Gemeente Hof van Twente

GEMEENTEBLAD

Officiële uitgave van de gemeente Hof van Twente

Nr. 131229

25 mei

2020

Strategisch informatieveiligheidsbeleid 2020-2022 Gemeente Hof van Twente

Inhoudsopgave

Documentmanagement

1.1 Auteurs en documenteigenaar

Aan College B&W, Managementteam
Auteur Esther Apperloo, CISO (documenteigenaar)
Datum April 2020
Status Concept

1.2 Gerelateerde documenten

Naam Eigenaar
Tactische informatieveiligheidsbeleid Esther Apperloo
Programma informatieveiligheid & privacy Esther Apperloo
Privacybeleid Saray Eggink

1.3 Vaststelling en periodieke actualisering

Dit document wordt vastgesteld door het college van burgemeester en wethouders. Voor tussentijdse wijzigingen en/of aanvullingen geldt het volgende:

- vaststelling door B&W als het beleidsmatige aanpassingen betreft;
- vaststelling door opdrachtgever Informatiebeveiliging bij overige, specifieke inhoudelijke documenten en aanpassingen, onder andere de organisatie inrichtingen.

Het strategische informatiebeveiligingsbeleid geldt voor een periode van 3 jaar. Eenmaal per jaar of zo nodig vaker beoordeelt documenteigenaar het document op actualiteit, volledigheid, overbodigheid en relevantie van de diverse aspecten. De documenteigenaar voert eventuele wijzigingen door en legt de gewijzigde versie vervolgens ter vaststelling voor aan het bevoegde management. De wijzigingen worden in de organisatie uitgedragen door de betreffende actiehouder, die door de opdrachtgever wordt aangewezen.

Na vaststelling van dit beleid door het college wordt dit beleid gepubliceerd en via het lijnmanagement gecommuniceerd met medewerkers en relevante externe partijen. Verdere communicatie momenten zijn uitgewerkt in het programma informatieveiligheid & privacy.

2. Inleiding

Informatiebeveiliging en bescherming van de persoonlijke levenssfeer (privacy) van personen bestaat uit een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische en juridische aard met als doel:
• behoud van de beschikbaarheid van de informatie (geen uitval van systemen, waarborgen continuïteit);
• betrouwbaarheid/integriteit van de informatie (gegevens zijn juist, actueel en volledig);
• vertrouwelijkheid van de informatie (onbevoegden hebben geen toegang tot informatie; persoonsgegevens worden alleen verwerkt in overeenstemming met de daarvoor geldende wetgeving).

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie én vertrouwelijke omgang met informatie is essentieel voor een gemeente omdat het de basis is voor juist en efficiënt handelen. Gemeente Hof van Twente heeft haar ambities vastgelegd in de Coalitievisie 2018-2022: 'Samen doen' en dient hierbij transparant te zijn richting haar inwoners en proactief verantwoording af te leggen aan interne en externe toezichthouders. Dit strategische informatiebeveiligingsbeleid is het kader voor informatiebeveiliging. Hierbij volgen wij het landelijk voorbeeld vanuit de Informatie Beveiligingsdienst (IBD) en werken wij stapsgewijs toe aan het voldoen aan de Baseline Informatiebeveiliging Overheden (BIO).

2.1 Doel van dit beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Dit beleid geldt voor de jaren 2020 tot en met 2022 en vervangt het
"Beleidsplan informatieveiligheid & privacy 2017". Het is het bestuurlijk kader om de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens en andere informatie(systemen) te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving. Dit strategische informatiebeveiligingsbeleid is gericht op het:
• Verstevigen van de governance:
De verantwoordelijkheid voor informatieveiligheid is primair in de lijn belegd. Dit betekent een centrale rol voor afdelingsmanagers.
• Risico gebaseerd sturen:
Dit betekent dat het management verantwoordelijk is voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.
• Goede verantwoording, geïntegreerd in de planning- en control cyclus:
Informatieveiligheid is opgenomen in de integrale P&C- cyclus. Implementatie en verantwoording vindt plaats via de planning van de ENSIA verantwoording. Er vindt een uniforme verantwoording plaats aan interne en externe toezichthouders.

Dit beleid draagt bij aan een verdere professionalisering van informatieveiligheid en hiermee aan het behalen van de gestelde doelen in de Coalitievisie 2018-2022: 'Samen doen'.

2.2 Scope van het strategische informatieveiligheidsbeleid
Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) 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. Het heeft betrekking op het politiek bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen van de gemeente.

3. Beleidskader informatieveiligheid

3.1 Plaats van dit beleid
Het strategisch informatiebeveiligingsbeleid is in lijn met de relevante landelijke en Europese wet- en regelgeving. Het strategisch informatiebeveiligingsbeleid is een onderdeel van het informatiebeleid en bestaat uit de volgende documenten:
1. strategische informatiebeveiligingsbeleid: dit beleidsdocument, waarin de uitgangspunten en randvoorwaarden zijn geschetst en de rollen zijn belegd ten aanzien van informatieveiligheid.
2. tactische informatiebeveiligingsbeleid: een handboek waarin de strategische kaders zijn vertaald in operationele uitgangspunten, dit is gelijk aan de BIO.
3. specifieke beleidskaders: dit zijn beleidsstukken per specifiek terrein, zoals o.a. toegangsbeveiliging, thuiswerkbeleid en back-up beleid.
4. informatiebeveiligingsbeleidsplan(nen): dit is o.a. het programma informatieveiligheid & privacy waarin staat beschreven wat wij per jaar gaan doen om geleidelijk aan de bio te voldoen.

In het tactische beleid staan onderwerp-specifieke beleidsregels die de implementatie van informatiebeveiliging verplicht stellen. De uitwerking van het strategische en het tactische beleid staat opgenomen in het programma informatieveiligheid & privacy. Dit plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen, zoals
- Basisregistratie Personen (BRP),
- Paspoorten en Nederlandse identiteitskaarten (PNIK),
- Digitale Identiteit (DigiD),
- Structureel Uitvoeringsorganisatie Werk en Inkomen (SUWI),
- Basisregistratie Adressen en Gebouwen (BAG),
- Basisregistratie Grootschalige Topografie (BGT),
- Basisregistratie Ondergrond (BRO)
- Algemene Verordening Gegevensbescherming (AVG).

Hiervoor gelden specifieke beleidskaders en/of informatiebeveiligingsplannen. Het onderwerp privacy is in een apart beleid opgenomen.

3.2 Grondslagen

Dit strategische informatiebeveiligingsbeleid is gebaseerd op:
• NEN-ISO/IEC 27001:2017
• NEN-ISO/IEC 27002:2017
• Baseline Informatiebeveiliging Overheid (BIO) en de 10 principes voor informatiebeveiliging (zie hoofdstuk 4).
• De architectuurprincipes van de gemeente (zie paragraaf 3.3)

3.3 Architectuurprincipes

Architectuurprincipes zijn richtinggevend en helpen gemeenten om bewust keuzes te maken bij het inrichten van de gemeentelijke processen, bijhorende informatievoorziening en zijn de basis om informatiebeveiliging te implementeren.
De gemeente Hof van Twente volgt hierbij landelijke richtlijnen van Nederlandse Overheid Referentie Architectuur (NORA) en de daarvan afgeleide Gemeentelijke Model Architectuur (GEMMA).

De acht GEMMA basisprincipes zijn:
1 Onze gemeente denkt vanuit de positie van de klant.
2 Onze gemeente gebruikt generieke processen en functies.
3 Onze gemeente voert regie over uitbestede diensten.
4 Onze gemeente biedt de klant een goede informatiepositie.
5 Onze gemeente digitaliseert haar diensten en processen.
6 Onze gemeente stelt openbare gegevens als open data beschikbaar.
7 Onze gemeente hergebruikt gegevens.
8 Onze gemeente gaat op een vertrouwde manier met gegevens om.
Deze architectuurprincipes dienen als een leidraad voor de procesarchitectuur.

3.4 Uitgangspunten

De belangrijkste uitgangspunten van dit informatiebeveiligingsbeleid zijn:
1. Dit beleid vormt samen met het tactische informatiebeveiligingsbeleid en het programma informatieveiligheid & privacy het kader om informatieveiligheid in de organisatie te borgen.
2. Informatiebeveiliging mag niet ten koste gaan van de veiligheid van personen.
3. Het college, het management en de teamcoördinatoren dragen dit beleid uit en sturen op de implementatie van dit beleid.
4. Informatiebeveiliging is georganiseerd. Het management heeft continu aandacht voor het vergroten van het bewustzijn van medewerkers om zo de menselijke schakel te versterken.
5. De rol van de coördinator van informatiebeveiliging (Chief Information Security Officer: CISO), is ingevuld.
6. Regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid zijn vastgesteld.
7. Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én de coördinatie op dit proces is informatieveiligheid binnen de organisatie verankerd.
8. Informatiebeveiliging is een onderdeel van risicomanagement.

3.5 Randvoorwaarden

Belangrijke randvoorwaarden om dit beleid te implementeren zijn:
1. De informatiebeveiligingstaken zijn belegd binnen de bedrijfsprocessen en de benodigde kwalitatieve en kwantitatieve resources zijn beschikbaar gesteld.
2. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures. Medewerkers kennen de beveiligingsprocedures en gebruiken deze procedures. Medewerkers zijn daarnaast op de hoogte van eisen die vanuit wet- en regelgeving aan hun bedrijfsprocessen gesteld worden en kennen deze kaders.
3. Medewerkers gaan verantwoord om met (persoons)gegevens en andere informatie(systemen), spreken elkaar aan op onveilig gedrag en melden mogelijke hiaten direct aan de leidinggevenden.
4. De informatiebeveiliging maakt deel uit van afspraken met ketenpartners en dienstenleveranciers.
5. Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd bij alle lagen binnen de organisatie, ketenpartners en externe partijen.
6. Er zijn voldoende maatregelen geïmplementeerd die zorgen dat kwetsbaarheden in bedrijfsprocessen worden verkleind. Hierdoor worden informatiebeveiligingsincidenten verkleind en de effecten van de incidenten beperkt.
7. Periodiek worden onafhankelijke audits uitgevoerd om vast te stellen of de vereiste maatregelen uit het beleid in voldoende mate zijn geborgd.
8. De digitale weerbaarheid wordt verhoogd door de basis op orde te brengen.
9. Security en privacy by design principes worden toegepast bij innovaties. Denk hierbij aan common ground, internet of things (IoT) en Smart City, kunstmatige intelligentie (AI).

Zolang deze uitgangspunten en randvoorwaarden zijn ingericht is de informatieveiligheid voldoende geborgd.

3.6 Financiën

Informatiebeveiliging is de verantwoordelijkheid van het lijnmanagement en is integraal onderdeel van de bedrijfsvoering. De kosten voor het zorgen voor een efficiënte uitvoering van de maatregelen met betrekking tot het gemeentebrede basisniveau aan beveiliging van informatie worden, net zoals hiervoor, in eerste instantie gedekt uit bestaande kostenposten. Hierbij valt te denken aan kosten voor specifieke maatregelen, audits en kwetsbaarheidsanalyses, bewustwordingscampagnes voor het personeel, en de aanschaf en onderhoud van specifieke hulpmiddelen voor het registreren van gegevensverwerkingen of het beheren van maatregelen (ISMS). Met deze keuze gaan we in tegen het landelijke advies waarin wordt geadviseerd dat de CISO haar eigen budget heeft. Mochten we in de loop van tijd erachter komen dat dit niet werkt en de CISO haar eigen budget nodig heeft, dan kan dit altijd later aangepast worden in overleg met afdeling bedrijfsvoering. Voor nu loopt de samenwerking tussen de CISO en afdeling bedrijfsvoering goed waardoor er geen verandering wordt verwacht.

4. Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van dit informatiebeveiligingsbeleid zijn hieronder beschreven.

4.1 Een nieuwe baseline voor informatieveiligheid

De Baseline Informatiebeveiliging Overheid (BIO) is vanaf 2020 het nieuwe normenkader voor de gehele overheid. Deze baseline is ten opzichte van de Baseline Informatiebeveiliging Gemeenten (BIG) meer gericht op risicomanagement. De bestuurders en de (afdelings)managers hebben een prominente rol met betrekking tot informatiebeveiliging en met de komst van de BIO een cruciale rol met betrekking tot risicomanagement. Hierbij maakt het bestuur en het management op voorhand keuzes en continu afwegingen of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

De BIO helpt het management bij het nemen van haar verantwoordelijkheid ten aanzien van informatiebeveiliging. In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus gedefinieerd met bijbehorende verplicht in te richten beveiligingsmaatregelen. Het management bepaalt op basis van een risicoafweging, hoe aan deze beveiligingsmaatregelen kan worden voldaan. Waar naleving (nog) niet volledig mogelijk is, maakt het management de aanwezige risico's inzichtelijk aan hun stakeholders.

Het management legt verantwoording af over de risicoafweging en over de effectieve invulling van de beheersmaatregelen. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over informatiebeveiliging. De BIO biedt hiermee de basis om te zorgen dat informatiebeveiliging geïmplementeerd en geborgd wordt.

4.2 Handvatten voor de rol van de bestuurder
VNG heeft aan het gemeentelijk bestuur de 10 principes van informatiebeveiliging uitgereikt. Deze principes bieden het bestuur handvatten op welke wijze het zijn rol kan invullen bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers.

De 10 principes zijn:
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.

Deze 10 principes staan nader uitgewerkt in de uitgewerkte rolverdeling van hoofdstuk 6.

5. Organiseren van informatiebeveiliging
De wijze waarop het informatiebeveiligingsbeleid binnen de gemeente is verankerd, vormt het kader van de borging op informatiebeveiliging. Het vaststellen van een beheerkader is van belang om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te borgen.

Het college, het management en de teamcoördinatoren spelen een cruciale rol bij het uitvoeren van dit beleid. De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten. Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. Hieronder is toegelicht welke rollen, taken en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn belegd in de organisatie. In het kopje ‘overige rollen’ zijn de specifieke rollen uitgewerkt.

5.1 Gemeenteraad
De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan de gemeenteraad toekent.

5.2 College van burgermeester en wethouders
Het College van Burgemeester en Wethouders is integraal (politiek) verantwoordelijk voor de borging van informatieveiligheid binnen de gemeente. Zij stelt kaders op voor informatieveiligheid (dit strategische beleid). Bij het onderwerp waardedocumenten is bij wet bepaald dat de bevoegdheid voor het vaststellen van kaders bij de burgemeester ligt in plaats van bij het college. De ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging is door het college gemandateerd aan de gemeentesecretaris.

Zowel het college van Burgemeester en Wethouders als de Raad (controle functie) kunnen opdracht geven om controle te laten uitvoeren. Het college legt verantwoording af aan de Raad en aan externe toezichthouders.

5.3 Het management
Het management is ambtelijk verantwoordelijk voor kaderstelling en sturing op tactisch niveau. Het management stuurt hierbij op concernrisico’s. De gemeentesecretaris draagt de gemandateerde verantwoordelijkheid voor informatieveiligheid.

Het management :
- zorgt voor voldoende resources om informatiebeveiliging in de organisatie te borgen.
- adviseert het college van B&W over het vast te stellen strategische beleid.
- zorgt dat het tactische (specifieke) beleid, informatiebeveiligingsplan(nen) en procedures worden opgesteld en vastgesteld.
- draagt het informatiebeveiligingsbeleid uit aan de organisatie en stuurt op concern risico’s.

• zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een proceseigenaar en ziet erop toe dat de proceseigenaar adequate maatregelen nemen.
• zorgt dat de teamcoördinatoren zich verantwoorden over de stand van zaken van informatieveiligheid binnen hun bedrijfsprocessen.
• Spreekt elkaar aan op naleving van dit beleid ook als verbetermaatregelen niet tijdig worden doorgevoerd.
• controleert of de getroffen maatregelen overeenstemmen met de gestelde eisen en of deze voldoende bescherming bieden.
• informeert de eindverantwoordelijke portefeuillehouder(s) binnen het College gevraagd en ongevraagd over informatiebeveiliging.
• ziet erop toe dat informatiebeveiligingsonderwerpen onderdeel zijn van de Planning & Control gesprekken en dat risicovolle onderwerpen worden opgenomen in de auditplannen.
• evalueert periodiek het informatiebeveiligingsbeleid. Voor het strategische beleid geldt een periode van 3 jaar of bij belangrijke wijzigingen.

5.4 De teamcoördinatoren (proceseigenaren)

De teamcoördinatoren (proceseigenaren) zijn operationeel eindverantwoordelijk voor de bedrijfsprocessen. De proceseigenaren zijn hiermee eigenaar van de applicaties binnen dit bedrijfsproces. Daar waar applicaties worden gebruikt in meerdere bedrijfsprocessen geldt dat het bedrijfsproces met het hoogst noodzakelijke beveiligingsniveau leidend is. De teamcoördinatoren kunnen hun verantwoordelijkheid niet delegeren, uitvoerende werkzaamheden wel. De teamcoördinatoren zorgen dat de inrichting van informatiebeveiliging en privacy voldoet aan de vereiste wet- en regelgeving. Hierbij worden zij ondersteund door de Privacy Officer (PO), de CISO en de Functionaris Gegevensbescherming (FG). Teamcoördinatoren rapporteren over de door hun tactisch- en operationeel uitgevoerde activiteiten aan het management.

De teamcoördinatoren:
• stellen specifiek beleid, specifieke informatiebeveiligingsplan(nen) en procedures, op en vast en dragen deze uit.
• sturen op beveiligingsbewustzijn, bedrijfscontinuïteit, privacy en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
• bespreken beveiligingsincidenten en de consequenties die dit heeft voor beleid en te implementeren beheersmaatregelen
• stellen het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast.
• signaleren vroegtijdig de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
• zorgen ervoor dat actuele risicoanalyse(s) worden uitgevoerd; implementeren de noodzakelijke informatiebeveiliging en privacy maatregelen. Deze beveiligingsmaatregelen bepalen zij op basis van risicomanagement en op basis van de kaders die eigen wet- en regelgeving met zich meebrengen.
• bewaken dat gekozen gegevensbeschermingsmaatregelen uit risicoanalyses worden opgenomen in doorontwikkelplannen. Stellen vast of de getroffen maatregelen aantoonbaar worden nageleefd. Rapporteren hierover aan de CISO en het management. Leveren input voor wijzigingen op maatregelen en procedures.
• stemmen de inhoudelijke aanpak om informatiebeveiliging te borgen af met de afdelingen en/of teams.
• leveren alle informatie aan die nodig is voor het invullen van het jaarlijkse verantwoordingstraject informatiebeveiliging (ENSIA).

5.5 CISO

De CISO ondersteunt vanuit een onafhankelijke positie de organisatie met betrekking tot het borgen van informatieveiligheid en heeft de mogelijkheid om rechtstreeks aan de directie en/of portefeuillehouder te rapporteren. De CISO is aangesteld volgens een vastgesteld CISO- functieprofiel.

De CISO is binnen de gemeente degene die kaders stelt op het gebied van informatiebeveiliging die voor de gehele organisatie gelden. Dit gebeurt uiteraard binnen de kaders die het college m.b.v. het strategisch beleid stelt. De CISO stuurt de organisatie aan met betrekking tot informatiebeveiliging. Hiermee zorgt de CISO ervoor dat de organisatie informatiebeveiliging doorvoert in haar processen, conform wet- en regelgeving. Daarnaast creëert de CISO het draagvlak voor informatiebeveiliging binnen de organisatie. De rol van de CISO is vooral adviserend en coördinerend. De CISO is in het kader van het verantwoordingstraject informatiebeveiliging tevens coördinator ENSIA.

Om aan bovenstaande te kunnen voldoen, heeft de CISO de volgende bevoegdheden:
• gevraagd en ongevraagd onderzoek kunnen doen en advies geven aan het college van B&W / Raad
• mogelijkheid tot direct ingrijpen zonder toestemming vooraf bij beveiligingsincidenten

De CISO is onderdeel van de concernstaf. De CISO voert geen operationele taken uit. Hiermee is het risico geminimaliseerd dat de eigenlijke taken van de CISO blijven liggen en de onafhankelijke positie in het geding komt. Daarnaast heeft de CISO rechtstreekse toegang tot de portefeuillehouder van informatiebeveiliging.

5.6 FG
De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op het gebied van privacy. De FG houdt toezicht op de wijze waarop de organisatie invulling geeft aan maatregelen om aan de privacywetgeving te voldoen. In het privacybeleid staan de taken van de FG opgenomen.

5.7 Privacy officer
Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

5.8 De operationele rollen

5.8.1 Beveiligingscontroller
Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.
De rol van beveiligingscontroller heeft op twee specifieke deelgebieden een voorgeschreven officiële benaming. Dit betreft het gebied van reisdocumenten en rijbewijzen. Het betreft de volgende benamingen:
• Beveiligingsfunctionaris reisdocumenten. Deze is verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
• Beveiligingsfunctionaris rijbewijzen. Deze is verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

5.8.2 Manager bedrijfsvoering:
De manager bedrijfsvoering is verantwoordelijk voor de fysieke toegangsbeveiliging en de kantoorinrichting (archiefkasten, kluizen enzovoort).

5.8.3 Afdeling I&A
Het team informatiemanagement, waarvan de Systeembeheerders deel uit maken, beheert de werkplekken, serverplatformen, lokale netwerken, wifi verbindingen, externe netwerkverbindingen (zoals Gemnet en Suwinet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en hulpmiddelen voor kantoorautomatisering. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

5.8.4 Team beleid en advies, cluster P&O:
Het team beleid en advies, cluster P&O is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviserende rol op het gebied van organisatie- en informatieprocessen.

5.8.5 De beveiligingsbeheerder
Deze rol draagt verantwoordelijkheid voor het beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. Binnen wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden, ten aanzien van specifieke methodes van gegevensverzameling. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan de beveiligingsbeheerder. De deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming, zijn de volgende: BRP,

reisdocumenten (officieel autorisatiebevoegde reisdocumenten/aanvraagstations) , rijbewijzen (autorisatiebevoegde rijbewijzen), BAG, SUWI (officieel Security Officer SUWI) en DigiD.
De autorisatiebevoegde reisdocumenten/aanvraagstations is verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).
De autorisatiebevoegde rijbewijzen is verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

5.8.6 Security Officer SUWI
De Security Officer beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen wordt geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert deze evenals de beveiliging van Suwinet en ziet erop toe of de maatregelen worden nageleefd. Het evalueren van de uitkomsten, advies geven hierover en het doen van voorstellen tot implementatie c.q. aanpassingen van plannen op het gebied van de beveiliging van Suwinet, behoort ook tot zijn takenpakket. De Security Officer heeft wat betreft rapportages formeel gezien een bijzondere rol. Hij rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke.

5.8.7 Functioneel applicatiebeheerder
Verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.

5.8.8 De medewerkers
Alle medewerkers dragen verantwoordelijkheid voor de informatieveiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien de betrouwbaarheid, de integriteit en de beschikbaarheid van de informatieprocessen waarbij zij zijn betrokken.

5.8.9 Gegevensbeheerder
De gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten, gericht op de inhoudelijke kwaliteitszorg van gegevensverzameling, gegevensverwerking en de informatievoorziening.

6. Communicatie en betrokkenheid stakeholders

6.1 Stakeholders
De gemeente Hof van Twente onderhoudt contacten met relevante overheidsinstanties (zoals externe toezichthouders), speciale belangengroepen (zoals Informatie Beveiligingsdienst Gemeenten) en interne stakeholders. Een nadere toelichting over het contact met de IBD is opgenomen in paragraaf 7.2. Stakeholders worden periodiek op de hoogte gesteld over de stand van zaken rondom informatiebeveiliging. Het onderwerp informatiebeveiliging is een vast onderdeel op de agenda van bestuur en lijnmanagement met als doel om sturing te kunnen geven. In de onderstaande tabel bij paragraaf 7.3 is opgenomen wat de contactmomenten met stakeholders zijn.

6.2 Aansluiting informatiebeveiligingsdienst gemeenten
Eén van de doelen van de IBD is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
Wij maken indien nodig gebruik van deze ondersteuning. De IBD informeert de gemeente via vastgestelde contactpersonen namelijk de algemeen contactpersoon informatiebeveiliging (ACIB) en de vertrouwde Contactpersoon Informatiebeveiliging (VCIB).

6.3 Contactmomenten

Contactmoment	Deelnemers	Frequentie	Doel
Opdrachtgever- opdrachtnemer	Concerncontroller CISO	Per kwartaal	Afstemming en coördinatie van informatieveiligheid
Bilateraal overleg bedrijfsvoering	Manager Bedrijfsvoering CISO	Per maand	Afstemming, sparren en updaten over de stavaza en aanpak informatieveiligheid

Kerngroep AVG	FG, PO, CISO, Juridisch medewerker W&I, Adviseur informatiemanagement	Per maand	Afstemmen en samenwerken om onze organisatie AVG-proof te maken (privacy)
Verantwoording ENSIA MT	MT, CISO	Per jaar	In beeld brengen risico's in proces en stand van zaken implementatie informatiebeveiliging
Crisisoverleg	FG, CISO, crisisteam	Per incident	Grip op crisis en input voor analyse en rapportage van incident
SIO	Manager Bedrijfsvoering, CISO, Beleidsmedewerker Informatievoorziening en medewerker informatiebeheer	Per kwartaal	Grip krijgen op de informatiestromen binnen onze organisatie en de buitenwereld en binnenwereld rondom informatiebeleid beter te verbinden.

7. Rapportagemomenten informatieveiligheid

Periodieke rapportages vloeien voort uit bovengenoemde contactmomenten met stakeholders. Rapportages worden opgesteld van incidenten, het verantwoordingstraject ENSIA en periodieke rapportages over de stand van zaken (P&C-cyclus). Aangezien het college en de Raad met name een rol spelen in het verantwoordingstraject wordt dit traject in onderstaande paragraaf toegelicht. In het programma informatieveiligheid & privacy zijn de onderdelen opgenomen van dit verantwoordingstraject.

7.1 Verantwoordingstraject ENSIA

Ter afsluiting van het jaarlijkse verantwoordingstraject rapporteren de afdelingsmanagers over de risico's binnen hun bedrijfsprocessen en over de stand van zaken van de implementatie van informatiebeveiliging van het afgelopen jaar. De CISO coördineert dit proces en stelt jaarlijks vóór 1 mei aan de hand van de deelrapportages van de afdelingsmanagers een bestuurlijke rapportage op voor de ambtelijke en bestuurlijke opdrachtgever.

Het college van B&W legt met deze bestuurlijke rapportage, een raadsbrief én met een aparte paragraaf in het jaarverslag verantwoording af aan haar interne toezichthouder de gemeenteraad én aan de externe toezichthouders (Rijk). Op deze wijze kan de ambtelijk en de bestuurlijk opdrachtgever en het college sturen op informatiebeveiliging. Zij kunnen hiermee besluiten nemen om informatiebeveiligingsrisico's tot een acceptabel niveau te brengen.

de Höfte 7, 7471 DK Goor
Postbus 54, 7470 AB Goor
0547 – 85 85 85
info@hofvantwente.nl