Lokale governance Informatiebeveiliging gemeente Tholen

Versiebeheer

Versie	Datum	Door	Wijzigingen
1.0	01-11-2017	CISO	Eerste versie
1.1	03-10-2019	CISO	Tekstuele aanpassingen, verantwoordelijkheden afdeling overstijgende (informatie)systemen, BRO beheerder toegevoegd, term ‘verantwoordelijken’ omgezet in ‘eigenaar’, verantwoordelijkheden en taken op afdelingsniveau en teamniveau omschrijving dubbelrollen toegevoegd, organigram en piramide geactualiseerd, bij de FG meldingen AP toegevoegd, toevoeging Collegeverklaring DigiD en SUWI-officer.

Inhoud

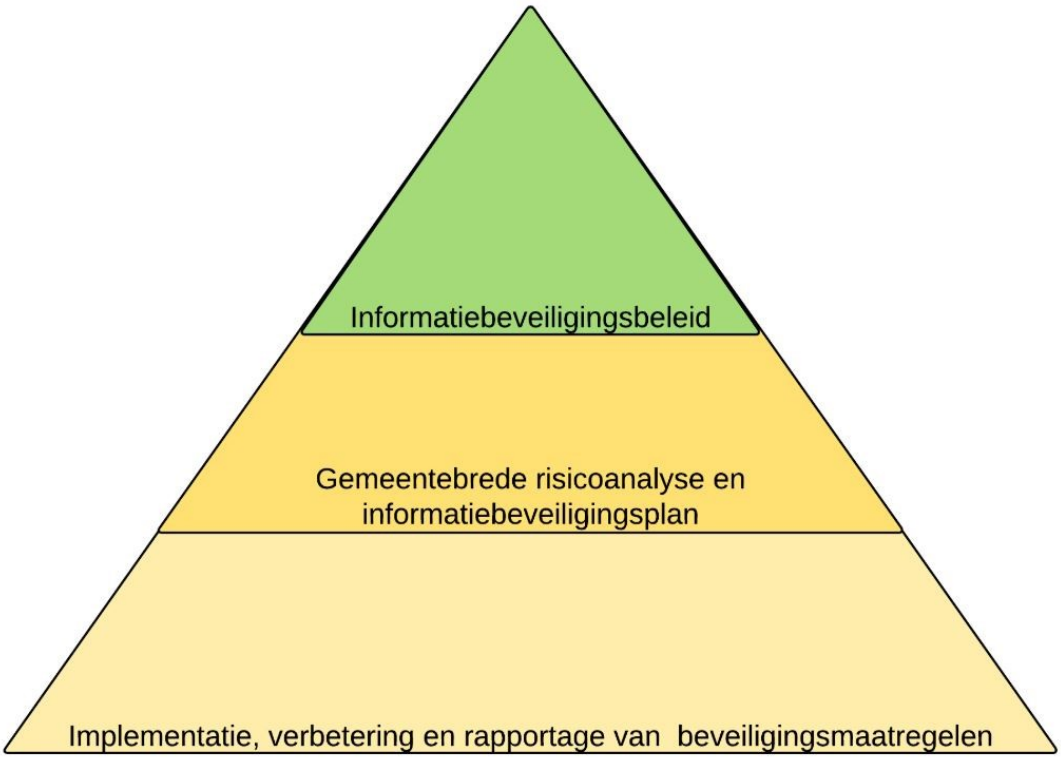
1. Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris.

De vaststelling en implementatie van de informatiebeveiligingsstructuur en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Tholen. Voor het nemen van operationele maatregelen is de gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij afdeling-overstijgende (informatie)systemen.

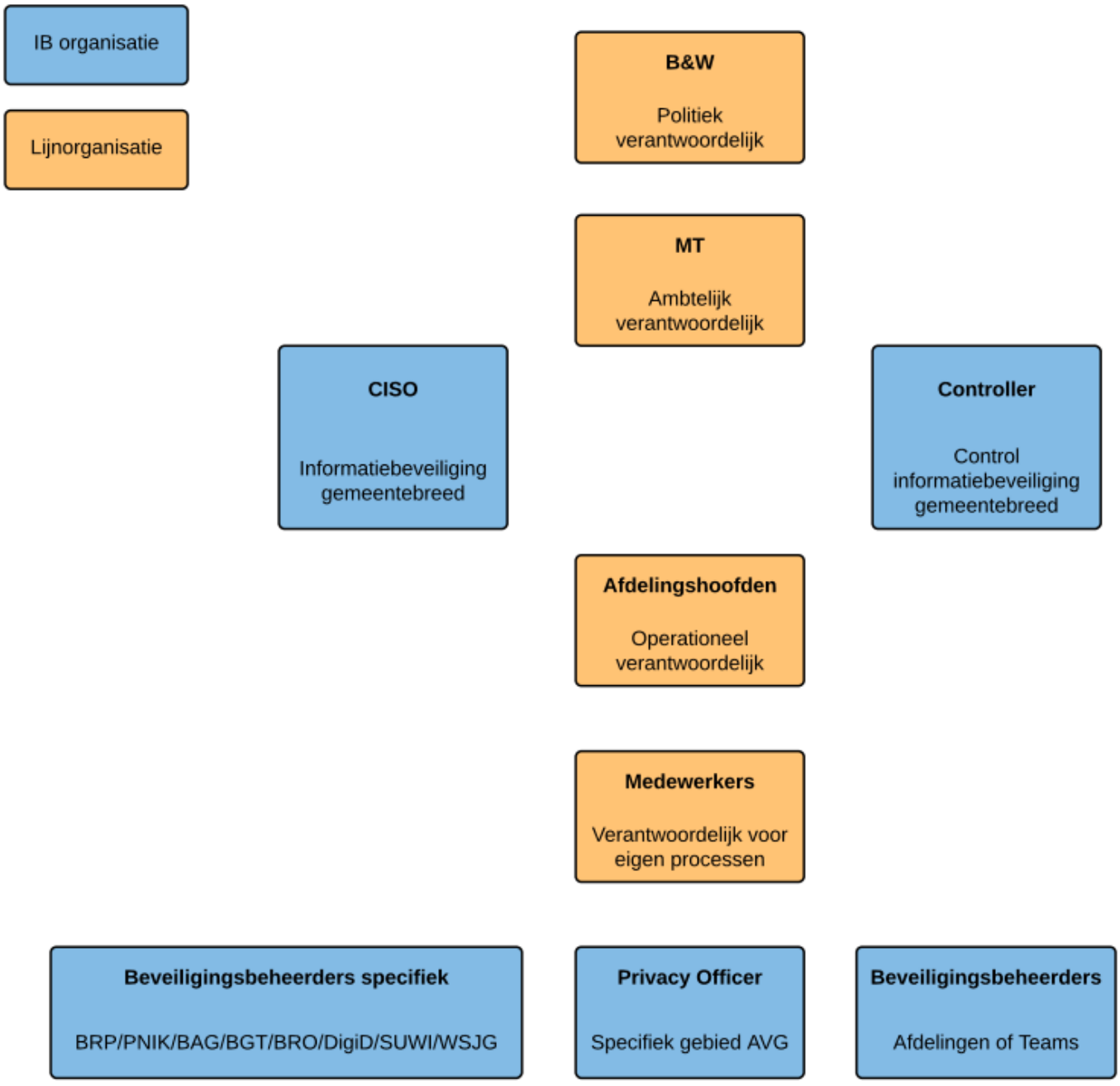
De afdelingshoofden zijn verantwoordelijk voor de informatiesystemen en processen waarvan zij eigenaar zijn. Zij dienen deze systemen en processen te classificeren en in te richten zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

1.1 Informatiebeveiligingspiramide



Afbeelding 1: Weergave van het strategisch informatiebeveiligingsbeleid, de tactische inrichting en de operationele uitvoering in de vorm van een piramide.

1.2 Organigram Informatieveiligheidsorganisatie



Afbeelding 2: Organigram van de informatiebeveiligingsorganisatie

2. Beschrijving van rollen, taken en verantwoordelijkheden

2.1 College Burgemeester & Wethouders

Het College van B&W van de gemeente Tholen draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan de gemeentesecretaris.

2.2 Gemeentesecretaris

De gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij leidinggevenden op organisatieniveau. De gemeentesecretaris en *het* MT hebben in ieder geval de volgende verantwoordelijkheden:

- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op concern risico's;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging;
- Het aanwijzen van een coördinator informatiebeveiliging en een controller informatiebeveiliging.

2.3 Functionaris Gegevensbescherming

De Functionaris gegevensbescherming (FG) is intern toezichthouder op de verwerking van persoonsgegevens. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG de Wet bescherming persoonsgegevens (Wbp). De FG ondersteunt bij de implementatie van essentiële elementen van de AVG, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen, "privacy by design en privacy by default", de administratie van gegevensverwerkingen, beveiliging van het verwerkingsproces, en melding van en communicatie over datalekken. De rol van FG heeft een strategisch karakter. De FG:

- Draagt zorg voor inventarisaties van gegevensverwerkingen;
- Houdt meldingen van gegevensverwerkingen bij;
- Behandelt vragen en klachten van mensen binnen en buiten de organisatie;
- Meldt vertrouwelijkheidsincidenten bij de Autoriteit Persoonsgegevens;
- Ontwikkelt Interne regelingen;
- Adviseert over technologie en beveiliging (privacy by design);
- Levert input bij het opstellen of aanpassen van gedragscodes.

2.4 Coördinator Informatieveiligheid (CISO)

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. De CISO ziet organisatiebreed toe op de naleving van het informatieveiligheidsbeleid en daaruit voortvloeiende maatregelen, zorgt voor onderzoek en adviseert in complexe beveiligingsvraagstukken, initieert organisatiebrede security awareness programma's en opleidingen en vervult een adviserende rol naar managementteam en gemeentebestuur. Tevens zorgt de coördinator informatiebeveiliging voor heldere communicatie bij incidenten op het vlak van informatiebeveiliging. De rol van CISO heeft een strategisch karakter. De CISO:

- Coördineert het formuleren van informatieveiligheidsbeleid en houdt dit actueel;
- Stelt het informatieveiligheidsplan op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering van informatieveiligheidsmaatregelen uit het informatieveiligheidsplan;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de directie en de leidinggevenden met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen en initieert organisatiebrede security awareness programma's;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en het informatieveiligheidsplan;
- Zorgt voor registratie van informatieveiligheidsincidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Initieert security audits (indien van toepassing ook risico analyses);
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages;
- Ziet toe op naleving van het informatieveiligheidsbeleid en daaruit vloeiende maatregelen.

2.5 Verantwoordelijkheden en taken op afdelingsniveau en teamniveau

De leidinggevenden (afdelingshoofden respectievelijk de teamleiders) zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling c.q. team. De leidinggevenden hebben in ieder geval de volgende verantwoordelijkheden*:*

- Het uit (laten) voeren van maatregelen uit het informatieveiligheidsplan die op de afdeling van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op resultaatsafspraken, beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de CISO*,* over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages;
- Classificeren van informatie (uitgangspunt GEMMA/GIBIT);
- Verstrekken, intrekken van en controleren op autorisaties;
- Incidenteel melden van datalekken aan betrokkenen

Een persoon vervult bij voorkeur slechts één van onderstaande functies. Het is echter mogelijk om door capaciteitsgebrek als afdeling of team te beslissen om een persoon meerdere rollen te geven. Het is echter niet wenselijk om een toezichthoudende rol te combineren met een verantwoordelijke of uitvoerende rol. Dit omdat de rol van toezichthouder in dat geval moeilijk zuiver uit te voeren valt. De slager keurt dan namelijk zijn eigen vlees.

2.6 Controller Informatieveiligheid

Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten. De Controller informatiebeveiliging:

- Toetst periodieke op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- Controleert de voortgang van het uitvoeren van de maatregelen uit het informatieveiligheidsplan;
- Houdt toezicht op de periodieke actualisatie van informatieveiligheidsbeleid en het Informatiebeveiligingsplan;
- Toets en bewaakt het niveau van informatieveiligheid;
- Toetst het evaluatieproces van beveiligingsincidenten.

2.7 Regiefunctionaris ICT

De Regiefunctionaris ICT is in de organisatie direct aanspreekpunt voor het ICT samenwerkingsverband ICTWBW. ICTWBW beheert de werkplekken, serverplatformen, lokale netwerken en de toegang tot straalverbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij verantwoordelijk voor het (laten) realiseren van 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 proceseigenaren voor (informatie)systemen afgelegd.

2.8 Privacy beheerder

Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming (AVG). De privacy beheerder is aanspreekpunt op het vlak van bescherming van persoonsgegevens en privacy binnen de organisatie en informeert en adviseert het management, bestuur en de collega's van de organisatie over de wijze waarop optimaal gebruik van informatie kan worden gemaakt. De Privacy beheerder draagt tevens bij aan de bewustwording en doorontwikkeling van Informatiebeveiliging en Privacy in de organisatie. De Privacy beheerder:

- Houdt toezicht op de naleving van specifieke regelgeving, waaronder de AVG en de Wet Basisregistratie Personen (BRP);
- Adviseert organisatiebreed over privacybescherming en over activiteiten ter bescherming van persoonsgegevens;
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Geeft aanwijzingen aan gebruikers van systemen met betrekking tot persoonsregistraties;
- Geeft (ongevraagd) advies over alle procedures en producten die betrekking hebben op de registratie van personen;
- Is contactpersoon van de gemeente voor de Autoriteit Persoonsgegevens (AP);
- Beheert het register met daarin alle persoonsregistraties die onder verantwoordelijkheid van de organisatie vallen.
- Levert een bijdrage aan de ontwikkeling van beleid, protocollen, normen, regelingen en gedragscodes.

2.9 ENSIA Coördinator

De ENSIA- Coördinator heeft een toezichthoudende en controlerende taak op ‘compliance’, d.w.z. overeenstemming van de beveiligingsorganisatie met een voorgeschreven norm (ENSIA). De ENSIA Coördinator werkt aan het begeleiden, bewaken en bijsturen van het ENSIA- verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor de hele gemeente en het organiseren van samenwerking.

2.9.1 Beveiligingsbeheerder

Deze rol is uitvoerend verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan, en gedefinieerd als Beveiligingsbeheerder. Hierna volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations), Rijbewijzen (Autorisatiebevoegde Rijbewijzen), BAG, SUWI (officieel Security Officer SUWI volgens het BKWI) en DigiD. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering: Facilitaire Zaken, ICT, DIV, P&O, WSJG, BRO en BGT/GEO. De beveiligingsbeheerder is -voor het toegewezen deelgebied- verantwoordelijk voor:

- Het geheel van activiteiten gericht op de naleving en verbetering van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid en de onderliggende informatieveiligheidsplannen. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons;
- De medewerker voert interne controles uit en let op de naleving van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.2 Beveiligingsbeheerder BRP

De Beveiligingsbeheerder BRP is verantwoordelijk voor het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen Basisregistratie Personen, het toetsen op de uitvoering van regelgeving en procedures ten aanzien van de Basisregistratie Personen, de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Basisregistratie Personen (College B&W).
De Beveiligingsbeheerder BRP:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.3 Beveiligingsbeheerder waardedocumenten (PNIK)

De Beveiligingsbeheerder waardedocumenten is verantwoordelijk voor het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen Waardedocumenten (PNIK), het toetsen op de uitvoering van regelgeving en procedures ten aanzien van het waardedocumentenproces, de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Waardedocumenten (College B&W). De Beveiligingsbeheerder waardedocumenten (PNIK):

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.4 Beveiligingsbeheerder BAG

De Beveiligingsbeheerder BAG is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

- Draagt zorg voor de BAG-gerelateerde maatregelen uit de BIO in ENSIA;
- Rapporteert de uitkomsten van de zelfevaluatie van de BAG in ENSIA aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.5 Beveiligingsbeheerder SUWI

De beveiligingsbeheerder SUWI beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De beveiligingsbeheerder SUWI:

- Bevordert en adviseert over de beveiliging van Suwinet,en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet;
- Ziet er op toe dat de maatregelen worden nageleefd;
- Evalueert de uitkomsten van verbetermaatregelen;
- Verzorgt rapportages met betrekking tot de beveiligingsstatus van Suwinet aan het MT en/of college;
- Doet controles op het gebruik van Suwinet door de gemeente en vraagt daarvoor (specifieke) rapportages op bij het BKWI;
- Draagt zorg voor de ICT-gerelateerde maatregelen uit de BIO in ENSIA;
- Doet jaarlijks een zelfevaluatie op het geldende (specifieke) normenkader en stelt de Collegeverklaring op in het kader van ENSIA;
- Is aanspreekpunt tijdens de externe audit op de Collegeverklaring;
- Rapporteert de uitkomsten van de zelfevaluatie en externe audit op Suwinet aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.6 Beveiligingsbeheerder DigiD

De Beveiligingsbeheerder DigiD is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. Hieronder vallen:

- De preventie van beveiligingsincidenten en het geven van een adequate respons;
- Draagt zorg voor de DigiD-gerelateerde maatregelen uit de BIO in ENSIA;
- Doet jaarlijks een zelfevaluatie op het geldende (specifieke) normenkader en stelt de Collegeverklaring op in het kader van ENSIA;
- Rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.7 Beveiligingsbeheerder Facilitaire Zaken

De Beveiligingsbeheerder Facilitaire Zaken is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op facilitaire zaken en Huisvesting en Services en is verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).
De Beveiligingsbeheerder Facilitaire Zaken:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.8 Beveiligingsbeheerder ICT

De Beveiligingsbeheerder ICT is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op ICT. De Beveiligingsbeheerder ICT is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het Informatieveiligheidsplan. De Beveiligingsbeheerder ICT:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Draagt zorg voor de ICT-gerelateerde maatregelen uit de BIO en ENSIA;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.9 Beveiligingsbeheerder DIV

De Beveiligingsbeheerder DIV is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op DIV en is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie, het informatieveiligheidsplan en wet en regelgeving specifiek ten aanzien van DIV, waaronder de Archiefwet in relatie tot de wet Revitalisering Generiek Toezicht (RGT). De Beveiligingsbeheer DIV:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.9.1 Beveiligingsbeheerder P&O

De Beveiligingsbeheerder P&O is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op P&O en heeft een belangrijke adviesrol op het gebied van organisatie en informatieprocessen. De Beveiligingsbeheerder P&O is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. De Beveiligingsbeheer P&O:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.9.2 Functioneel applicatiebeheerder

De Functioneel applicatiebeheer is verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatie-voorziening.

2.9.9.3 Certificaatbeheerder

De certificaatbeheerder beheert de elektronische sleutels van PKI/Overheid conform de voorschriften. Public key infrastructure (PKI) is het systeem waarmee uitgiften en beheer van digitale certificaten wordt gerealiseerd. Aan het gebruik zijn voorschriften verbonden ten aanzien van installatie, beveiliging, update, geldigheid en toepassing. De certificaatbeheerder is hiervoor verantwoordelijk.

2.9.9.4 Gegevensbeheerder

De Gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

2.9.9.5 Gegevenseigenaar

De gegevenseigenaar (ook wel Informatie-eigenaar of Data-eigenaar) is verantwoordelijk voor de gegevens binnen een specifiek data domein. Een gegevenseigenaar moet ervoor zorgen dat de gegevens binnen zijn domein correct wordt beheerd over verschillende systemen en bedrijfsactiviteiten. Specifieke verantwoordelijkheden voor de gegevenseigenaar zijn:

- Goedkeuren van data definities;
- Zorgen voor de juistheid van informatie zoals gebruikt binnen en door de gehele organisatie;
- Datakwaliteit;
- Beoordelen en goedkeuren van de Master Data Management (MDM) aanpak, resultaten en activiteiten. MDM heeft als doel het stroomlijnen van data uitwisseling en het bieden van een enkele, consistente weergave van kritische data voor iedereen binnen de organisatie.
- Samenwerken met andere Data-eigenaren om data problemen en onbegrip tussen de verschillende bedrijfseenheden op te lossen;
- Input geven over softwareoplossingen, beleid of wettelijke vereisten die van invloed zijn op het data domein van de Data-eigenaar.

2.9.9.6 Proceseigenaar

De proceseigenaar is verantwoordelijk voor een proces. Deze verantwoordelijkheid kan meerdere aspecten betreffen:

- Het ontwerp en de invoering van het proces zelf. We onderscheiden een procesontwikkelings-verantwoordelijkheid (omvat zowel ontwerp als verbetering van het proces) en een procesimplementatie-verantwoordelijkheid (inclusief de verantwoordelijkheid voor interne audits waarmee aangetoond wordt dat het proces 'werkt');
- De resultaten van het proces. Deze procesbesturingsverantwoordelijkheid betreft de operationele beheersing en logistieke aspecten van resultaat (kwaliteit, tijd) en resourceverbruik (mensen, middelen). Het gaat daarbij om de eind- resultaten van het proces;
- Hiërarchische verantwoordelijkheid voor de medewerkers met de belangrijkste rollen in het proces.

2.9.9.7 Systeemeigenaar

De systeemeigenaar bepaalt wat er nodig is voor een optimale ondersteuning van de informatievoorziening van de bedrijfsprocessen. De systeemeigenaar (die ook proceseigenaar kan zijn) bepaalt de prioriteiten voor zowel de exploitatie als het doorvoeren van wijzigingen. Het budget betreft niet alleen de ICT-kosten, maar ook bijvoorbeeld wat beschikbaar is voor de ondersteuning door functioneel beheer. Systeemeigenaarschap is geen ICT-rol. Een systeemeigenaar mag voor wat betreft de technologie afstand nemen, maar is wel verantwoordelijk voor de informatievoorziening die nodig is voor de ondersteuning van bedrijfsprocessen.

2.9.9.8 Autorisatiebevoegde Reisdocumenten/Aanvraagstations

De Autorisatiebevoegde Reisdocumenten is verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).

2.9.9.9 Autorisatiebevoegde Rijbewijzen

De Autorisatiebevoegde Rijbewijzen is verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

2.9.9.10 Vertrouwde Contactpersoon Informatiebeveiliging (VCIB)

De VCIB krijgt waarschuwingen en informatie van de IBD met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten waarvan de inhoud een vertrouwelijk karakter heeft en die niet met anderen gedeeld mogen worden.

2.9.9.11 Algemene Contactpersoon Informatiebeveiliging (ACIB)

De ACIB krijgt algemene waarschuwingen en informatie van de IBD met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten.

3. Overleg en afstemmingsorganen

De CISO is voorzitter van het overleg informatiebeveiliging dat 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De (CISO);
- De Controller informatiebeveiliging;
- Agenda-leden: Beveiligingsbeheerders t.a.v: BRP,PNIK, BRO, BAG, SUWI, DigiD, GEO/BGT;
- Agenda-leden: Beveiligingsbeheerders t.a.v: FZ, ICT, DIV en P&O;
- Agenda-lid: Privacy beheerder;
- Agenda-leden: Managementteam (MT)lid of specialist, Regiefunctionaris ICT.

3.1 Onderwerpen

- Voortgang uitvoering maatregelen Beveiligingsplan c.q. Plan van Aanpak;
- Behandeling veiligheidsincidenten;
- Planning en voorbereiding van audits, inspecties en evaluaties;
- Evaluatie en actualisatie informatiebeveiliging en informatieveiligheidsplan;
- Actuele informatiebeveiligingsonderwerpen.

4. ICT crisisbeheersing

Voor interne crisisbeheersing is een kernteam informatiebeveiliging geïnstalleerd. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat o.a. uit:

- De coördinator informatieveiligheid (CISO);
- Functionaris Gegevensbescherming (FG);
- Regiofunctionaris;
- De beveiligingsbeheerder ICT;
- Betrokken MT lid (verantwoordelijk voor ICT/Informatievoorziening);
- Relevante experts;
- Een lid van het team Communicatie.

5. Rapporteren beveiligingsincidenten

De CISO wordt door de proceseigenaren geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd.
Er wordt minimaal eenmaal per jaar gerapporteerd aan het MT door de coördinator Informatieveiligheid (CISO).

6. Verantwoordelijkheden afdeling overstijgende (informatie)systemen

Afdeling overstijgende (informatie)systemen binnen de gemeente Tholen worden onder de verantwoordelijkheid van de systeemeigenaar (contracthouder) gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd eigenaar van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften (het gemeentelijk informatieveiligheidsbeleid) worden nageleefd en dat de verantwoordelijkheden voor (informatie)beveiliging voor alle betrokken partijen duidelijk omschreven zijn. De systeemeigenaar rapporteert over de mate van compliancy van overstijgende systemen en

schaft waar nodig nieuwe systemen aan, escaleert meldingen over systemen wanneer niet wordt voldaan aan afspraken (SLA),

De procesverantwoordelijke maakt schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:

- Voorwaarden voor het toegestane gebruik van het afdeling overstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatiebeveiliging;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van de afspraken en oplossing van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audit bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatieveiligheidsbeleid voldoet.

7. Contracten met derden

7.1 Service level agreement (niveau van dienstverlening)

Bij structurele / langdurige ondersteuning (externe inhuur) en/of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen de gemeente / een afdeling en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatiebeveiliging en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatiebeveiliging. In het ondersteunings- of uitbestedingscontract wordt verwezen naar de SLA.

7.2 Inhuur derden

Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van het verantwoordelijke afdelingshoofd. Deze manager dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

7.3 Toegang

- Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden de onderstaande uitgangspunten:
- Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen;
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald;
    - welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn;
    - welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn;
    - hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt;
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een Standaard Verwerkersovereenkomst conform artikel 14) afgesloten;
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd;
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld;

- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

7.4 Grote projecten

Voor grote ICT-projecten gelden specifieke, op centraal niveau vastgestelde, richtlijnen, met name ten aanzien van (Europese) aanbesteding, screening van bedrijven en juridische aspecten.

NB in een aparte bijlage staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie. De toewijzing van de rollen wordt door het MT vastgesteld.