equalit

Informatiebeveiliging bij de gemeente Zundert

Dienstbeschrijving

Documentinformatie

Documentdetails

Documenttype	Template	**Deelnemer**	Zundert
Reviewcycle	Jaarlijks	**Aanpreekpunt Deelnemer**	Inge van Eekelen (DLR)/ Anjo Bogers (TOD)/ Marco Schuurmans

Documenthistorie[1]

Versie	Versiedatum	Status	Auteur
0.9	28-09-2018	Concept	Karin van Zanten
1.0	9-10-2018	Defintief	Karin van Zanten

Laatste goedkeuring[2]

Naam	Datum	Paraaf

[1] De laatste definitieve versie maakt alle voorgaande versies ongeldig.
[2] Elke definitieve versie moet worden goedgekeurd door de proceseigenaar. Ook de reviewcycle moet als zodanig worden afgetekend door proceseigenaar ook indien er geen wijziging van het document nodig is.

Inhoud

1 Inleiding

Bij de deelnemers van Equalit is behoefte om informatiebeveiliging op lange termijn goed in te richten. Equalit wil hier graag in meedenken en de inrichting vanuit de share faciliteren. In deze dienstbeschrijving wordt een toelichting te geven op wat informatiebeveiliging inhoudt, wat het resultaat van de dienstverlening is, wat de resultaten zullen zijn, welke rollen en verantwoordelijkheden bij de CISO liggen en wat bij de deelnemer zelf ligt. Tevens worden randvoorwaarden en specifieke afspraken tussen de deelnemer en de CISO weergegeven in het laatste hoofdstuk.

Onderstaande dienstbeschrijving is gebaseerd op de memo 'verdiepen faciliteren security' welke op 29 maart 2018 door de Deelnemersraad op hoofdlijnen is goedgekeurd. Met de individuele deelnemers is tijdens de telefoongesprekken afgesproken dat er bij start van de CISO bij de gemeente een finesse aangebracht kan worden op ondergenoemde afspraken op hoofdlijnen. Deze dienstbeschrijving is bedoeld om de afspraken tussen gemeente Zundert en Equalit over de levering van de dienst 'informatiebeveiliging' vast te leggen.

2 Wat houdt informatiebeveiliging binnen een gemeente in?

2.1 Algemeen

Informatiebeveiliging is het geheel van maatregelen, procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van de informatievoorziening binnen een organisatie garandeert. Deze definitie is heel breed. Concreet zou je kunnen denken aan het treffen van maatregelen om bijvoorbeeld hacks of DDoS aanvallen te voorkomen of medewerkers te trainen hoe ze kunnen voorkomen dat informatie in handen valt van mensen voor wie deze informatie niet bedoeld is.

Het college van Burgemeester en Wethouders (college van B&W) is integraal verantwoordelijk voor de beveiliging van informatie en privacy binnen de gemeente. Zij stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. De VNG (vereniging Nederlandse Gemeenten) heeft een normenkader opgesteld wat door iedere gemeente gebruikt dient te worden om aan alle (landelijke) eisen ten behoeve van informatiebeveiliging te voldoen. Dit normenkader heet de BIG;

2.2 De BIG

De BIG staat voor Baseline Informatiebeveiliging Gemeenten en voldoet aan de internationale beveiligingsstandaarden ISO 27001/27002. De BIG is een set van beveiligingsmaatregelen (normenkader) die een basis-beveiligingsniveau voor gemeenten neerlegt. De gemeente dient periodiek te rapporteren over de getroffen beveiligingsmaatregelen aan het college van B&W. Dit wordt ook wel de *horizontale* verantwoording genoemd.

Naast de verantwoording aan het college van B&W dient de gemeente of gemeentelijke instelling ook te rapporteren over een aantal getroffen beveiligingsmaatregelen aan diverse ministeries. Dit wordt de *verticale* verantwoording genoemd. Deze verantwoording vindt plaats middels ENSIA;

2.3 ENSIA

ENSIA staat voor Eenduidige Normatiek Single Information Audit. ENSIA is een zelfevaluatielijst die gebaseerd is op de BIG. Daarnaast staan er in deze evaluatielijst een aantal normen voor specifieke onderdelen van de organisatie. Dit zijn normen op het gebied van de Basisregistratie Personen (BRP), DigiD, Paspoort- en Nederlandse Identiteitskaarten (PNIK), Suwinet, Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Adressen en Gebouwen (BAG). Gemeenten leggen *verticaal* door middel van ENSIA verantwoording af aan een ministerie en integraal over informatiebeveiliging m.b.v. de BIG aan het college van B&W.

Een veelgebruikt managementsysteem om aan te tonen dat binnen een organisatie voldoende aandacht wordt besteed aan informatiebeveiliging is het ISMS.

2.4 ISMS

Het ISMS staat voor Information Security Management System. Door het inrichten van een ISMS en het uitvoeren van verplichte activiteiten kan aantoonbaar gemaakt worden dat voldoende aandacht wordt besteed aan informatiebeveiliging. Een goede inrichting van het ISMS helpt bij het afleggen van zowel de verticale als horizontale verantwoording. Binnen het Equalit samenwerkingsverband maken we momenteel gebruik van de ISMS tool van leverancier SEP.

3 Resultaat van de dienstverlening

3.1 Concreet resultaat

De CISO is dé spin in het web als het gaat om de beveiliging van informatie binnen de gemeente. Hij is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen de gemeente. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan de BIG; een set van organisatorische en technische beveiligingsmaatregelen die geïmplementeerd en beheerd dienen te worden.

3.2 Beschikbaarheid van de CISO

Tussen de deelnemer en Equalit is afgesproken dat de deze recht heeft op ondersteuning op informatiebeveiligingsgebied. De CISO is zo veel mogelijk fysiek aanwezig op locatie voor wat betreft de afgesproken fte's. Tevens is afgesproken dat de kosten voor deze CISO voor rekening van de deelnemer komen.

Vanuit de share is het wenselijk dat de CISO's elkaar regelmatig zien en spreken om zo optimaal te kunnen profiteren van het samenwerkingsverband. De CISO's werken 1 vaste dag per week (0.2fte) samen op de locatie bij Equalit (donderdag), zodat ook werkzaamheden voor het shareverband uitgevoerd kunnen worden. Deze tijdsbesteding komt voor rekening van Equalit. Een overzicht van de werkzaamheden voor het shareverband zijn terug te vinden in hoofdstuk 4.2 Rollen en taakverdeling.

3.3 Periodieke evaluatie

De periodieke evaluatie vindt tijdens het eerste jaar van de CISO 1x per kwartaal plaats. Daarna vindt de evaluatie 2x per jaar plaats. De evaluatie wordt gedaan door of namens de coördinator van de CISO samen met het DLR lid van de betreffende gemeente (of diens vervanger) en de CISO zelf. Het doel van de periodieke evaluatie is om vast te stellen dat of er voldaan wordt aan wederzijdse verwachtingen en of er eventueel bijsturing plaats dient te vinden op eerder gemaakte afspraken.

3.4 Ondersteuning en klachten

Indien de deelnemer niet tevreden is over de dienstverlening van de betreffende CISO, dan kan dit aangekaart worden bij de coördinator van de CISO's.

4 Taakverdeling

4.1 Plaatsing binnen de organisatie

De CISO acteert vooral op strategisch en tactisch niveau. De CISO denkt mee over de visie op langere termijn op het gebied van informatiebeveiliging. De CISO acteert op het hoogste managementniveau en spreekt dan ook de taal van directie/bestuurders . De CISO levert input aan de controller, zodat deze onafhankelijk kan toetsten of de organisatie voldoet aan de gestelde eisen.

4.2 Overzicht van Rollen en taken

Taken CISO	Wat wordt opgeleverd door de CISO	Taken voor de deelnemers zelf
Beleid en coördinatie		
De CISO faciliteert bij het opstellen en actualiseren van het beleid. Door hergebruik van het beleid uit de share en vertaling naar couleur locale kan maximaal geprofiteerd worden van het samenwerkingsverband.	Informatiebeveiligingsbeleid voor de individuele deelnemer.	De CISO heeft input nodig van de deelnemer om tot een informatiebeveiligingsbeleid te komen wat aansluit op de wensen en behoeften van de individuele deelnemer. De managers, coördinatoren of afdelingsleiders van de organisatie dienen zelf het informatiebeveiligingsbeleid binnen de afdeling, unit of cluster waarvoor ze verantwoordelijk zijn uit te dragen.
De CISO faciliteert bij het opstellen en actualiseren van het beveiligingsplan (vanuit ISMS en ENSIA) voor de individuele deelnemer.	Beveiligingsplan voor de individuele deelnemer.	Het beveiligingsplan voor de gehele organisatie wordt door vertaald naar informatiebeveiligingsplannen voor afdelingen en deelgebieden. Hier wordt een actieve rol van het management verwacht. De SO (beveiligingsbeheerder) kan het management faciliteren bij het maken van een doorvertaling naar de afdeling.
Controle en registratie		
Het opstellen van een controleplan voor informatiebeveiliging voor de deelnemer.	Controleplan voor de individuele deelnemer.	Dit controleplan wordt in afstemming opgesteld met verantwoordelijk (concern) control en management.
De coördinatie op het uitvoeren van het controleplan (zelfevaluaties (ENSIA) en audits (BIG)).	-Zelfevaluaties (ingevulde vragenlijst) op het gebied van ENSIA aan verantwoordelijk ministerie -Input aan (concern) controller ten behoeve van de audit op de BIG	De SO (beveiligingsbeheerder) ondersteund de CISO en de controller bij het ophalen van input uit de organisatie waaruit blijkt dat aan de gestelde eisen op het gebied van informatiebeveiliging wordt voldaan. De controller van de deelnemer toetst onafhankelijk of de organisatie voldoet aan alle gestelde eisen met betrekking tot informatiebeveiliging.
De CISO initieert risico- analyses bij de individuele deelnemers. Veel risico's zijn voor alle deelnemers binnen het shareverband hetzelfde. Vanuit deze overkoepelende risico's kan een vertaling worden gemaakt naar de individuele deelnemers.	Risico analyse voor de individuele deelnemer	Van de deelnemer wordt verwacht dat deze input levert voor de risico analyses.
Het initiëren en coördineren van informatie over de aanwezige beveiligingsmaatregelen in de ISMS tool.	Gevuld ISMS	Het verantwoordelijk management vult de ISMS tool samen met de CISO. De CISO heeft hier een regierol, het is de verantwoordelijkheid van de deelnemer zelf dat de

		informatie die aangeleverd wordt voor het vullen van het ISMS juist en volledig is.
De coördinatie op het oppakken en afhandelen van opgetreden incidenten. Het initiëren van een registratie voor interne beveiligingsincidenten, evenals en het adviseren over te nemen preventieve maatregelen ter voorkoming van dergelijke incidenten.	-Input voor het register van beveiligingsincidenten -Advies over te nemen preventieve maatregelen	Het opstellen van een register van beveiligingsincidenten en dit register up to date houden is een taak van de deelnemer zelf. Een SO (beveiligingsbeheerder) zou hierbij kunnen ondersteunen. De implementatie van getroffen maatregelen ter voorkoming van incidenten dient door de deelnemer zelf geïnitieerd te worden.
Communicatie en voorlichting		
Het onderhouden van interne contacten op alle niveaus binnen het kader met betrekking tot informatiebeveiliging.		De controller van de deelnemer onderhoudt het contact met de externe accountant en is dan ook het eerste aanspreekpunt voor de accountant. De CISO kan de controller ondersteunen bij vragen over informatiebeveiliging binnen de deelnemer.
De CISO coördineert een overleg met betrekking tot informatiebeveiliging (beveiligingscommissie).	Verslag van het coördinerend overleg met betrekking tot informatiebeveiliging.	Het is aan de organisatie zelf om meer deelnemers te leveren voor dit overleg.
Het adviseert en stuurt aan op voorlichtingscampagnes en interne opleidingen aan het personeel van de deelnemer op het gebied van informatiebeveiliging. Door de collectieve aanschaf van bijvoorbeeld e-learnings kan maximaal geprofiteerd worden van de samenwerking in de share.	Advies voor de inrichting van voorlichtingscampagnes en elearnings.	De verantwoordelijkheid voor de implementatie van voorlichtingscampagnes en interne opleidingen ligt bij de deelnemer zelf.
Advies en rapportage		
De CISO initieert en stuurt op projecten met betrekking tot informatiebeveiliging.		De CISO wordt bij projecten met betrekking tot informatiebeveiliging gefaciliteerd door de deelnemer.
Het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie.		
Het geven van gevraagd en ongevraagd advies aan de leiding van de organisatie (in Zundert DT) over de te nemen maatregelen op strategisch en tactisch niveau.		De SO (beveiligingsbeheerder) beantwoord vragen op operationeel niveau.
De CISO coördineert het opstellen van rapportages aan de leiding van de organisatie over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles (BIG en ENSIA).	Input voor rapportages aan het college van B&W over de status van informatiebeveiliging binnen de gemeente (BIG en ENSIA)	De controller van de deelnemer toetst onafhankelijk of de organisatie voldoet aan alle gestelde eisen met betrekking tot informatiebeveiliging.
Werkzaamheden shareverband Equalit		
De CISO levert een bijdrage aan het informatiebeveiligingsbeleid en het informatiebeveiligingsplan voor het samenwerkingsverband.	-Informatiebeveiligingsbeleid voor de share -Informatiebeveiligingsplan voor de share	
Deelname aan expertgroepen binnen het Equalit samenwerkingsverband.		
Het uitvoeren of initiëren van risico analyses op shareniveau	Risico analyse op shareniveau	
Deelnemers informeren over beveiligingsincidenten op shareniveau.		
Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging en de doorvertaling maken naar de gevolgen voor de share.		

Aansluiten bij diverse landelijke gremia op het gebied van informatiebeveiliging en het volgen van trainingen en opleidingen op het gebied van informatiebeveiliging om nieuwe ontwikkelingen en wetgeving te vertalen naar de share.		

5 Voorwaarden voor de dienstverlening

5.1 Randvoorwaarden

Momenteel is er een tekort aan security specialisten op de markt. Equalit heeft met de deelnemers tijdens de deelnemersraad van maart 2018 afgesproken dat er gewerkt gaat worden met young professionals en dat we deze, in samenwerking met de deelnemers, zelf op willen leiden tot security specialisten middels een traineeship. De young professionals zullen begeleiding nodig hebben om tot het gewenste niveau te komen. De begeleiding vindt plaats op inhoudelijk vlak door het aanbieden van een opleidingsprogramma gericht op informatiebeveiliging. Daarnaast worden de young professionals gecoached door een senior CISO die de young professional inhoudelijk op weg kan helpen. Tevens dienen de young professionals begeleid te worden bij het ontwikkelen van persoonlijke competenties. Te denken valt hierbij bijvoorbeeld aan gesprekstechnieken, analyserend vermogen en plannen en organiseren. Deze begeleiding kan plaatsvinden door een buddy vanuit Equalit of een deelnemer. De young professionals zullen worden gestimuleerd om kennis te delen. Dit wordt gedaan door onderling bij elkaar mee te lopen, door intervisies of door het geven van presentaties onderling aan elkaar. Er dient rekening gehouden te worden met een opleidingstraject van 2 jaar.

5.2 Specifieke afspraken gemeente Zundert

- Per 15 oktober vervangt Ivo Caré, Karin van Zanten ivm haar zwangerschapsverlof
- Het aanspreekpunt voor de CISO bij de gemeente Zundert is Marco Schuurmans
- Het overzicht van rollen en taken is niet statisch, wanneer flexibiliteit in de werkzaamheden nodig is, zal dit in onderlinge afstemming tussen de deelnemer en de CISO van Equalit plaatsvinden.
- Marco Schuurmans vindt het prettig om op de hoogte te zijn van de werkzaamheden die uitgevoerd worden op het gebied van informatiebeveiliging. De werkzaamheden zullen in onderlinge samenwerking uitgevoerd worden.
- De CISO van Equalit zal periodiek (1x per 2 maanden) een koffie moment inplannen met het DLR lid van de gemeente.
- VCIB meldingen voor Zundert, zullen via Sringkela doorgestuurd worden naar Ivo.
- Ivo komt op woensdag in Zundert werken, de andere dag is in overleg.
- Voor 2018: Marco vult ISMS tot hoofstuk 10. Karin/Ivo vullen het ISMS vanaf hoofdstuk 10.

6 Goedkeuring

Deze dienstbeschrijving is goedgekeurd door de medewerkers van Equalit (Sringkela, Ivo en Karin) en door de gemeente Zundert (Anjo en Marco) op 9 oktober 2018.