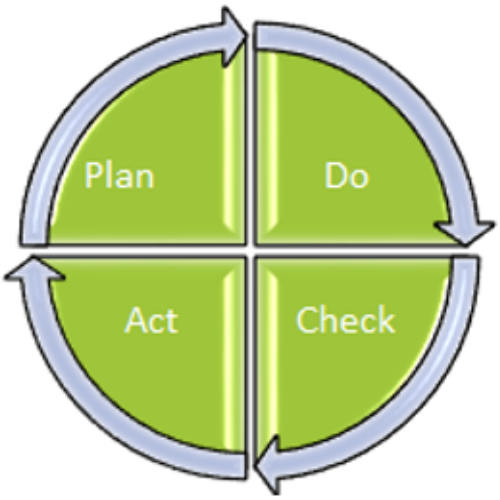
1.2 Wat is informatiebeveiliging

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 (continuïteit), 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 politiek bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitieniveau

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 de kwaliteitseisen te beschermen.

Om informatieveiligheid te realiseren hebben we een systeem nodig wat ons helpt om op een adequaat niveau te komen. 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 presenteren van het Strategisch Informatiebeveiligingsbeleid voor de jaren 2019 tot 2022. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).
De beveiligingsrichtlijn SUWI, beveiligingsrichtlijn Basisregistratie Personen en de beveiligingsrichtlijn waardedocumenten maken onderdeel uit van dit strategisch beleid (zie bijlage 3).

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[1]is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG (Baseline Informatiebeveiliging Gemeenten). 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 zij op voorhand keuzes en continu afwegingen maken of informatie in

1) *BIO: Zie bijlage 1*

bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging[2]

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die het college aan 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 Nederlandse Gemeenten

Het dreigingsbeeld 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 ook 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.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid 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 informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[3] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen.

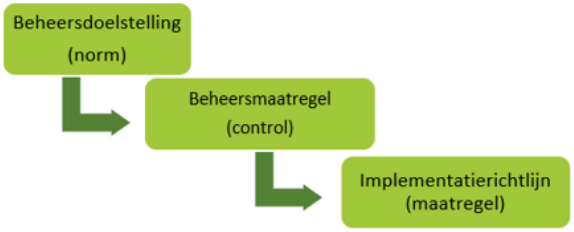
2.3.1 Opzet BIO

De BIO kent dezelfde opbouw als de ISO27001. De niveaus beheersdoelstellingen, beheersmaatregelen en implementatierichtlijnen zijn identiek aan de ISO27002. De beheersdoelstellingen (normen) kennen beheersmaatregelen (controls) die op hun beurt zijn uitgewerkt in implementatierichtlijnen (maatregelen). Een deel van de controls is uitgewerkt in verplichte implementatierichtlijnen (overheidsmaatregelen), omdat zij:

- Voortvloeien uit wet- en regelgeving;
- Zo basaal zijn dat zij het fundament vormen van een betrouwbare informatievoorziening;
- Dienstbaar zijn aan de beveiliging in een procesketen of netwerk.

2) ***10 Bestuurlijke principes voor informatiebeveiliging: Zie bijlage 2; Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Vereniging Nederlandse Gemeenten (VNG)***

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



2.4 Plaats van het strategisch beleid
Het strategische beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven aan de verdere invulling van informatiebeveiliging op tactisch- en operationeel niveau.
Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactisch beleid en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'gemeentelijk informatiebeveiligingsplan'.

2.4.1 Gemeentelijk Informatiebeveiligingsplan
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 informatieveiligheid 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 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, informatie en gegevens van de gemeente, externe partijen (bijvoorbeeld politie) en dienstenleveranciers, 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. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze zijn in aanvullende beveiligingsrichtlijnen 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 en de afdelingshoofden 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.

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.

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 & W is eindverantwoordelijke voor de informatiebeveiliging.
- 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 gemeentelijk informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het gemeentelijk informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed 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 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.

2.6.3 Praktische invulling uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
- Het college van B & W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- 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 Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie.
- Er dient 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 auditplannen.
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging 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 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 beveiligings-procedures.
- 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 rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

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 zijn aanvullende maatregelen nodig. Er kunnen ondanks de implementatie van de BIO nog kwetsbaarheden bestaan. Door organisatorische en technische veranderingen kunnen daarnaast steeds weer nieuwe kwetsbaarheden ontstaan.

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.

2.6.5 Randvoorwaarden
Belangrijke randvoorwaarden zijn:
- 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.

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) 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 portefeuillehouder binnen het college gevraagd en ongevraagd geïnformeerd wordt 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
Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingshoofden. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn

(CISO). Deze verantwoordelijkheid 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. 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 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;
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.3 Controle en verantwoording
Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente Hulst. De bestuurders en directie van de gemeente Hulst zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het tonen 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 jaarlijks over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat 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&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 wordt 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 Baseline Informatiebeveiliging Overheid
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 daar de 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 beheer aspect 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 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 devices 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 ieder brok aan informatie wordt beheerd vanuit een

aangewezen organisatie-onderdeel 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 aan eisen worden meegenomen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd en aan de eisen vanuit de AVG wordt voldaan. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn.

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
Organisaties 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 de eisen wordt voldaan.

Incidentenbeheer

Doelstelling
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheid incidenten, 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 plaatsvindt 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.

Aldus besloten in de vergadering van burgemeester en wethouders van 12 november 2019.

Burgemeester en wethouders van de gemeente Hulst,
De secretaris,

De burgemeester,

5. Bijlagen

Bijlage 1: Baseline Informatiebeveiliging Gemeenten
Baseline Informatiebeveiliging Overheid

Bijlage 2: 10 Bestuurlijke principes voor informatieveiligheid
10 bestuurlijke principes voor informatieveiligheid

Bijlage 3: Beveiligingsrichtlijnen SUWI, Basisregistratiepersonen, waardedocumenten