DCJM

Informatie veiligheidsbeleid

Commeyne, Mario
14-12-2016

Managementsamenvatting

De directie van het Departement Cultuur, Jeugd, Sport en Media (verder het 'departement' genoemd) vindt bescherming van informatie van medewerkers, leveranciers en klanten van essentieel belang. Deze informatie staat opgeslagen op informatiesystemen. Deze informatiesystemen dienen op een toereikend niveau beveiligd te worden. Het Informatieveiligheidsbeleid geeft hiervoor de richtlijnen en uitgangspunten aan.

Dit document beschrijft het Informatieveiligheidsbeleid van het departement. Allereerst worden in hoofdstuk 2.2 de uitgangspunten en de doelstelling van het Informatieveiligheidsbeleid voor het departement toegelicht. Het gaat hierbij om het borgen van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de informatie binnen het departement.

In hoofdstuk 3 worden de strategische uitgangspunten voor het Informatieveiligheidsbeleid beschreven.

Om informatieveiligheid binnen een organisatie effectief te laten functioneren, dient een beveiligingsorganisatie opgezet te worden. Het informatieveiligheidsproces, zoals dat gehanteerd wordt binnen het departement beschrijft de organisatie van het beveiligingsproces, inclusief rollen en taken. Deze twee laatste, organisatie en proces staan beschreven in de hoofdstukken 4 en 5. In hoofdstuk 5 wordt onder andere beschreven hoe het beveiligingsproces raakvlakken heeft met, of samenwerkt met andere bedrijfsprocessen van de organisatie zoals bedrijfscontinuïteit, projectbeheer en incidentbeheer.

Na het opstellen van het Informatieveiligheidsbeleidsdocument zorgen ontwikkelingen op technisch en sociaal gebied ervoor dat het Informatieveiligheidsbeleid veroudert. Om dit te voorkomen dient het Informatieveiligheidsbeleid periodiek herzien te worden. De periode waarna of situaties die leiden tot het herzien van het Informatieveiligheidsbeleid staan beschreven in hoofdstuk 6.

Omdat informatieveiligheid begint bij de medewerkers van de organisatie is het belangrijk voldoende in te zetten op verhoogde of voortdurende bewustwording bij medewerkers en het management op vlak van informatieveiligheid. Dit wordt in hoofdstuk 7 uitgewerkt.

Informatieveiligheidsbeleid Departement Cultuur, Jeugd en Media

Inhoud

1 Versies en historiek van het document

1.1 Versies

Versie	Datum	Verantwoordelijke	Voornaamste wijzigingen
0.1	17/06/2016	Mario Commeyne	
0.2	26/07/2016	Gert Van Tittelboom	
0.3	14/11/2016	Mario Commeyne	Opmerkingen van Gert Willems en Gert van Tittelboom verwerkt.
0.5	14/12/2016	Mario Commeyne	Opmerkingen van de IT Taskforce verwerkt.
1.1	24/02/2017	Mario Commeyne	Aangepast naar de nieuwe naamgeving DCJSM vervangen door DCJM

1.2 Goedkeuring

Versie	Goedgekeurd op	Verantwoordelijke bestuur
1.0	23/01/2017	Directiecomite Deparement Cultuur, Jeugd en Media

2 Inleiding

2.1 Missie van de organisatie

Voorlopig heeft het departement geen missie, zodra de missie officieel wordt goedgekeurd wordt deze opgenomen in het informatieveiligheidsplan.

2.2 Definitie informatieveiligheid en doelstelling

Onder informatieveiligheid wordt het proces verstaan van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit evenals het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Het gaat om de beveiliging van informatie, die over het algemeen is opgeslagen in informatiesystemen, maar ook opgeslagen kan zijn op papieren dragers.

Met vertrouwelijkheid wordt bedoeld: het waarborgen dat informatie alleen toegankelijk is voor diegenen die hiertoe zijn geautoriseerd;

Met beschikbaarheid wordt bedoeld: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot de informatie/informatiesystemen;

Met integriteit wordt bedoeld: het waarborgen van de correctheid en volledigheid van de informatie.

Het informatieveiligheidsbeleid is erop gericht om, op basis van risicomanagement, zeker te stellen dat de informatie van het departement correct en volledig is en tijdig toegankelijk voor de geautoriseerde personen.

2.3 Toepassingsgebied

Het informatieveiligheidsbeleid is bindend voor alle afdelingen van het departement.
Het informatieveiligheidsbeleid is van toepassing op het gehele proces van informatievoorziening en geldt gedurende de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het terrein van de informatieveiligheid beperkt zich niet tot bepaalde functies of functionarissen, maar geldt voor alle medewerkers en voor alle (mondelinge en schriftelijke) informatie. Het strekt zich uit over zowel de strategische, de tactische als de operationele organisatieniveaus. Tot slot heeft het informatieveiligheidsbeleid ook betrekking op ketens van informatiesystemen die zich kunnen uitstrekken tot buiten het departement en de externe partijen waarmee het departement samenwerkt.

2.4 Beheer van het beleidsdocument

Het informatieveiligheidsbeleid wordt minimaal jaarlijks, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Bij deze actualisatie worden nieuwe ontwikkelingen op het terrein van de bedrijfsvoering en op het terrein van informatieveiligheid en privacy meegenomen. Verantwoordelijke voor het bijstellen en actueel houden van het informatieveiligheidsbeleid is de Informatieveiligheidsconsulent

De Informatieveiligheidsconsulent onderhoudt contact met de relevante partijen, waaronder:

- Andere overheidsinstellingen
- Expertisegroepen
- ICT-leveranciers

De Informatieveiligheidsconsulent gebruikt deze contacten om informatieveiligheid te verbeteren en zo nodig te vertalen naar nieuw beleid. Het informatieveiligheidsbeleid wordt van kracht na validatie door het directiecomité. Bij het van kracht worden van dit document worden vorige versies van het informatieveiligheidsbeleid ingetrokken.

Het geactualiseerde informatieveiligheidsbeleid wordt gepubliceerd op het extranet.

3 Strategische uitgangspunten

De volgende uitgangspunten worden gehanteerd om de doelstelling van informatieveiligheid binnen het departement te verwezenlijken:

- Het informatieveiligheidsbeleid van het departement voldoet aan de Belgische wet- en regelgeving en inzonderheid de privacywetgeving
- Het informatieveiligheidsbeleid volgt de minimale normen van de Kruispuntbank Sociale Zekerheid (KSZ) ten aanzien van informatieveiligheid. Deze zijn gebaseerd op de ISO 27002 norm.

3.1 Uitgangspunten informatieveiligheidsbeleid bij het departement

Het departement is gehouden om de minimale normen van het KSZ te volgen. Deze zijn gebaseerd op de ISO 27002 norm en vormen dan ook de hoeksteen van het informatieveiligheidsbeleid.

Het generieke veiligheidsbeleid van de Vlaamse overheid, uitgewerkt volgens dezelfde ISO-norm wordt bij deze ook onderschreven.

3.2 De toepassingsdomeinen met de doelstellingen

ISO Referentie

5 Informatieveiligheidsbeleid

5.1 Aansturing door de directie van de informatieveiligheid

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatieveiligheid in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

6 Organiseren van informatieveiligheid

6.1 Interne organisatie

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatieveiligheid binnen de organisatie te initiëren en te beheersen.

6.2 Mobiele apparatuur en telewerken

Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

7 Veilig personeel

7.1 Voorafgaand aan het dienstverband

Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.

7.2 Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatieveiligheid en deze nakomen.

7.3 Beëindiging en wijziging van dienstverband

Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

8 Beheer van bedrijfsmiddelen

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.

8.2 Informatieclassificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.

8.3 Behandelen van media

Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

9 Toegangsbeveiliging

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatie verwerkende faciliteiten beperken.

9.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

9.3 Verantwoordelijkheden van gebruikers

Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie informatie.

9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

9..5 Toegangsbeveiliging op programmabroncode

10 Cryptografie

10.1 Cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

11 Fysieke beveiliging en beveiliging van de omgeving

11.1 Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.

11.2 Apparatuur

Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

12 Beveiliging bedrijfsvoering

12.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.

12.2 Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.

12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens.

12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.5 Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen.

12.6 Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

12.7 Overwegingen betreffende audits van informatiesystemen

Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

13 Communicatiebeveiliging

13.1 Beheer van netwerkbeveiliging

Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.

13.2 Informatietransport

Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14.1 Beveiligingseisen voor informatiesystemen

Doelstelling: Waarborgen dat informatieveiligheid integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling: Bewerkstelligen dat informatieveiligheid wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

14.3 Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.

15 Leveranciersrelaties

15.1 Informatieveiligheid in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

15.2 Beheer van dienstverlening van leveranciers

Doelstelling: Een overeengekomen niveau van informatieveiligheid en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

16 Beheer van informatieveiligheidsincidenten

16.1 Beheer van informatieveiligheidsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheidsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

17 Informatieveiligheidsaspecten van bedrijfscontinuïteitsbeheer

17.1 Informatieveiligheidscontinuïteit

Doelstelling: Informatieveiligheidscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.

18 Naleving

18.1 Naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatieveiligheid en beveiligingseisen.

18.2 Informatieveiligheidsbeoordelingen

Doelstelling: Verzekeren dat informatieveiligheid wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.

3.3 Opsomming van de wetgevingen

Voor het departement zijn er geen aparte wetgevingen m.b.t. informatieveiligheid van toepassing.

3.3.1 Website privacycommissie

http://www.privacycommission.be/nl/wetgeving-en-normen

3.3.2 Website VTC

VTC : Vlaamse ToezichtsCommissie

http://vtc.corve.be/wetgeving.php

4 Informatieveiligheidsorganisatie

4.1 Rollen binnen Informatieveiligheid

Hieronder worden beknopt de rollen, bevoegdheden en verantwoordelijkheden beschreven voor de informatieveiligheid.

4.1.1 Leidinggevend ambtenaar

De secretaris-generaal is verantwoordelijk voor het dagelijks bestuur. Daardoor is hij de eindverantwoordelijke voor de verwerking van persoonsgegevens en informatieveiligheidsbeleid. Dit informatieveiligheidsbeleid wordt jaarlijks goedgekeurd door het directiecomité.

4.1.2 CIO

~~De CIO is verantwoordelijk voor het vaststellen van de betrouwbaarheidseisen en een samenhangend pakket aan beveiligingseisen voor de systemen (opzet, bestaan en werking), mede-gebaseerd op de classificatie van de informatie die op dat systeem wordt verwerkt of opgeslagen. Hij wordt hierin bijgestaan door de CISO;~~

Het departement heeft geen Chief Information Officer. Een deel van zijn takenpakket wordt uitgevoerd door de informatieveiligheidsconsulent.

4.1.3 CISO

~~De Security Officer onderhoudt de departementale architectuur en standaarden vanuit de afgesproken(informatieveiligheids) kaders; bewaakt het overzicht van informatiesystemen en hun eigenaars; vertaalt de beveiligingsnormen naar eisen aan de processen en systemen en controleert of projecten voldoen aan deze eisen; signaleert bij het voornemen om nieuwe informatiesystemen in productie te nemen het eventueel ontbreken van een risicoanalyse (en maatregelen) aan de CIO;~~

Het departement heeft geen Chief Information Security Officer. Een deel van zijn takenpakket wordt uitgevoerd door de informatieveiligheidsconsulent.

4.1.4 Informatieveiligheidscel

(zie minimale normen KSZ: 3.1.4)

De informatieveiligheidscel volgt de uitvoering van het beveiligingsbeleid op. De informatieveiligheidscel bestaat uit de volgende medewerkers:

- verantwoordelijke ICT
- verantwoordelijke Personeel
- verantwoordelijke Communicatie
- verantwoordelijke Facility (gebouwen)
- informatieveiligheidsconsulent

De informatieveiligheidscel heeft een adviserende, stimulerende, documenterende en controlerende opdracht binnen de organisatie op vlak van informatieveiligheid.

De informatieveiligheidscel wordt op de hoogte gesteld van incidenten en risico's die de informatieveiligheid van persoonsgegevens in gedrang brengen en genomen maatregelen die van invloed zijn op de informatieveiligheid van persoonsgegevens.

De veiligheidsconsulent is de voorzitter van de informatieveiligheidscel.

4.1.5 Veiligheidsconsulent

De taken en bevoegdheden van de veiligheidsconsulent staan beschreven in het "Besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten"

Art. 3.

De veiligheidsconsulent is, met het oog op de veiligheid van de gegevens, ermee belast om:

1° op eigen initiatief of op verzoek van de verantwoordelijke voor het dagelijks bestuur van de instantie of entiteit deskundige adviezen en aanbevelingen te verstrekken aan de verantwoordelijke voor het dagelijks bestuur van de instantie of de entiteit in kwestie over alle aspecten op het vlak van de informatieveiligheid. De adviezen worden schriftelijk en gemotiveerd uitgebracht, tenzij de risico's niet voldoende ernstig zijn. Binnen de periode, vereist door de omstandigheden, van maximaal drie maanden beslist de verantwoordelijke voor het dagelijks bestuur het advies al dan niet te volgen en deelt hij de veiligheidsconsulent de genomen beslissing mee. Als de beslissing afwijkt van een schriftelijk advies van de veiligheidsconsulent, wordt ze schriftelijk en op gemotiveerde wijze aan de veiligheidsconsulent meegedeeld;

2° opdrachten uit te voeren die aan hem worden toevertrouwd door de verantwoordelijke voor het dagelijks bestuur van de instantie of de entiteit in kwestie.

Art. 6.

De veiligheidsconsulent bevordert en ziet toe op de naleving van de veiligheidsvoorschriften, opgelegd door of krachtens een wets-, decretale of reglementsbepaling, en controleert of de personen die in de instantie of de entiteit persoonsgegevens verwerken, een veiligheidsgedrag vertonen.

De veiligheidsconsulent legt de nodige documentatie aan over de informatieveiligheid. Alle vastgestelde overtredingen worden schriftelijk en uitsluitend aan de verantwoordelijke voor het

dagelijks bestuur van de instantie of de entiteit meegedeeld, en de nodige adviezen worden bijgevoegd om dergelijke overtredingen in de toekomst te vermijden.

Art. 8.

De veiligheidsconsulent werkt onder het rechtstreekse functionele gezag van de verantwoordelijke voor het dagelijks bestuur van de instantie of de entiteit in kwestie. Hij werkt nauw samen met de diensten waarin zijn optreden vereist is of kan zijn, inzonderheid met de informaticadienst en de preventieadviseur van de instantie of de entiteit in kwestie.

4.1.6 Lijnmanagement

Het lijnmanagement ziet toe op de correcte toepassing van het informatieveiligheidsbeleid. Eventuele tekortkomingen en/of inbreuken worden gemeld aan de informatieveiligheidsconsulent.

4.1.7 Medewerkers

De medewerker is verantwoordelijk voor het zorgvuldig omgaan met (vertrouwelijke) informatie conform het Informatieveiligheidsbeleid. Binnen het departement tekent iedere medewerker een overeenkomst waarin hij of zij verklaart zich aan de gedragscode ICT te houden.

4.1.8 Dienst IT

De medewerkers van de dienst IT hebben, meer nog dan de gewone medewerkers, toegang tot vertrouwelijke informatie. Zij kunnen gegevens (databanken, systemen, documenten) raadplegen die in se niet toegankelijk zijn voor hen.

4.1.9 Externe partijen

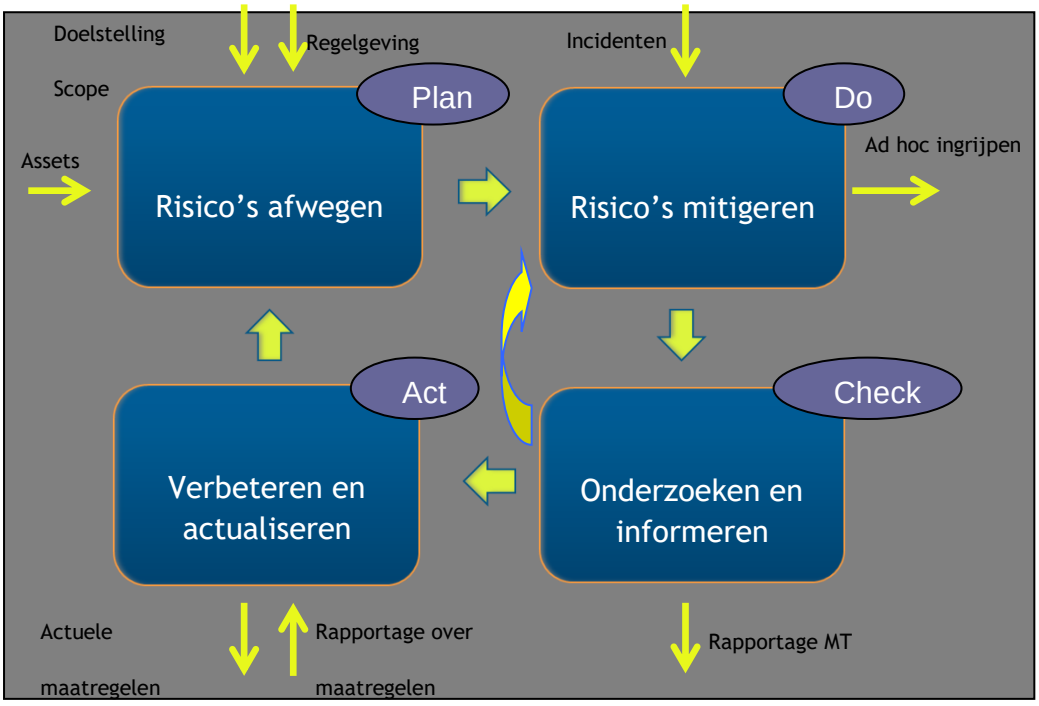
Wanneer in het kader van informatieveiligheid taken worden uitgevoerd door externe organisaties worden in een schriftelijke dienstverleningsovereenkomst de belangen van het departement geborgd.

5 Informatieveiligheidsproces

In dit hoofdstuk worden het informatieveiligheidsproces, risicomanagement en het gemeenschappelijk informatieveiligheidsniveau beschreven. Doel van dit hoofdstuk is om inzicht te geven in het proces van informatieveiligheid, de aansturing van dit proces en de samenhang met de bedrijfsprocessen van het departement.

5.1 Informatieveiligheidsproces (PDCA-cyclus)

Het informatieveiligheidsproces zelf is, in overeenstemming met de ISO 27002 norm, ingericht op basis van de Plan-Do-Check-Act-cyclus (zie figuur 1). De PDCA-cyclus zorgt voor periodieke toetsing van de werking en de noodzaak van gekozen maatregelen en leidt zo tot continue verbetering van de informatieveiligheid. De maatregelen worden geïmplementeerd op basis van risicomanagement en een bewuste kosten-baten afweging. Dit zorgt voor een optimale beveiliging tegen een aanvaardbare kost. Hiermee wordt invulling gegeven aan beleid van het departement om veilig te faciliteren in plaats van maximaal te beveiligen.



Figuur 1 het beveiligingsproces.

5.2 Aansturing van het proces

Informatieveiligheid gaat om het voortdurend bepalen van risico's, het kunnen reageren op incidenten en het nemen van adequate maatregelen op basis van risicomanagement. Om de risico's te bewaken en te beheersen is binnen het departement een informatieveiligheidsproces ingericht. Het proces wordt aangestuurd vanuit het lijnmanagement, omdat daar de verantwoordelijkheid ligt met betrekking tot de informatieveiligheid.

Het management wordt daarbij ondersteund door de informatieveiligheidsconsulent. Doel van het beveiligingsproces is het inzichtelijk maken van de (rest)risico's voor een bepaalde situatie of informatiesysteem zodat de lijnmanager op basis hiervan tot een weloverwogen besluit kan komen.

Wet- en regelgeving stellen de minimumeisen waaraan informatieveiligheid moet voldoen. Het eerbiedigen ervan is een uitgangspunt voor de inrichting van het beveiligingsproces. Andere organisaties van binnen en buiten het departement kunnen eisen stellen aan de informatieveiligheid van het departement voor de borging van hun bedrijfsprocessen. Andersom zal het departement bij het buiten de organisatie brengen van informatie eisen stellen aan de informatieveiligheid van de ontvangende partijen en bij het ontvangen van informatie eisen stellen aan de informatieveiligheid van de leverende partijen.

Om de risico's te verkleinen worden maatregelen getroffen in de bedrijfsprocessen en de daarbinnen gebruikte informatiesystemen. Informatieveiligheidsincidenten kunnen aanleiding zijn om (aanvullende) maatregelen te nemen en de bestaande maatregelen te evalueren.

Directies en ICT-dienstverleners rapporteren over de voortgang, actualiteit en de effectiviteit van de maatregelen. Vanuit het beveiligingsproces kan hierop worden ingegrepen door verbetervoorstellen in te dienen.

5.3 Bedrijfscontinuïteitsbeheer (BCM)

De Bedrijfscontinuïteit die wordt ondersteund door toepassingen , wordt uitvoerig behandeld in

Business Continuity Management – partim ICT

5.4 Projecten

In projecten met een ICT-component wordt, voorafgaand aan de ontwikkeling of aankoop, een risicoanalyse gedaan om de betrouwbaarheidseisen te bepalen. De afweging ten aanzien van de noodzaak en de wijze van beveiliging dienen een onderdeel van de investeringsbeslissing te vormen, ook wanneer wordt besloten een externe partij in te huren. De informatieveiligheid binnen projecten komt ten laste van het budget van de projectverantwoordelijke.

5.5 Security impact assessment (SIA)

Een SIA dient te worden uitgevoerd:

- Voor nieuwe functionaliteiten en/of nieuwe informatiesystemen die persoonsgegevens verwerken in de zin van de privacywetgeving;
- Bij belangrijke herzieningen van een informatiesysteem dat persoonsgegevens verwerkt.

De uitkomst van de SIA moet worden voorgelegd de informatieveiligeidscel. Deze SIA maakt onderdeel uit van de releaseplanning.

5.6 Incident management

De eindverantwoordelijkheid voor de melding en afhandeling van incidenten en inbreuken op de informatieveiligheid berust bij de informatieveiligheidsconsulent.

Informatieveiligheidsincidenten zowel met als zonder een ICT-component worden gemeld aan de informatieveiligheidsconsulent.

De externe dienstverlener belast met het End-to-End management rapporteert over de informatieveiligheidsincidenten aan de informatieveiligheidsconsulent.

De informatieveiligheidsconsulent houdt een registratie bij van alle informatieveiligheidsincidenten en de afhandeling daarvan, om inzicht te krijgen in trends en ontwikkelingen. Dit dient als input voor de evaluatie en het bijstellen van het informatieveiligheidsbeleid en/of het veiligheidsplan.

Incidenten die een risico vormen voor andere entiteiten binnen de Vo worden gemeld aan het centrale meldpunt informatieveiligheid Vo.

6 Evaluatie, verantwoording, toetsing, toezicht

6.1 Evaluatie

Het beleid, de betrouwbaarheidseisen en de maatregelen worden op centraal niveau (door een onafhankelijke deskundige) één keer in de drie jaar geëvalueerd, om vast te stellen of deze leiden tot de gewenste mate van beveiliging. De evaluatie kan aanleiding geven tot het bijstellen van het informatieveiligheidsbeleid, de betrouwbaarheidseisen en/of de maatregelen.

6.2 Verantwoording

Het departement legt jaarlijks verantwoording af over informatieveiligheid aan de KSZ door het invullen van de vragenlijst ter evaluatie van de minimale veiligheidsnormen.

6.3 Toetsing

De opzet, bestaan en werking van de maatregelen worden periodiek getoetst met een audit en/of penetratietest. Het doel van deze toetsing is na te gaan of aan de afgesproken normen wordt voldaan.

6.4 Toezicht

De informatieveiligheidsconsulent houdt toezicht op de informatieveiligheid door middel van bovengenoemde toetsingsinstrumenten en door middel van de jaarlijks zelfevaluaties die worden uitgevoerd.

6.5 Rapportages

Jaarlijks rapporteert de informatieveiligheidsconsulent aan het lijnmanagement over de evaluatie, verantwoording, toetsing, toezicht.

7 Bevordering Security Awareness

7.1 Zwakste en sterkste schakel

Een goede informatieveiligheid hangt niet alleen af van technische maatregelen maar heeft ook een belangrijke relatie met het gedrag van medewerkers. De beveiligingsketen is zo sterk als de zwakste schakel. Dit blijkt vaak het gedrag van medewerkers te zijn, die zich niet steeds bewust zijn van de risico's van hun handelen. Technische maatregelen kunnen dit vaak niet oplossen.

Daarom is het belangrijk medewerkers te wijzen op veilig gedrag. Medewerkers hebben een eigen verantwoordelijkheid bij het zorgvuldig en integer omgaan met informatie die zij verwerken. Dit betekent niet alleen dat zij vertrouwelijke informatie als zodanig herkenbaar maken voor anderen (classificeren), maar ook dat zij vertrouwelijke informatie alleen delen met anderen die deze informatie nodig hebben voor hun werkzaamheden, vertrouwelijke informatie volgens het vier ogen-principe verwerken, en ervoor zorgen dat onbevoegden geen kennis

kunnen nemen van deze informatie (veilig opbergen of clear desk-principe, versleuteld verzenden, informatie alleen delen op basis van need to know in plaats van nice to know). Medewerkers volgen de classificatierichtlijnen en kennen de regels voor informatieveiligheid.

7.2 Activiteiten om het beveiligingsbewustzijn te vergroten

Het vergroten van het veiligheidsbewustzijn bij medewerkers van het departement wordt bereikt door periodiek gerichte activiteiten te organiseren. Het departement initieert en coördineert de periodiek uit te voeren bewustwordingsprogramma's in de vorm van bewustwordingscampagnes, gedragscodes, nieuwsbrieven, presentaties en nieuwsvoorziening via het extranet. Het extranet bevat de basisinformatie die steeds toegankelijk is voor de medewerkers van het departement en regelmatig geactualiseerd wordt. Het departement stelt hiervoor een actieplan op. Informatieveiligheid maakt eveneens een standaard onderdeel uit van de introductieopleiding voor nieuwe medewerkers.

De lijnmanagers verlenen hun medewerking aan en ondersteunen deze activiteiten. Daarnaast is de lijnmanager zelf ook verantwoordelijk voor het vergroten van de bewustwording van zijn/haar medewerkers. Dit kan bijvoorbeeld door informatieveiligheid bespreekbaar te maken in werkoverleggen en in start- en functioneringsgesprekken.