College van burgemeester en wethouders

GOEDGEKEURD
Zitting van 26 maart 2019
Organisatie Ondersteuning - Organisatieadvies

4 **2019_B&W_00136** **Informatienota (informatie)beveiligheidsbeleid - informeren**

Samenstelling:

Aanwezig:
de heer R. Bats, Burgemeester; de heer B. Harmsma, Wethouder; mevrouw T. Jongman, Wethouder; de heer M. Scheringa, Wethouder; mevrouw T. Bijl; mevrouw J. de Groot, Secretaris

Informatienota

Inleiding
Informatiebeveiliging gaat verder dan alleen ICT. Beveiliging van gegevens en systemen is een zaak van de hele organisatie. Het gaat om mensen in de organisatie, om de manier waarop zij met risico's omgaan. Het gaat om het inrichten van processen en procedures, om kennis en bewustzijn. En in de laatste plaats pas om techniek. Of de bedreiging nu komt van een onbewuste medewerker, een criminele organisatie of een stroomstoring: de technische- en organisatorische maatregelen om schade te voorkomen, te beperken en te vermijden zijn hetzelfde. De aanpak van informatiebeveiliging is 'risk-based', dat wil zeggen dat maatregelen worden getroffen op basis van een uitgevoerde risicoanalyse en monitoring / analyse van uitgevoerde onderzoeken. Het Informatiebeveiligingsplan 2019 is op basis van deze aanpak tot stand gekomen.

Kernboodschap
Inwoners en ondernemers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn, dat de informatie die de gemeente uitwisselt met andere overheden betrouwbaar is en dat de gemeente zorgt voor een veilige leefomgeving. Een betrouwbare overheid start immers met het beschermen van de persoonlijke levenssfeer en gegevens die daarop betrekking hebben.

Consequenties voor de gemeente
Het informatiebeveiligingsplan 2019 ondersteunt de realisatie van het beveiligingsbeleid en wordt jaarlijks bijgesteld aan de eisen en ontwikkelingen op het gebied van informatieveiligheid.

Communicatie
Niet van toepassing.

Vervolg
Niet van toepassing.

Besluit

Beslispunt 1

De gemeenteraad met bijgevoegde brief en het informatiebeveiligingsplan 2019 te informeren over de wijze waarop in 2019 verdere invulling wordt gegeven aan het (informatie)beveiligingsbeleid.

Bijlagen

1. Raadsbrief d.d. 26 maart 2019.pdf
2. Jaarplan Informatiebeveiliging 2019.pdf

Gemeenteraad Steenwijkerland
Postbus 162
8330 AD STEENWIJK

zaaknummer
behandeld door Jilke Marinus
uw brief/kenmerk
Bijlage(n) Informatiebeveiligingsjaarplan 2019

datum 26 maart 2019

onderwerp Informatiebeveiligingsjaarplan 2019

Geachte leden van de gemeenteraad,

Inwoners en ondernemers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn, dat de informatie die de gemeente uitwisselt met andere overheden betrouwbaar is en dat de gemeente zorgt voor een veilige leefomgeving. Een betrouwbare overheid start immers met het beschermen van de persoonlijke levenssfeer en gegevens die daarop betrekking hebben. Steenwijkerland ziet de beveiliging van de aan haar toevertrouwde informatie dan ook als één van de hoogste prioriteiten.

Informatiebeveiliging.
We worden steeds afhankelijker van digitale voorzieningen die veelal tijd en plaatsonafhankelijk moet zijn waardoor informatiebeveiliging steeds belangrijker wordt.
Informatiebeveiliging gaat verder dan alleen ICT. Beveiliging van gegevens en systemen is een zaak van de gehele organisatie. Het gaat om mensen in de organisatie, om de manier waarop zij met risico's omgaan, het inrichten van processenen en procedures, om kennis en bewustzijn.

Informatiebeveiligingsjaarplan 2019
Voor u ligt het informatiebeveiligingsplan 2019. Het informatiebeveiligingsplan ondersteunt de realisatie van het beveiligingsbeleid en wordt jaarlijks aangepast aan de eisen en ontwikkelingen op het gebied van informatieveiligheid. De aanpak van informatiebeveiliging is 'risk-based'. Dat wil zeggen dat maatregelen worden getroffen op basis van een uitgevoerde risicoanalyse en monitoring/analyse van uitgevoerde onderzoeken.

De in het informatiebeveiligingsjaarplan 2019 opgenomen speerpunten en prioriteiten zijn de uitkomsten uit de in november 2018 uitgevoerde integrale risicoanalyse en de gedurende het jaar uitgevoerde interne en externe evaluaties.

Tot slot
Bij het op te stellen jaarverslag over 2019 zult u worden geïnformeerd over de stand van zaken uitvoering informatiebeveiligingsjaarplan 2019.

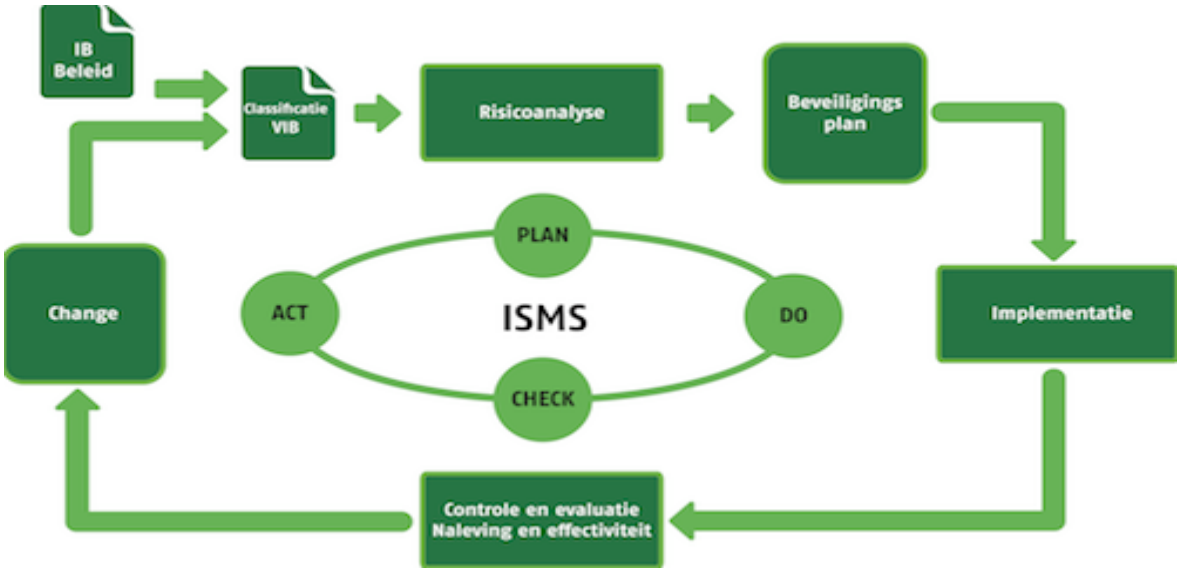
Met vriendelijke groet,

Burgemeester en wethouders van Steenwijkerland,

De secretaris,	de burgemeester,
Judith de Groot	Rob Bats

Fout! Ongeldige bestandsnaam.

Informatiebeveiligingsplan 2019



Auteur: CISO
Datum: 7 februari 2019
Versie: 1.0

VERSIEBEHEER

Versie	Datum	Auteur	Opmerkingen
0.1	januari 2019	CISO	Concept jaarplan 2019
1.0	4 februari 2019	CISO	Concept jaarplan 2019
1.1	7 februari 2019	CISO	Jaarplan 2019

INHOUDSOPGAVE

1. INLEIDING 2
1.1 Informatiebeveiliging 2
1.2 Trends en ontwikkelingen 2
2. INHOUDELIJKE SPECIFICATIE 3
2.1 Situatieschets 3
2.2 Doelstellingen van dit jaarplan 3
3. INFORMATIEBEVEILIGINGSPROCES STEENWIJKERLAND 4
3.1 Information Security Management System (ISMS) 4
4. Actiepunten 2019 4
4.1 Organisatie en Governance 4
4.2 Informatiegebruik en personele aspecten 5
4.3 Beheer 5
4.4 Toegangsbeveiliging en autorisatie 5
4.5 Bedrijfscontinuïteits-beheer 6
4.6 Naleving en controle 6
5. BEHEERSASPECTEN 7
5.1 Tijdsplanning mijlpalen (ingedeeld op kwartaal) 7

1. INLEIDING

Informatiebeveiliging wordt steeds belangrijker(ook binnen de gemeente), omdat we steeds afhankelijker worden van digitale informatievoorziening die veelal tijd en plaatsonafhankelijk toegankelijk moet zijn. Ook allerlei (nieuwe) wetgeving legt eisen op aan de informatiebeveiliging van gemeenten.
Dit plan geeft een overzicht van de acties op het gebied van informatiebeveiliging (security) voor het jaar 2019.

Voor u ligt het informatiebeveiligingsplan 2019 voor de gemeente Steenwijkerland.
Het informatiebeveiligingsplan ondersteunt de realisatie van het beveiligingsbeleid en wordt jaarlijks bijgesteld aan de eisen en ontwikkelingen op het gebied van informatieveiligheid. De aanpak van de informatiebeveiliging van de gemeente Steenwijkerland is 'risk based'. Dat wil zeggen dat maatregelen worden getroffen op basis van een uitgevoerde risicoanalyse en monitoring/ analyse van uitgevoerde onderzoeken. Het informatiebeveiligingsplan volgt de planning- en controlcyclus van de organisatie. In het beveiligingsplan worden de concrete doelen voor het betreffende jaar en de aanpak van de realisatie vastgelegd.

Met de komst van de Algemene Verordening gegevensbescherming (AVG) in mei 2018, is er (hernieuwde) aandacht voor de bescherming van persoonsgegevens (privacy) gekomen. Informatiebeveiliging en privacy zijn aandachtsgebieden die nauw met elkaar zijn verweven. Daar waar mogelijk zullen maatregelen uit het plan vanuit zowel informatiebeveiliging- als privacy oogpunt worden uitgevoerd.
Verantwoordelijk voor de uitvoering van dit plan is de Chief Information Security Officer (CISO). Daar waar het een integrale aanpak betreft op het gebied van privacy ligt de verantwoordelijkheid voor de uitvoering binnen de privacy-driehoek waarin naast de Privacy Officer (PO) ook de Functionaris Gegevensbescherming (FG) en de CISO werkzaam zijn.

1.1 Informatiebeveiliging.

Steenwijkerland ziet de beveiliging van de aan haar toevertrouwde informatie als één van hoogste prioriteiten. Inwoners en ondernemers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn, dat de informatie die de gemeente uitwisselt met andere overheden betrouwbaar is en dat de gemeente zorgt voor een veilige leefomgeving. Een betrouwbare overheid start immers met het beschermen van de persoonlijke levenssfeer en gegevens die daarop betrekking hebben.
Voor een goede informatiebeveiliging is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) leidend. Het conform de BIG opgestelde (Informatie)beveiligingsbeleid gemeente Steenwijkerland 2017-2020, moet ervoor zorgen dat zowel op strategisch als tactisch niveau wordt voldaan aan deze BIG-normen. Daarbij zijn de stand van de techniek en de behoeftes van de organisatie voortdurend aan veranderingen onderhevig. Dit maakt informatiebeveiliging een continue proces. Daarnaast wil Steenwijkerland met het oog op toekomstige samenwerking, onder andere op het gebied van de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI), aansluiten bij landelijke standaarden.

1.2 Trends en ontwikkelingen.

De belangrijkste trends en ontwikkelingen voor de gemeentelijke informatieveiligheid voor 2019/2020 zijn:
(bron IBD)

1. **Aandacht voor privacy**.
   De invoering van de AVG heeft een boost gegeven in de aandacht voor de bescherming van persoonsgegevens. Een positieve ontwikkeling die tevens helpt de informatieveiligheid te vergroten.
2. **Baseline informatieveiligheid**.
   De Baseline informatiebeveiliging Overheid (BIO) gaat de huidige BIG vervangen en wordt het nieuwe normenkader voor alle overheden.

3. **Internet of things en smart society**.
   Smart society-projecten dragen bij aan het vergroten van de leefbaarheid en veiligheid binnen de gemeente, zoals slimme lantaarnpalen of afvalbakken die aangeven dat ze vol zijn. De IoT- apparatuur en software die hiervoor kan worden ingezet zorgen echter wel voor meer risico's en kwetsbaarheden.
4. **Artificial Intelligence.**
   Kunstmatige intelligentie kan de gemeente helpen om beter inzicht te krijgen in hun processen en gegevens en daarmee zorgen voor een betere dienstverlening aan onze inwoners en ondernemers. De technologie is echter nog erg onvolwassen en vormt daarmee een risico op de bedrijfsvoering.
5. **Common Ground.**
   Vanuit het principe Common Ground werken gemeenten gezamenlijk aan de doelstelling om grip te hebben en te houden op de gemeentelijke informatievoorziening. Hiermee wordt een grote stap gezet in de richting van een open, transparante overheid waarbinnen gegevens sneller en veiliger kunnen worden uitgewisseld (GGI). Hiermee werkt de gemeente stapsgewijs aan de modernisering van de ICT-infrastructuur.

2. INHOUDELIJKE SPECIFICATIE

2.1 Situatieschets

Informatiebeveiliging gaat verder dan alleen ICT. Beveiliging van gegevens en systemen is een zaak van de hele organisatie. Het gaat om mensen in de organisatie, om de manier waarop zij met risico's omgaan. Het gaat om het inrichten van processen en procedures, om kennis en bewustzijn. En in de laatste plaats pas om techniek. Of de bedreiging nu komt van een onbewuste medewerker, een criminele organisatie of een stroomstoring: de technische en organisatorische maatregelen om schade te voorkomen, te beperken en te vermijden zijn hetzelfde. Risicomanagement is de basis van een goede informatiebeveiliging.

Voor het opstellen van het informatiebeveiligingsplan 2019 is de input verkregen vanuit de volgende rapporten/acties:

- Risico-inventarisatie en evaluatie 2018.
- Rekenkameronderzoek 2018.
- Aanbevelingen interim rapportage accountant 2018.
- Zelfevaluatie ENSIA 2018.
- GAP-analyse BIG.
- Nul-meting Privacy Baseline.
- Uitgevoerde Clean-desk acties.

2.2 Doelstellingen van dit jaarplan

1. Continue aandacht voor bewust omgaan met (gemeentelijke) informatie.
2. Verder verbeteren van informatiebeveiliging om daarmee de digitale weerbaarheid te verhogen.
3. Het informatiebeveiligingsbeleid en de bedrijfsvoering in overeenstemming brengen en houden met de vereisten uit de BIG. Dit beleid moet kenbaar en vindbaar zijn voor de organisatie.
4. Toepassen van een integrale benadering, vooral daar waar het gaat om informatiebeveiliging en privacy.
5. Informatiebeveiliging en privacy vormen een vast onderdeel van de bedrijfsvoering.

3. INFORMATIEBEVEILIGINGSPROCES STEENWIJKERLAND

3.1 Information Security Management System (ISMS)

Het Information Security Management System (ISMS) is de motor van de informatiebeveiligingsactiviteiten. Voor het monitoren en onderhouden van de beveiligingsactiviteiten wordt gebruik gemaakt van de verbetercyclus zoals de Plan-Do-Check-Act (PDCA)-cyclus.
In het (Informatie)beveiligingsbeleid Gemeente Steenwijkerland 2017-2020 zijn in de 'plan-fase' de volgende beveiligingsonderwerpen in het beleidskader informatiebeveiliging benoemd:

- Organisatie en Governance
- Informatiegebruik en personele aspecten
- Beheer
- Toegangsbeveiliging en autorisatie
- Bedrijfscontinuïteits-beheer
- Naleving en controle

Bij het opstellen van het jaarplan Informatiebeveiliging 2019 is de volgorde van de in de 'plan-fase' benoemde beveiligingsonderwerpen gehanteerd.

4. Actiepunten 2019

4.1 Organisatie en Governance

Voor het beheren van de informatieveiligheid binnen de organisatie is een kader noodzakelijk om deze te implementeren, te initiëren en te beheersen. De organisatie van de informatiebeveiliging in Steenwijkerland is geborgd met de vastgestelde Governance structuur (Informatiebeveiligingsbeleid gemeente Steenwijkerland 2017-2020). Hierin zijn functies, rollen en verantwoordelijkheden belegd en kan invulling worden gegeven aan de bijbehorende activiteiten, procedures en instrumenten om structureel uitvoering te geven en borgen van de noodzakelijke beheersmaatregelen.

	Actiepunten	kwartaal				wie
1.	Jaarlijks relevante informatiebeveiligingsrisico's in beeld brengen door middel van het uitvoeren van een Risico- Inventarisatie en Evaluatie(RI&E).				X	CISO
2.	Opstellen van een informatiebeveiligingsjaarplan op basis uitgevoerde zelfevaluaties en risico-inventarisaties.	X				CISO
3.	Opstellen implementatieplan Baseline Informatiebeveiliging Overheid (BIO)			X	X	CISO
3.	Opstellen en implementeren procedures om te kunnen voldoen aan wet- en regelgeving inzake intellectuele eigendomsrechten			X	X	TL O&F[1]
4.	Opstellen en implementeren processen 'Borging, Tijdigheid, Volledigheid en Juistheid' in het kader van de Basis Registratie Ondergrond (BRO)	X	X	X	X	TL ICT&B.[2]
5.	Vaststellen en implementeren van het proces Juistheid in het kader van de Basisregistratie Adressen en Gebouwen (BAG)	X	X			TL ICT&B.
6.	Onderzoek naar borging informatieveiligheid binnen het inkoopproces	X	X			TL OA[3]
7.	Organisatiebreed doorvoeren prestatieverklaarders	X	X	X	X	TL OA
8.	Voor nieuwe processen en systemen zal voorafgaand een Data Protection Impact Assessment (DPIA) worden uitgevoerd om een risicobeoordeling uit te voeren.	X	X	X	X	TL ICT&B.

[1] TL O&F>teamleider Ondersteuning en Faciliteiten
[2] TL ICT&B >teamleider ICT en Belastingen
[3] TL OA > teamleider Organisatie Advies

4.2 Informatiegebruik en personele aspecten

De meeste incidenten worden nog steeds veroorzaakt door menselijk handelen. Het is verleidelijk om met technologie te proberen om alle gebruiker-gerelateerde beveiligingsincidenten terug te dringen. Maar technologie alleen is niet de oplossing. Informatiebeveiliging begint bij de (bewuste) medewerker. Voldoende en regelmatige aandacht voor bewustwording van medewerkers is noodzakelijk. Bewuste medewerkers zijn namelijk de belangrijkste verdedigingslinie tegen informatiebeveiligingsincidenten. Aandacht voor informatiebeveiliging begint al bij het aannemen of inhuren van personeel en de benodigde opleiding van medewerkers.

	Actiepunten	Kwartaal				Verantwoordelijk
1.	Opstellen bewustwordingsjaarplan en uitvoeren organisatiebrede trainingen (informatieveiligheid en privacy)	X	X			CISO/FG/PO
2.	Uitvoeren van Clean-desk acties in samenwerking met teamleiders		X		X	CISO
3.	Training management en beveiligingsorganisatie d.m.v. crisisgame InformatieBeveiligingsDienst (IBD)	X		X		CISO
4.	Opstellen huisregels ten behoeve van medewerkers en extern ingehuurd personeel.	X				TL OA
5.	Verificatie van de achtergrond van alle personeel (vast, tijdelijk of extern) wordt periodiek gecontroleerd aan de hand van de eisen volgend uit de classificatie van informatie waar men toegang toe heeft.			X	X	TL OA
6.	Opleiden vervanger Basisregistratie Grootschalige Topografie (BGT) als beheerder in het kader van bedrijfscontinuïteit		X	X		TL ICT&B

4.3 Beheer

Inzake beheer is de doelstelling het waarborgen van een correcte en veilige bediening van ICT-voorzieningen en het vaststellen van verantwoordelijkheden en procedures voor beheer en bediening van deze voorzieningen. Het ontbreken van (de juiste) gegevens kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer/gebruik of problemen rondom de continuïteit van bedrijfsprocessen.

	Actiepunten	Kwartaal				Verantwoordelijk
1.	Implementeren van de richtlijnen voor classificatie en functiescheiding voor alle bedrijfsprocessen en essentiële gegevensverzamelingen(privacy gevoelig)	X	X	X	X	TL ICT&B
2.	Wegwerken achterstanden in meetwerk Basisregistratie Grootschalige Topografie (BGT)	X	X			TL ICT&B

4.4 Toegangsbeveiliging en autorisatie

Naast fysieke beveiliging dient onze technische beveiliging van informatie continue naar de stand van de techniek aangepast en verbeterd te worden. Bij informatiebeveiliging gaat het om het geheel van maatregelen, procedures en processen die erop zijn gericht de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de organisatie te garanderen. In het kader hiervan wordt in artikel 32 van de Algemene Verordening Gegevensbescherming (AVG) bijzondere aandacht gevraagd voor de beveiliging van persoonsgegevens. Technische beveiligingsincidenten, zoals hacks of onbevoegde toegang, moeten we zo goed mogelijk voorkomen.

	Actiepunten	Kwartaal				Verantwoordelijk
1.	Herzien toegangsbeleid (conform de BIG)	X		.		TL O&F
2.	Opstellen autorisatiematrix voor het toekennen van functie specifieke applicaties	X	X		.	TL OA
3.	Onderzoek instellen naar fysieke veiligheid tijdens avondopenstelling (geen conflictteam aanwezig)	X	X			TL OA
4.	Onderzoek naar extra beveiliging nooduitgangen	X				TL O&F

4.5 Bedrijfscontinuïteits-beheer

Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheersprocessen binnen de organisatie. Het onderbreken van bedrijfsactiviteiten moet worden tegengegaan en kritische bedrijfsprocessen moeten worden beschermd tegen de gevolgen van (omvangrijke) storingen in informatiesystemen.

	Actiepunten	Kwartaal				Verantwoordelijk
1.	Periodiek toepassen van een updatecyclus (Patchmanagement)	X	X	X	X	TL ICT&B
2.	Identificeren en vastleggen van gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden en de gevolgen hiervan (bedrijfscontinuïteit en informatiebeveiliging)	X	X	X	X	TL ICT&B
3.	Overzicht van systemen en applicaties waarin informatie wordt verwerkt updaten. (inrichten DSP)	X	X			TL OA

4.6 Naleving en controle

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin gewerkt wordt met (gevoelige) informatie. Door het monitoren van de informatieveiligheid kunnen risico's tijdig worden geïdentificeerd en passende beheersmaatregelen worden toegepast. Controle is onderdeel van het werkproces met als doel het waarborgen van de kwaliteit van informatie en ICT en compliance aan wet- en regelgeving.

	Actiepunten	Kwartaal				Verantwoordelijke
1.	Periodieke controle van logging bij bedrijfskritische/ privacy gevoelige applicaties		X		X	TL OA
2.	Check op uitgevoerde controles bij bedrijfskritische applicaties				X	CISO
3.	Periodieke controle (d.m.v. penetratietesten) om risico's voor de technische beveiliging inzichtelijk te maken	X				TL ICT&B
4.	Ieder kwartaal uitvoeren interne controle op volledigheid en juistheid Basisregistratie Grootschalige Topografie	X	X	X	X	TL ICT&B
5.	Opvragen testverslagen noodstroomaggregaat	X				TL O&F
6.	Monitoring/evaluatie van beveiligingsincidenten/ datalekken.	X	X	X	X	CISO/FG/PO
7.	De CISO rapporteert aan het management over de voortgang van het jaarplan en stelt waar nodig nieuwe actiepunten op.		X		X	CISO

5. BEHEERSASPECTEN

5.1 Tijdsplanning mijlpalen (ingedeeld op kwartaal)

Nr.	Actiepunten	Verantwoordelijke	Opleveren
1.	Opstellen van een informatiebeveiligingsjaarplan op basis uitgevoerde zelfevaluaties en risico-inventarisaties.	CISO	Q1
2.	Training beveiligingsorganisatie d.m.v. crisisgame InformatieBeveiligingsDienst (IBD)	CISO	Q1en Q3
3.	Periodieke controle (d.m.v. penetratietesten) om risico's voor de technische beveiliging inzichtelijk te maken	TL ICT&B	Q1
4.	Opstellen huisregels ten behoeve van medewerkers en extern ingehuurd personeel	TL OA	Q1
5.	Herzien toegangsbeleid (conform de BIG)	TL O&F	Q1
6.	Onderzoek naar extra beveiliging nooduitgangen	TL O&F	Q1
7.	Opvragen testverslagen noodstroomaggregaat	TL O&F	Q1

Nr.	Actiepunten	Verantwoordelijke	Opleveren
1.	Opstellen bewustwordingsjaarplan en uitvoeren organisatiebrede trainingen (informatieveiligheid en privacy	CISO/FG/PO	Q1 /Q2
2.	Uitvoeren van Clean-desk acties in samenwerking met teamleiders	CISO	Q2 en Q4
3.	De CISO rapporteert aan het management over de voortgang van het jaarplan en stelt waar nodig nieuwe actiepunten op.	CISO	Q2 en Q4
4.	Opstellen autorisatiematrix voor het toekennen van functie specifieke applicaties	TL OA	Q1/Q2
5.	Overzicht van systemen en applicaties waarin informatie wordt verwerkt updaten. (inrichten DSP)	TL OA	Q1/Q2
6.	Periodieke controle van logging bij bedrijfskritische/ privacy gevoelige applicaties	TL OA	Q2 en Q4
7.	Onderzoek instellen naar fysieke veiligheid tijdens avondopenstelling (geen conflictteam aanwezig)	TL OA	Q1/Q2
8.	Onderzoek naar borging informatieveiligheid binnen het inkoopproces	TL OA	Q1/Q2
9.	Wegwerken achterstanden in meetwerk Basisregistratie Grootschalige Topografie (BGT).	TL ICT&B	Q1/Q2
10.	Vaststellen en implementeren van het proces Juistheid in het kader van de Basisregistratie Adressen en Gebouwen (BAG)	TL ICT&B	Q2

Nr.	Actiepunten	Verantwoordelijke	Opleveren
1.	Training management d.m.v. crisisgame InformatieBeveiligingsDienst (IBD)	CISO	Q3
2.	Opleiden vervanger Basisregistratie Grootschalige Topografie (BGT) als beheerder in het kader van bedrijfscontinuïteit	TL ICT&B	Q2/Q3

Nr.	Actiepunten	Verantwoordelijke	Opleveren
1.	Jaarlijks relevante informatiebeveiligingsrisico's in beeld brengen door middel van het uitvoeren van een risico- Inventarisatie en Evaluatie(RI&E).	CISO	Q4
2.	Opstellen implementatieplan Baseline Informatiebeveiliging Overheid (BIO	CISO	Q3/Q4
3.	Uitvoeren van Clean-desk acties in samenwerking met teamleiders	CISO	Q4
4.	De CISO rapporteert aan het management over de voortgang van het jaarplan en stelt waar nodig nieuwe actiepunten op.	CISO	Q4
5.	Check op uitgevoerde controles bij bedrijfskritische applicaties	CISO	Q4
6.	Monitoring/evaluatie van beveiligingsincidenten/ datalekken.	CISO/FG/PO	Q1t/m Q4
7.	Voor nieuwe processen en systemen zal voorafgaand een Data Protection Impact Assessment (DPIA) worden uitgevoerd om een risicobeoordeling uit te voeren.	TL ICT&B	Q1 t/m Q4
8.	Implementeren van de richtlijnen voor classificatie en functiescheiding voor alle bedrijfsprocessen en essentiële gegevensverzamelingen(privacy gevoelig)	TL ICT&B	Q1 t/m Q4
9.	Periodiek toepassen van een updatecyclus (Patchmanagement)	TL ICT&B	Q1 t/m Q4
10.	Identificeren en vastleggen van gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden en de gevolgen hiervan (bedrijfscontinuïteit en informatiebeveiliging)	TL ICT&B	Q1 t/m Q4
11.	Ieder kwartaal uitvoeren interne controle op volledigheid en juistheid Basisregistratie Grootschalige Topografie(BGT)	TL ICT&B	Q1 t/mQ4
12.	Opstellen en implementeren processen 'Borging, Tijdigheid, Volledigheid en Juistheid' in het kader van de Basis Registratie Ondergrond (BRO	TL ICT&B	Q1 t/m Q4
13.	Periodieke controle van logging bij bedrijfskritische/ privacy gevoelige applicaties	TL OA	Q4
14.	Organisatiebreed doorvoeren prestatieverklaarders	TL OA	Q1 t/m Q4
15.	Verificatie van de achtergrond van alle personeel (vast, tijdelijk of extern) wordt periodiek gecontroleerd aan de hand van de eisen volgend uit de classificatie van informatie waar men toegang toe heeft.	TL OA	Q3/Q4
16.	Opstellen en implementeren procedures om te kunnen voldoen aan wet- en regelgeving inzake intellectuele eigendomsrechten	TL O&F	Q3/Q4

*voor de toewijzing van de actiepunten aan de verantwoordelijke teamleiders is gebruik gemaakt van het huidige organisatiemodel/teamindeling. Bij toekomstige organisatie/teamwijzigingen kan het voorkomen dat actiepunten opnieuw moeten worden toegekend.