Governance en Incidentenprocedure gemeente Oegstgeest

Volgens de Baseline Informatiebeveiliging Nederlandse Gemeenten

Addendum bij het Statuut informatiebeveiliging

GEMEENTE
OEGSTGEEST

Versie	: 1.00
Auteurs	: Informatieveiligheidsorganisatie gemeente Oegstgeest
Begeleiding	: Hesther van der Zwan, Meike Aartsen MA (BMC)
Datum	: februari 2016

Inhoud

Inleiding

In maart 2013 is het Statuut Informatiebeveiliging voor de gemeenten Oegstgeest, Leiden, Leiderdorp, Zoeterwoude en Servicepunt71 vastgesteld. Hierin worden uitgangspunten benoemd met betrekking tot de organisatie van informatieveiligheid en enkele beleidsuitgangspunten met betrekking tot informatieveiligheid.

Het normenkader NEN-ISO/IEC 27002 wordt als uitgangspunt gehanteerd. Ook wordt gesteld dat de organisatie en de beveiligingsmaatregelen behoren te voldoen aan de wettelijke eisen en audits vanuit het Rijk.

De doelstelling van het Statuut luidt als volgt:
"Het bieden van een gezamenlijk raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de (geautomatiseerde) informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt op basis van ***NEN-ISO/IEC 27002****, teneinde de (geautomatiseerde) informatievoorziening te beschermen tegen interne en externe bedreigingen."*

In mei 2013 is de Baseline informatiebeveiliging Nederlandse gemeenten (BIG) ontwikkeld door VNG en KING. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de veiligheid van informatie binnen gemeentelijke organisaties. Bij het buitengewone VNG ledencongres (29 november 2013) is door de leden een resolutie aangenomen die van de gemeenten vraagt informatieveiligheid bestuurlijk en organisatorisch te borgen, de Baseline Informatiebeveiliging voor Nederlandse Gemeenten als standaard te hanteren en informatieveiligheid transparant te maken voor burgers, bedrijven en ketenpartners.

De gemeente Oegstgeest hanteert deze nieuwe gemeente standaard (BIG) als uitgangspunt bij de inrichting van de gemeentebrede informatieveiligheid. De ambitie is om in het eerste kwartaal van 2016 één gezamenlijk gemeentebreed informatieveiligheidsbeleid vast te stellen voor de gemeenten Oegstgeest, Leiden, Oegstgeest, Zoeterwoude en Servicepunt71, op basis van deze Baseline.
Om echter binnen een kort tijdsbestek al met de implementatie van de Baseline te kunnen starten, kiest Oegstgeest ervoor tussentijds dit Governance addendum toe te voegen aan het huidige Statuut. In dit addendum wordt op basis van de BIG en het reeds vastgestelde statuut de beveiligingsorganisatie en governance (besturing) van de informatieveiligheid vastgesteld. Dit betekent dat de rollen worden ingevuld, de interne informatieveiligheidsoverleggen binnen de gemeente Oegstgeest worden beschreven en de uitgangspunten ten aanzien van de incidentenprocedure worden beschreven.

De specifieke invulling voor de gemeente Oegstgeest heeft plaatsgevonden door middel van workshops met een brede afvaardiging uit de organisatie.

In het programmaplan “Versterken regionale i-Samenwerking Leiden, Leiderdorp, Zoeterwoude en Servicepunt71” dat ten tijde van het schrijven van dit addendum in ontwikkeling is, is de regionale governance ten behoeve van informatievoorziening opgenomen als uit te werken onderwerp. Hierin worden ook de rollen/functies/taken/verantwoordelijkheden op gebied van informatieveiligheid en gegevensbescherming meegenomen. Dit addendum zal, indien noodzakelijk, hierop worden aangepast.

1. Opzet en borging van het addendum

1.1 Addendum voor Governance en incidentenprocedure

Het College van B&W moet het addendum met betrekking tot de Governance en de incidentenprocedure, behorende bij het Statuut Informatiebeveiliging, goedkeuren, uitgeven en kenbaar te maken aan alle medewerkers, alsmede hiernaar handelen.
Minimaal zijn de volgende aspecten in dit beleidsdocument aanwezig:

- De organisatie van de informatieveiligheidsfunctie;
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende afdelingen en rollen;
- Een omschrijving van de incidentenprocedure;
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde Statuut met Governance addendum kunnen worden getoetst.

1.2 Informatieveiligheidsplan

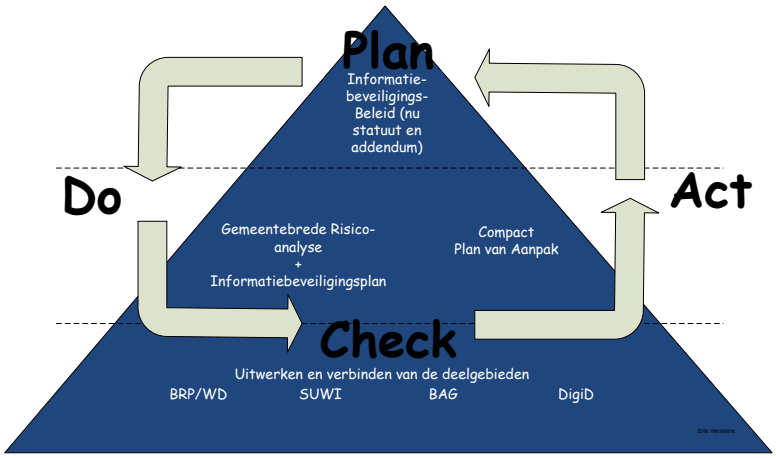
Na vaststelling van dit addendum behorende bij het Statuut Informatiebeveiliging, wordt een Risico analyse uitgevoerd. Hierbij wordt onderzocht of de beleidsuitgangspunten uit het Statuut en het addendum daadwerkelijk in de praktijk worden uitgevoerd en geïmplementeerd zijn. Deze risico analyse wordt uitgevoerd aan de hand van vijf aandachtsgebieden, te weten omgeving, gebouw en installaties, ICT, procedures en mensen. Hier vloeit een informatieveiligheidsplan uit voort met een concreet plan van aanpak. Hierin wordt aangegeven op welke wijze het beleid uitgevoerd zal worden.
De kernelementen in het informatieveiligheidsplan zijn:

- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van het gemeentebrede informatieveiligheidsplan wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau;
- Voor het bepalen van afhankelijkheden en risico's is een analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:
    - Risico's die onvoldoende af te dekken zijn door maatregelen;
    - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen;
    - Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden;
    - Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfskritisch zijn. Dit overzicht kan als bijlage aan het uitvoeringsplan worden toegevoegd.

1.3 Borging van het Statuut Informatiebeveiliging en het addendum

Om borging van het Statuut Informatiebeveiliging met addendum en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen, onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA cyclus:

1. Statuut Informatiebeveiliging met addendum (op termijn word dit een gezamenlijk informatieveiligheidsbeleid). Bevat de richtlijnen en de visie op informatieveiligheid. Bijstelling van deze documenten vindt plaats om de 4 jaar;
2. Informatieveiligheidsplan. Bevat de risicoanalyse (de toets aan de praktijk) op basis van het Statuut/informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van het Informatieveiligheidsplan vindt plaats na 1 jaar;
3. Plan van Aanpak. Bevat de concrete acties volgend uit de risicoanalyse. De prioritering van de verbeteracties die betrekking hebben op het Servicepunt71 (bijvoorbeeld ten aanzien van ICT en P&O) zullen worden afgestemd met de samenwerkende gemeenten. Bijstelling (hieronder valt ook de voortgang op de realisatie van de afgesproken acties en maatregelen) van het Plan van aanpak vindt 2 maal per jaar plaats.



Figuur 1: De informatieveiligheidspiramide met PDCA cirkel

2. Organisatie van de informatieveiligheid

Doelstelling:
Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.

Resultaat:
Verankering in de gemeentelijke organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid.

2.1 Organisatie volgens het Statuut Informatiebeveiliging (maart 2013)

De gemeente Oegstgeest stelt in het Statuut Informatiebeveiliging voor de gemeenten Leiden, Leiderdorp, Oegstgeest, Zoeterwoude en Servicepunt71 (maart 2013) de organisatie van informatieveiligheid als volgt vast:

Organisatie van de informatieveiligheid wordt als volgt cyclisch ingericht.
"Partij" betekent een van de vier gemeentes of het Servicepunt71.
*1. De **directie** van elke partij is eindverantwoordelijk voor beleidsontwikkeling van en de control op het informatieveiligheidsbeleid en bewaakt de realisatie van het uitvoeringsplan;*
*2. Het **college** (of het bestuur van SP71) stelt het beleid vast;*
*3. Elke partij benoemt een **coördinator informatieveiligheid**; deze stelt jaarlijks, op grond van een risicoanalyse, een uitvoeringsplan op en legt dat ter goedkeuring voor aan de directie;*
*4. De **Leidinggevenden** zijn vervolgens verantwoordelijk voor de te nemen maatregelen, daarbij ondersteund door de coördinator informatieveiligheid;*
*5. Analyse van incidenten, resultaten van audits, of andere in- of externe signalen kunnen leiden tot voorstellen voor aanpassing van beleid, aanpassing van het uitvoeringsplan, prioriteiten daarbinnen of andere maatregelen. De **coördinator informatieveiligheid** ontwikkelt voorstellen daartoe;*
*6. De **Leidinggevenden** blijven te allen tijde verantwoordelijk voor de beveiliging van hun eigen informatiesystemen. Bemoeienis en ondersteuning van de coördinator informatieveiligheid neemt die verantwoordelijkheid niet weg;*
*7. De **coördinatoren informatieveiligheid** vormen gezamenlijk een **vaktafel informatieveiligheid**. De vaktafel evalueert beleid en coördineert gezamenlijke beveiligingsissues.*
*8. De **vaktafel informatieveiligheid** toetst het gekozen beveiligingsniveau, controleert op de uitvoering en naleving van het informatieveiligheidsbeleid van Servicepunt71.*

Om de richtlijnen van de Baseline Informatiebeveiliging Nederlandse gemeenten te volgen, heeft de gemeente Oegstgeest onderstaande verantwoordelijkheidsniveaus nader geconcretiseerd en toegewezen binnen de organisatie. Onderstaande verantwoordelijkheidsniveaus dienen dus ter aanvulling op het Statuut Informatiebeveiliging.

Nb, de in het statuut genoemde coördinator informatieveiligheid wordt ook wel CISO (Chief Information Security Officer) genoemd.

2.2 Verantwoordelijkheidsniveaus van de informatieveiligheidsorganisatie binnen de gemeente Oegstgeest volgens de Baseline

Binnen de gemeente Oegstgeest worden de volgende verantwoordelijkheid- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:

2.2.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

Het College van B&W van de gemeente Oegstgeest draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Het college stelt de kaders ten aanzien van informatieveiligheid 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 nemen van beveiligingsmaatregelen op organisatieonderdelen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging opgedragen aan de algemeen directeur/gemeentesecretaris.

2.2.2 Verantwoordelijkheden en taken op organisatieniveau

De (door het College van B&W opgedragen) verantwoordelijkheid voor informatieveiligheid ligt bij de algemeen directeur/gemeentesecretaris. Deze stelt met het management het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De algemeen directeur/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.

2.2.3 Verantwoordelijkheden en taken op teamniveau

De teammanagers zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun team.

2.2.4 De coördinator informatieveiligheid

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.

2.2.5 De 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 rol van controller informatieveiligheid heeft op twee specifieke deelgebieden een voorgeschreven officiële benaming. Dit betreft het gebied van reisdocumenten en van rijbewijzen. Het gaat hierbij om de volgende benamingen; Beveiligingsfunctionaris reisdocumenten (belast met het beheer van en het toezicht op de naleving van de beveiligingsprocedure) en Beveiligingsfunctionaris rijbewijzen (belast met het beheer van en het toezicht op de naleving van de beveiligingsprocedure).

2.2.6 Servicepunt71 Service-eenheid ICT

De Service-eenheid ICT , waarvan systeembeheer deel uit maakt, beheert de werkplekken, serverplatformen, lokale netwerken, verbindingen, externe netwerkverbindingen (zoals Gemnet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast is Servicepunt71 verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen en laat zij ICT

audits uitvoeren. Verantwoording over het gevoerde beheer van de getroffen beveiligings-maatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

2.2.7 Facilitaire Zaken

Facilitaire Zaken is verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).

2.2.8 Servicepunt71 Service-eenheid HRM

De Service-eenheid HRM is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke advies rol op het gebied van organisatie en informatieprocessen.

2.2.9 De beveiligingsbeheerder

Deze rol is 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. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumenten (officieel Beveiligingsfunctionaris Reisdocumenten, Rijbewijzen (officieel Beveiligingsfunctionaris Rijbewijzen), BAG, SUWI (officieel Security officer SUWI) en DigiD.

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;
- evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Basisregistratie Personen (College B&W).

Beveiligingsfunctionaris reisdocumenten, is belast met;

- het beheer van en het toezicht op de naleving van de beveiligingsprocedure.

Beveiligingsfunctionaris rijbewijzen, is belast met;

- het beheer van en het toezicht op de naleving van de beveiligingsprocedure.

Beveiligingsbeheerder BAG

Er is geen aparte beveiligingsbeheerder BAG aangesteld, het element “beveiliging” is opgenomen bij de beheerder Basisregistratie Adressen en Gebouwen.

Security officer SUWI, is belast met;

- het beheer van beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd;
- het bevorderen van en adviseren over de beveiliging van Suwinet;
- het houden van toezicht op het naleven van de maatregelen zoals beschreven in het Informatiebeveiligingsplan SUWI;

- het gevraagd en ongevraagd adviseren van medewerkers en management en het doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet;
- het beheren van het informatiebeveiligingsplan SUWI.

Beveiligingsbeheerder DigiD, is belast met;

- het beheer van beveiligingsprocedures en -maatregelen in het kader van DigiD, zodanig dat de beveiliging van DigiD overeenkomstig wettelijke eisen is geïmplementeerd;
- het bevorderen van en adviseren over de beveiliging van DigiD;
- het houden van toezicht op het naleven van de maatregelen geldend voor DigiD (o.a. normenkader DigiD audit);
- het gevraagd en ongevraagd adviseren van medewerkers en management en het doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van DigiD;
- het aanspreekpunt zijn voor de betrokken leverancier(s);
- het laten uitvoeren van de jaarlijkse DigiD audit;
- het opvolgen/implementeren van aanbevelingen vanuit de DigiD audit.

2.2.10 Privacy beheerder(s)

Deze rol is gericht op de uitvoering en de naleving van de Wet Bescherming van Persoonsgegevens (WBP). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.
Er is in Oegstgeest een aparte privacy beheerder BRP benoemd. Taken, verantwoordelijkheden en bevoegdheden van deze functionaris zijn vastgelegd in de beheerregeling BRP.

2.2.11 Functionaris gegevensbescherming

Momenteel mogen organisaties zelf bepalen of ze een Functionaris voor de Gegevensbescherming benoemen: benoeming van een FG is nu niet verplicht. Dit wordt zeer waarschijnlijk anders zodra de Europese Privacy Verordening in werking treedt, naar verwachting per 2018. Deze rol wordt functionaris voor de gegevensbescherming (FG) of Data Protection Officer (DPO) genoemd. De functionaris gegevensbescherming is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. Deze toezichthouder wordt officieel functionaris voor de gegevensbescherming (FG) genoemd. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

2.2.12 Functioneel (applicatie)beheerder

Verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatie-systemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening (inclusief de informatieveiligheidsmaatregelen).

2.2.13 De medewerkers

Alle medewerkers dragen verantwoordelijkheid voor de veiligheid 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.

2.2.14 Gegevensbeheerder(s)

Verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening (inclusief de informatieveiligheidsmaatregelen).

Er is een beheerregeling BRP waarin de verantwoordelijkheden van de gegevensbeheerder BRP zijn gespecificeerd.

2.3 Toewijzing verantwoordelijkheden voor informatieveiligheid.

De *algemeen directeur/gemeentesecretaris* en *het management* 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. Het betreft hier risico's die impact hebben op de informatieveiligheid en niet binnen één specifieke afdeling zijn te adresseren maar de gehele organisatie aangaan;
- 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 informatieveiligheidscomponenten en systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid;
- Het aanwijzen van een coördinator informatieveiligheid en een controller informatieveiligheid.

De teammanagers hebben in ieder geval de volgende verantwoordelijkheden*:*

- Het uit (laten) voeren van maatregelen uit het informatieveiligheidsplan die op het team van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de informatiesystemen binnen het team;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de coördinator informatieveiligheid*,* over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages.

De *coördinator informatieveiligheid* heeft in ieder geval de volgende verantwoordelijkheden:

- Coördineert het formuleren van informatiebeveiligingsbeleid (nu Statuut Informatiebeveiliging met Addendum) ;
- Stelt het informatiebeveiligingsplan op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering van informatiebeveiligingsmaatregelen uit het informatiebeveiligingsplan;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatiebeveiliging;
- Ondersteunt de directie en de leidinggevenden met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatiebeveiliging;
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de Informatiebeveiligingsplannen;
- Bevorderen van het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;

- Toetst of informatiebeveiliging een onderdeel uitmaakt van het informatieplannings-, systeemontwikkelings- en onderhoudsproces;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C cyclus. Hierbij bundelt de coördinator de deelbijdragen van de teammanagers.

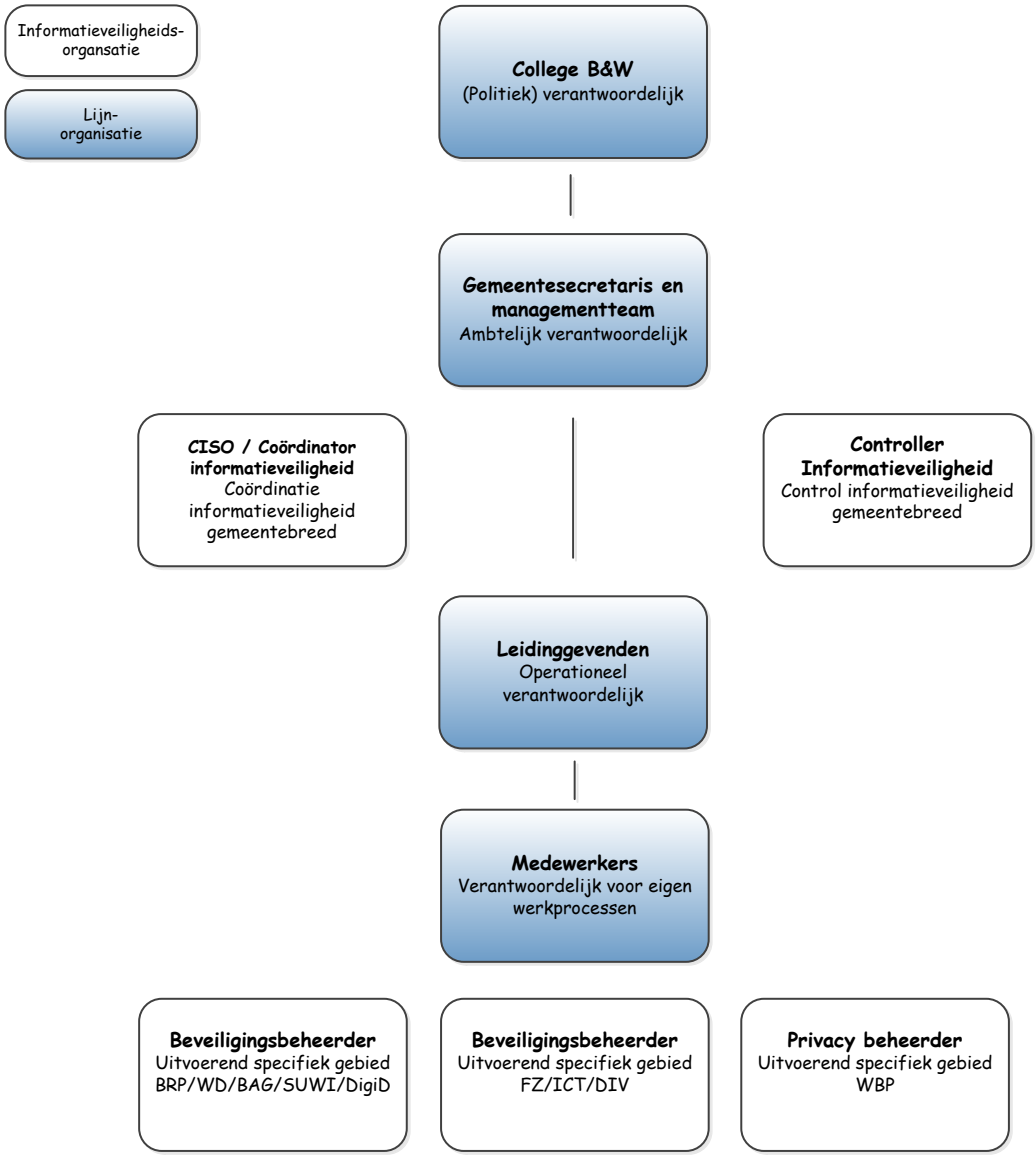
De *controller informatieveiligheid* heeft in ieder geval de volgende verantwoordelijkheden:
- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- De controle op de voortgang van het uitvoeren van de maatregelen uit het informatiebeveiligingsplan;
- De controle op de periodieke actualisatie van informatiebeveiligingsbeleid (nu Statuut informatiebeveiliging met Addendum) en op het Informatie-beveiligingsplan;
- Toetsen/bewaken van het niveau van informatiebeveiliging;
- Evalueren van beveiligingsincidenten.

De beveiligingsbeheerder is -voor het toegewezen deelgebied- verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het Statuut Informatiebeveiliging en het onderliggende 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 de coördinator informatieveiligheid en de controller informatieveiligheid.
NB, op grond van de bepalingen uit de PUN (Paspoortuitvoeringsregeling) en het Reglement rijbewijzen heeft de beveiligingsfunctionaris de bevoegdheid rechtstreeks aan de burgemeester te rapporteren en niet via de ambtelijke lijn.

De *privacy beheerder* heeft in ieder geval de volgende verantwoordelijkheden:
- Toezicht op de naleving van de Wet Bescherming Persoonsgegevens (WBP)
- Organisatiebreed adviseren (gevraagd en ongevraagd) over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.
- Aanwijzingen geven aan gebruikers van systemen met betrekking tot persoonsregistraties.
- Ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de registratie van personen.
- Contactpersoon voor de (nog aan te stellen) regionale Functionaris Gegevensbescherming
- Contactpersoon van de gemeente voor het College Bescherming Persoonsgegevens (CBP) en tevens verantwoordelijk voor het melden van ernstige/majeure incidenten richting het CBP.

NB, voor het naleven van de Wet Basisregistratie Personen (BRP) is een privacy beheerder BRP benoemd.

In bijlage 1 staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie.



Figuur 2: Rollen en verantwoordelijkheden in de informatieveiligheidsorganisatie (Nb, de Functionaris Gegevensbescherming ontbreekt in dit overzicht omdat deze regionaal zal worden aangesteld)

2.4 Overleg en afstemmingsorganen

De coördinator informatieveiligheid is voorzitter van het O*verleg informatieveiligheid* dat 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De coördinator informatieveiligheid
- De controller Informatieveiligheid;
- Beveiligingsbeheerders t.a.v: BRP, Reisdocumenten, Rijbewijzen, SUWI, BAG en DigiD;
- Beveiligingsbeheerders t.a.v: FZ, ICT en DIV
- Privacy beheerder(s);
- Agendaleden: directie lid of specialist.

Onderwerpen:

- 2 maal per jaar: voortgang uitvoering maatregelen Beveiligingsplan c.q. Plan van Aanpak;
- Veiligheidsincidenten;

- Planning en voorbereiding van Audits en controles;
- Evaluatie en actualisatie informatieveiligheid en informatieveiligheidsplan.

Daarnaast vindt afstemming plaats tussen de coördinator informatieveiligheid en de functioneel applicatie- en gegevensbeheerder(s) en de procesverantwoordelijke(n) van (informatie)systemen.

De coördinatoren van de gemeenten Oegstgeest, Leiden, Leiderdorp, Zoeterwoude en van Servicepunt71 vormen gezamenlijk een *Vaktafel informatieveiligheid*. De vaktafel evalueert beleid, coördineert gezamenlijke beveiligingsissues, toetst het gekozen beveiligingsniveau en controleert op de uitvoering en naleving van het informatieveiligheidsbeleid van Servicepunt71.

2.5 ICT crisisbeheersing

Voor ICT crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. We spreken van een incident op het moment dat de Beschikbaarheid, Integriteit en/of Vertrouwelijkheid van informatie of een informatiesysteem is aangetast. De coördinator informatieveiligheid bepaald echter per geval of het incident dermate groot en complex dat opschaling richting het Kernteam Informatiebeveiliging nodig is.

Dit team bestaat uit de coördinator informatieveiligheid (tevens coördinator Informatiebeleid), de beveiligingsbeheerder ICT, een lid van de directie, relevante interne of externe experts, een lid van het team communicatie en optioneel de privacy beheerder.

Daarnaast informeert de coördinator informatieveiligheid de controller informatieveiligheid, en verzorgt de coördinator informatieveiligheid de communicatie en afstemming met het bestuur van de gemeente.

Let op: het kernteam informatieveiligheid heeft een ander werkgebied dan de rampenstaf. De taken en verantwoordelijkheden van de rampenstaf betreffen namelijk crises, rampen en interventies die zich veelal buiten de gemeentelijke organisatie bevinden. Dit terwijl het kernteam informatieveiligheid zich richt op de interne organisatie.

2.6 Rapporteren beveiligingsincidenten

De coördinator informatieveiligheid wordt door de procesverantwoordelijken 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.

2.6.1 Definitie incident

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de **beschikbaarheid**, de **integriteit** of de **vertrouwelijkheid** van informatie of informatiesystemen in gevaar is of kan komen.

Hierbij staat *beschikbaarheid* voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. *Integriteit* staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). *Vertrouwelijkheid* heeft betrekking op exclusiviteit van informatie en de privacybescherming.

Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).

Voorbeelden van beveiligingsincidenten zijn: besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), niet beschikbaar zijn van de website met dienstverleningsportaal, verlies van usb-stick met gevoelige informatie, diefstal van data of hardware of een gecompromitteerde mailbox.

Afspraken moeten worden gemaakt over:
- doel van de registratie;
- inhoud van de registratie;
- mate van detaillering;
- wijze van handelen;
- wijze van rapporteren.

Er wordt minimaal eenmaal per jaar gerapporteerd aan het management door de coördinator Informatieveiligheid.

2.6.2 Procedure en omgang beveiligingsincidenten

Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Hiervoor gelden de volgende uitgangspunten:
- De coördinator informatieveiligheid is de beheerder van de registratie van beveiligingsincidenten;
- Een medewerker meldt geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct bij de coördinator informatieveiligheid van de gemeente;
- Beveiligingsincidenten die worden gemeld bij de ICT helpdesk, worden als zodanig geregistreerd en eveneens doorgegeven aan de coördinator informatieveiligheid;
- Vermissing of diefstal van apparatuur of media die gegevens van de gemeente kunnen bevatten wordt altijd ook aangemerkt als informatieveiligheidsincident;
- Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De coördinator informatieveiligheid bekijkt periodiek een samenvatting van de informatie;
- Er wordt een procedure voor communicatie naar de Informatieveiligheidsdienst (IBD) opgesteld;
- De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

Voor het melden van een datalek is een aparte procedure (en proces) beschikbaar. Dit is een vereiste vanuit de Meldplicht Datalekken, dit is een wijziging in de Wet Bescherming Persoonsgegevens (WBP) die vanaf 1 januari 2016 in werking is getreden. Van een datalek is volgens artikel 34a sprake als de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Hier kan het ook gaan over een hack, diefstal van een laptop, etc. Ook indien er wel sprake is van een voldoende beveiligingsniveau kan er dus wel degelijk sprake zijn van een datalek. In het proces “Meldplicht Datalekken” wordt de afweging gemaakt om een datalek al dan niet te melden aan het College Bescherming Persoonsgegevens en/of betrokkene(n).

2.7 Verantwoordelijkheden afdeling overstijgende (informatie)systemen

Het systeembeheer en het technisch applicatiebeheer worden door Servicepunt71 en/of leveranciers gefaciliteerd en onderhouden. De team overstijgende systemen (applicaties), die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder team overstijgend (informatie)systeem heeft het managementteam het primaat dit te mandateren aan een gegevensbeheerder binnen een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd gegevensbeheerder van een team overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk afgestemd en omschreven zijn.

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

Minimaal worden in deze afspraken vastgelegd:
- Voorwaarden voor het toegestane gebruik van het team overstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het team 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 informatieveiligheid;
- 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.

2.8 Contracten met derden

2.8.1 Service level agreement (niveau van dienstverlening)
Bij structurele / langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen een team en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatieveiligheid en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatieveiligheid. In het uitbestedingscontract wordt verwezen naar de SLA.

2.8.2 Inhuur derden
Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijk leidinggevende. Deze leidinggevende dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

2.8.3 Toegang
Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden in principe de onderstaande uitgangspunten:

- Informatieveiligheid is (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.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform artikel 14 WBP) 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.

Bijlage 1: rollen en namen

Rollen en namen binnen de gemeentebrede informatieveiligheidsorganisatie volgens de Baseline Informatiebeveiliging Nederlandse Gemeenten

Rol	**Naam**	**Indien van toepassing: vervanger**
Coördinator informatieveiligheid	Marjon Miggels	
Controller informatieveiligheid	Jan de Ruijter	
Beveiligingsbeheerder BRP	Lida ten Veen	
Beveiligingsfunctionaris Reisdocumenten	Lida ten Veen	
Beveiligingsfunctionaris Rijbewijzen	Lida ten Veen	
Beveiligingsbeheerder BAG	Sanne Griffioen	
Beveiligingsbeheerder DigiD	Niet belegd	
Beveiligingsbeheerder SUWI (Security Officer SUWI)	Marjon Miggels	
Beveiligingsbeheerder Facilitaire Zaken	Ger van Emmerik	
Beveiligingsbeheerder ICT	Maurice Derogee	
Beveiligingsbeheerder DIV	Ger van Emmerik	
Privacy beheerder (Wet Bescherming Persoonsgegevens)	Anne Goud	
Privacy beheerder BRP	Miriam Wolvers	

NB: Wanneer gemeenten in de toekomst (afhankelijk van de Europese wetgeving) mogelijk een Functionaris Gegevensbescherming (FG) dienen vast te stellen, zal deze in regioverband worden aangesteld.