DCJM

Informatie veiligheidsbeleid

InformatieVeiligheidsCel
1-1-2024

Managementsamenvatting

De directie van het Departement Cultuur, Jeugd, 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.

Inhoud

1 Versies en historiek van het document

1.1 Versies

Versie	Datum	Verantwoordelijke	Voornaamste wijzigingen
0.1	09/02/2023	Mario Commeyne	insteek
0.2	*30/03/2023*	*Informatieveiligheidscel*	*Opmerkingen AD*
0.3	04/05/2023	Mario Commeyne	Opmerkingen IVC verwerkt
1	08/11/2023	Departementsvergadering	Opmerkingen DV verwerkt

1.2 Goedkeuring

Versie	Goedgekeurd op	Verantwoordelijke bestuur
1	08/11/2023	Departementsvergadering

2 Inleiding

2.1 Visie en Missie van de organisatie

Visie

Als voortrekker bouwen we aan een creatief en inspirerend Vlaanderen, waar iedereen (van jong tot oud) cultuur kan beleven, maken en delen.

Missie

We stimuleren als knooppunt tussen samenleving en beleid de ontwikkeling van culturele en sociale ruimtes, met de blik op de lange termijn.

Onder “knooppunt” verstaan we: een centrum van kennis en expertise dat mensen, tendensen en ideeën uit de samenleving samenbrengt, denksporen ontwikkelt en helpt omzetten in beslissingen met een culturele impact.

Onder “culturele ruimtes” verstaan we: mentale en fysieke ruimtes waar individuen en groepen (van jong tot oud) – in een grote dynamiek en onderlinge verwevenheid – uitdrukking geven aan cultuur (in zijn breedste zin), op allerlei manieren en onder allerlei vormen; ruimtes ook waarin een ‘cultureel (zelf)bewustzijn’ leeft.

Onder “sociale ruimtes” verstaan we: mentale en fysieke ruimtes waarbinnen mensen (van jong tot oud) op verschillende manieren met elkaar in dialoog en interactie gaan en participeren aan de samenleving.

Onder “stimuleren” verstaan we: er mee voor zorgen dat bestaande ideeën en initiatieven opgepikt worden en gerealiseerd kunnen worden of dat nieuwe ideeën en initiatieven ontstaan en zich kunnen ontwikkelen. Dit doen we door te inspireren, te faciliteren (financieel of op andere wijze te ondersteunen) en te advies te verlenen.

https://www.vlaanderen.be/cjm/nl/over-cjm/missie-en-visie

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.

De beveiliging van informatie houdt in dat zij beschermd wordt tegen onbevoegde toegang en verwerking, waarbij er maatregelen worden genomen om volgende kwaliteitskenmerken te garanderen:

> Vertrouwelijkheid: de informatie is alleen toegankelijk voor geautoriseerde personen en entiteiten of voor de juiste processen;
>
> Integriteit: de informatie is juist en volledig;
>
> Beschikbaarheid: de informatie is op het gewenste moment toegankelijk en beschikbaar

Vaak worden informatieveiligheid en bescherming van persoonsgegevens als hetzelfde beschouwd. Dat is begrijpelijk, want er zijn verschillende raakvlakken. Zo speelt de risico gebaseerde aanpak,

waarbij op basis van een risicoanalyse maatregelen worden geselecteerd om de veiligheid van de gegevens te borgen, binnen beide domeinen een centrale rol. En beide domeinen zijn erop gericht om informatieveiligheidsrisico's te verkleinen. Maar er zijn ook verschillen:

- De aard van de gegevens: informatieveiligheid omhelst ***alle*** gegevens waarover DCJM beschikt, persoonsgegevens zijn die gegevens die herleidbaar zijn naar een natuurlijk persoon.

- De aard van de risico's: zowel bescherming van persoonsgegevens als informatieveiligheid beoogt risico's terug te brengen tot een aanvaardbaar niveau. Maar er zit een verschil in de aard van die risico's. Bij bescherming van persoonsgegevens draait het om risico's die impact hebben op mensen. Bij informatieveiligheid draait het niet om de impact voor individuen, maar om het beheersen van bedrijfsrisico's: informatieveiligheid gaat dan over het beschermen van informatie om de bedrijfsvoering te kunnen garanderen. Oftewel, hoe ervoor zorgen dat de juiste mensen en systemen toegang hebben tot de juiste informatie op het juiste moment.

- Al dan niet aanvaarden van risico's: bij het beheersen van risico's wordt er bekeken of er al dan niet actie moet worden genomen. Organisaties bepalen zelf hoeveel risico zij bereid zijn om te nemen. Sommige organisaties zijn risico avers en zullen er alles aan doen om deze bedrijfsrisico's zo klein mogelijk te houden. Andere organisaties hebben een grotere risico appetijt en zijn bereid om meer risico te accepteren, als daar een potentieel voordeel tegenover staat. Binnen de Vo moet risicoacceptatie op het juiste managementniveau gebeuren afhankelijk van het risico; indien een risico rechtstreeks impact heeft op andere Vo entiteiten moet hiermee rekening worden gehouden. De afweging hoeveel bedrijfsrisico wordt genomen is dus aan de Vo zelf. Gaat het echter over bescherming van persoonsgegevens, dan geldt er strikte wetgeving, namelijk de AVG. Het accepteren van risico's voor persoonsgegevens zou een directe inbreuk van de AVG kunnen betekenen, waardoor het geen optie meer is om die risico's te accepteren. Organisaties zullen in die gevallen dan noodgedwongen moeten kiezen voor het vermijden of verkleinen van risico's.

Natuurlijk zijn er ook raakvlakken: waar een organisatie technische en organisatorische maatregelen inricht om bedrijfsinformatie te beschermen, zijn die er ook om persoonsgegevens die de organisatie verwerkt, te beveiligen.

Bij bescherming van persoonsgegevens staat dus veel meer de mens (persoon van wie gegevens opgeslagen/verwerkt worden) centraal, waar bij informatiebeveiliging de gegevens zelf en de verantwoordelijke organisatie centraal staan.

Binnen organisaties zien we dan ook vaak dat verschillende partijen zich bezighouden met informatieveiligheid dan wel bescherming van persoonsgegevens: informatieveiligheid is het domein van de CISO terwijl de DPO (Data Protection Officer) zich buigt over de bescherming van persoonsgegevens en conformiteit met de betreffende wetgeving.

2.3 Toepassingsgebied

Een beleid (of policy) is een thematische groepering van regels die de organisatie en haar medewerkers moeten volgen. Het informatieveiligheidsbeleid beschrijft dus de regels waaraan de organisatie en haar medewerkers moeten voldoen m.b.t. informatieveiligheid. Het legt daarvoor definities, processen, vereisten en beperkingen vast.

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 CISO.

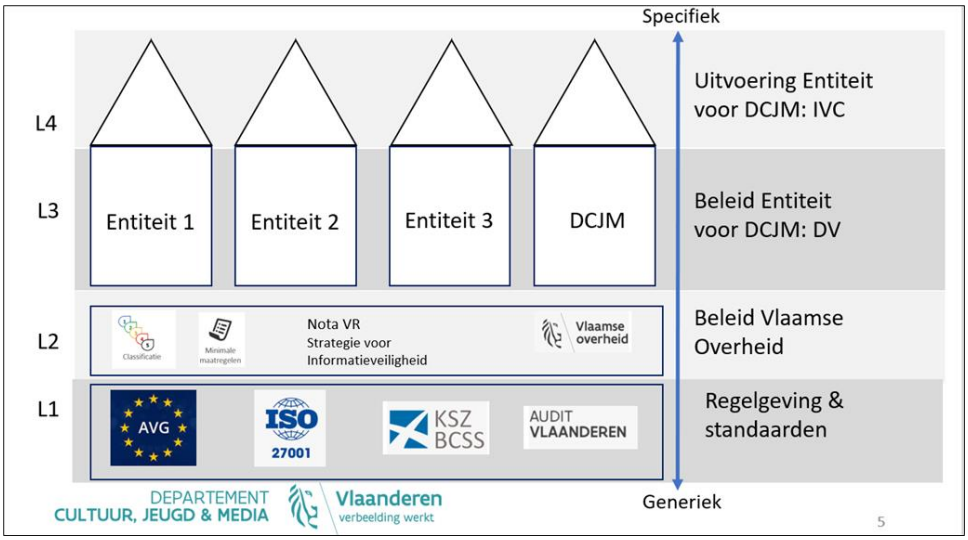
Het informatieveiligheidsbeleid wordt van kracht na validatie door de Departementsvergadering. Bij het van kracht worden van dit document worden vorige versies van het informatieveiligheidsbeleid ingetrokken.

Het geactualiseerde informatieveiligheidsbeleid wordt gepubliceerd op het de website van DCJM.

3 Context

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

- Het informatieveiligheidsbeleid van het departement voldoet aan de Algemene Verordening Gegevensbescherming, en andere Europese regelgeving inzake informatieveiligheid
- Het informatieveiligheidsbeleid van het departement voldoet aan de Belgische wet- en regelgeving.
- Het informatieveiligheidsbeleid volgt de nota aan de Vlaamse Regering betreffende “Strategie voor Informatieveiligheid” van 2021. Deze nota bevat de doelstellingen, leidende principes en rollen/verantwoordelijkheden met betrekking tot informatieveiligheid binnen de Vlaamse overheid.
- Het informatieveiligheidsbeleid voldoet aan het Raamwerk voor VO-informatieclassificatie (of InformatieClassificatieRaamwerk [ICR]). Dit Raamwerk is de leidraad voor informatiebeveiliging op niveau van de Vlaamse Overheid. Op basis van de classificatie van de informatie, bepaalt het de minimummaatregelen die op een gemeenschappelijke manier van toepassing zijn op alle Vlaamse entiteiten in scope van deze nota. Dit raamwerk is gebaseerd op de ISO 27001 norm.
- Het informatieveiligheidsbeleid voldoet aan de minimale normen van de Kruispuntbank Sociale Zekerheid (KSZ) ten aanzien van informatieveiligheid. Ook deze minimale normen zijn gebaseerd op de ISO 27001 norm.



Figuur 1 Schematisch (het informatieveiligheidsbeleid situeert zich op L3)

Merk op dat hoewel DCJM enkel verantwoordelijk is voor het uitwerken en beschrijven van niveau 3 en 4, de organisatie erop moet toezien dat alle vereisten en beperkingen die in de bovenliggende niveaus beschreven staan, worden opgenomen in haar beleid.

Voorbeeld

- L1: De ISO-standaard schrijft voor dat er een vorm van informatieclassificatie moet worden geïmplementeerd.
- L2: Het Stuurorgaan Informatie- en ICT-beleid schrijft een classificatiemodel met bijhorende maatregelen voor.
- L3: Het informatieveiligheidsbeleid van DCJM bepaalt om dit model te volgen en legt de procedure vast om de informatieklasse vast te stellen.
- L4: De documentatie van elke asset beschrijft de informatieklasse en deze informatie wordt opgenomen in het assetregister.

3.1 Opsomming van de toezichthoudende autoriteiten

3.1.1 Gegevensbeschermingsautoriteit

https://www.gegevensbeschermingsautoriteit.be/

3.1.2 VTC

VTC: Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens https://overheid.vlaanderen.be/vlaamse-toezichtcommissie

4 Informatieveiligheidsorganisatie

4.1 Rollen binnen Informatieveiligheid

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

4.1.1 Leidend 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 de Departementsvergadering.

4.1.2 Teamverantwoordelijke IT

De teamverantwoordelijke IT is verantwoordelijk voor het ontwerpen en implementeren van een geïntegreerd pakket aan technische veiligheidsmaatregelen conform de vereisten van het informatieclassificatieraamwerk en de classificatie van de informatie die van toepassing is. De teamverantwoordelijke IT wordt hierin bijgestaan door de CISO en de adviseur-informaticus bij team IT.

4.1.3 Chief/Corporate Information Security Officer (CISO)

De CISO onderhoudt de departementale architectuur en standaarden vanuit de afgesproken (informatieveiligheid-)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.

- Definieert het informatiebeveiligingsbeleid en de informatieveiligheidsstrategie vanuit een op risico gebaseerde benadering. Hierbij houdt hij rekening met een continu veranderend dreigingsbeeld en analyseert daarbij trends en organisatiebehoeften.
- Richt de informatiebeveiligingsorganisatie in, definieert de daarvoor benodigde middelen en wijst ze toe.
- Initieert en coördineert de implementatie van informatiebeveiliging voor de hele organisatie, houdt toezicht vanuit een tweedelijnsrol en rapporteert aan het topkader.
- Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie.
- Wordt door interne en externe belanghebbenden gezien als de deskundige op het gebied van informatiebeveiligingsstrategie.

(bron: De rol van de CISO – Blauwdruk van het profiel)

4.1.4 Informatieveiligheidscel

De informatieveiligheidscel volgt de uitvoering van het informatieveiligheidsbeleid op. De informatieveiligheidscel wordt samengesteld door de Departementsvergadering.

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 in gedrang brengen en genomen maatregelen die van invloed zijn op de informatieveiligheid.

De Algemeen Directeur is de voorzitter van de informatieveiligheidscel.

4.1.5 Functionaris voor gegevensbescherming

De taken en bevoegdheden van de Functionaris voor gegevensbescherming staan beschreven in het "Besluit van de Vlaamse Regering betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische gegevensverkeer"

> *Art. 3.*
>
> *De functionaris voor gegevensbescherming vervult de taken, vermeld in de algemene verordening gegevensbescherming:*

Specifiek met het oog op de veiligheid van de persoonsgegevens die de instantie verwerkt, waarbij hij de functie van functionaris voor gegevensbescherming vervult, en met het oog op de bescherming van de rechten van de personen op wie die gegevens betrekking hebben, is hij ervoor verantwoordelijk:

1° adviezen en aanbevelingen te verstrekken aan de verantwoordelijke voor het dagelijks bestuur binnen de instantie, over alle aspecten op het vlak van de informatieveiligheid;

2° voor de verantwoordelijke voor het dagelijks bestuur binnen de instantie een veiligheidsplan voor een termijn van drie jaar op te stellen, met vermelding van de middelen op jaarbasis die vereist zijn om het plan uit te voeren. Dat plan wordt minstens één keer per jaar met de verantwoordelijke voor het dagelijks bestuur besproken en zo nodig aangepast. Het veiligheidsplan wordt beschouwd als een advies als vermeld in artikel 39, lid 1, a), van de algemene verordening gegevensbescherming;

3° jaarlijks een verslag op te stellen voor de verantwoordelijke voor het dagelijks bestuur binnen de instantie in kwestie.

4° opdrachten uit te voeren die de verantwoordelijke voor het dagelijks bestuur hem binnen de instantie heeft toevertrouwd, als dat zijn onafhankelijkheid niet in het gedrang brengt en als de inhoud en de hoeveelheid van zijn andere opdrachten hem in staat stellen om zijn taken als functionaris voor gegevensbescherming conform de algemene verordening gegevensbescherming te vervullen.

Art. 6.

In het kader van zijn taken bevordert en ziet de functionaris voor de gegevensbescherming toe op de naleving van de voorschriften voor de gegevensbescherming, opgelegd door de algemene verordening gegevensbescherming, de regelgeving over de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens en het beleid van de verwerkingsverantwoordelijke over de bescherming van persoonsgegevens.

De functionaris voor de gegevensbescherming wordt geïnformeerd over eventuele overtredingen van of problemen met de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens binnen de instantie, zodat hij daarover, als dat nodig is of wenselijk is, een advies of aanbeveling kan formuleren. Alle vastgestelde overtredingen worden schriftelijk en uitsluitend aan de verantwoordelijke voor het dagelijks bestuur binnen de instantie meegedeeld. De nodige adviezen worden erbij gevoegd om dergelijke overtredingen in de toekomst te vermijden.

Art. 8.

De functionaris voor gegevensbescherming werkt onder het rechtstreekse functionele gezag van de verantwoordelijke voor het dagelijks bestuur binnen de instantie. Hij werkt nauw samen met de andere diensten binnen de instantie die mee instaan voor de gegevensbescherming.

4.1.6 Verandermanager

De verandermanager volgt de invoering van het informatieclassificatieraamwerk op binnen de eigen entiteit. Het takenpakket bestaat o.m. uit:

- aanspreekpunt zijn voor de implementatie binnen de eigen entiteit;
- verantwoordelijk zijn voor de opvolging van en rapportering over de implementatie van het programma en de in de strategie gestelde doelen binnen de eigen entiteit ;
- overleggen met de werkgroep Informatieveiligheid onder het Stuurorgaan Informatie en ICT;
- informatie uitwisselen over de eigen entiteit die relevant is voor de implementatie;

- ondersteunen van de toepassingseigenaar bij het opstellen van een Informatieclassificatie

4.1.7 De leidinggevenden

De leidinggevenden zien toe op de correcte toepassing van het informatieveiligheidsbeleid. Eventuele tekortkomingen en/of inbreuken worden gemeld aan de CISO of de IT-helpdesk.

4.1.8 Medewerkers

Iedere medewerker is verantwoordelijk voor het zorgvuldig omgaan met informatie conform het Informatieveiligheidsbeleid. Eventuele tekortkomingen en/of inbreuken worden gemeld aan de CISO of de IT-helpdesk.

4.1.9 Team IT

De medewerkers van het Team 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. Voor deze accounts worden bijzonder beheersmaatregelen getroffen waaronder extensieve logging, bijhouden van een logboek, … Deze maatregelen worden uitgewerkt in het ICR onder de minimale maatregelen m.b.t. Priviliged Access Management (PAM).

4.1.10 Externe partijen

Wanneer taken worden uitgevoerd door externe organisaties of consultants worden in een schriftelijke dienstverleningsovereenkomst de belangen van het departement geborgd. Deze dienstverleningsovereenkomst bevat de nodige elementen m.b.t. informatieveiligheid en (indien vereist) wordt bijkomend een NDA (non-disclosure agreement) opgemaakt. Iedere medewerker die een externe partij aanstuurt, ziet erop toe dat de een schriftelijke dienstverleningsovereenkomst als dusdanig wordt ingevuld. In voorkomend geval, dient de externe partij de aangeboden opleiding m.b.t. Informatieveiligheid en omgaan met vertrouwelijke informatie te volgen.

5 Informatieveiligheidsproces

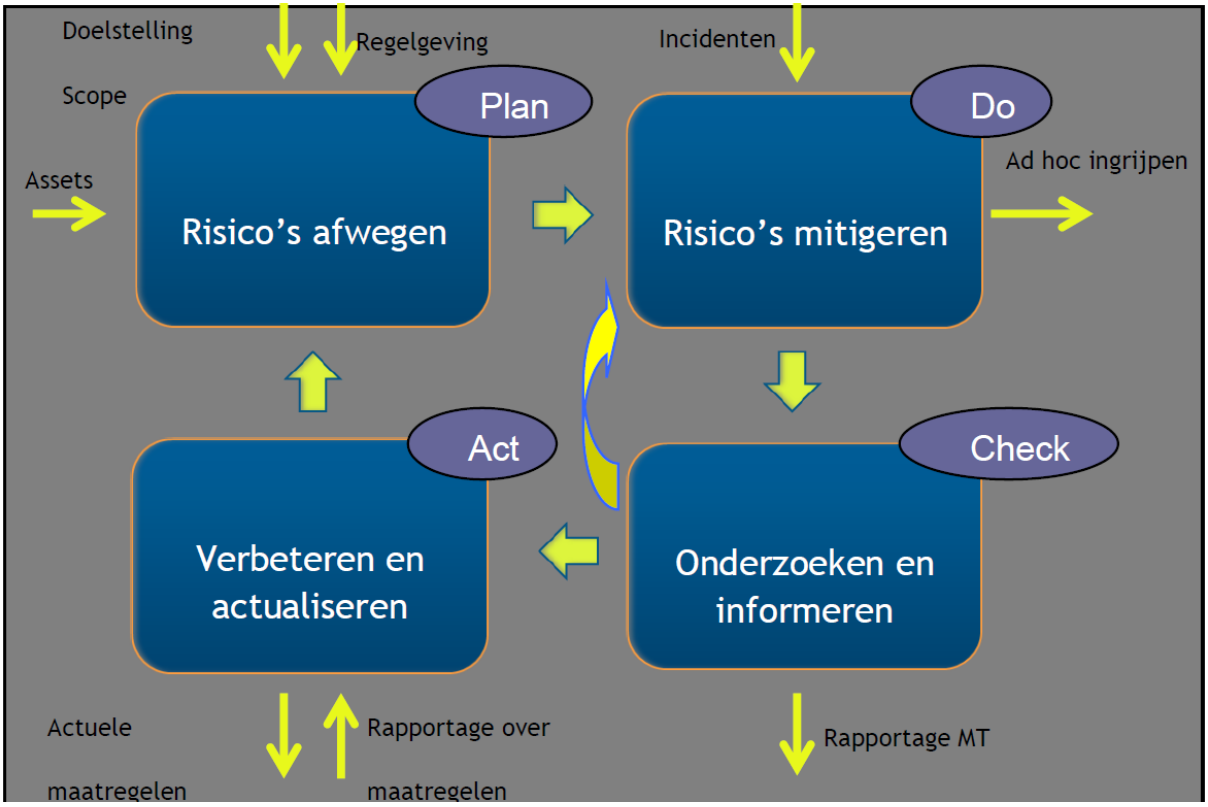
In dit hoofdstuk worden het informatieveiligheidsproces, risicomanagement en het gemeenschappelijk informatieveiligheidsniveau beschreven. Doel van dit hoofdstuk is om inzicht te geven in het proces van informatieveiligheid, de aansturing van dit proces en de samenhang met de bedrijfsprocessen van het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

5.1 Informatieveiligheidsproces (PDCA-cyclus)

Het informatieveiligheidsproces zelf is, in overeenstemming met de ISO 27001 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. Rekening houdend met de VO-context, worden de risico's in kaart gebracht vanuit het VO-brede informatieclassificatieraamwerk (ICR) waarbij maatregelen worden geënt op de Informatieclassificatie. Deze Informatieclassificatie wordt bepaald op het niveau van informatieAssets.

De maatregelen worden uitgewerkt in een 3-jarig actieplan, volgens de beheersaspecten zoals uiteengezet in Annex A van de ISO 27001 norm (zie INFOVEI ControleMaatregelen [in Jira]) .



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 de Departementsvergadering (DV) , omdat daar de verantwoordelijkheid ligt met betrekking tot de informatieveiligheid. De DV duidt voor welke deelaspecten elke organisatorische eenheid (team, programmabureau, projectteam, …) de risicobeheersing uitwerkt. Bijvoorbeeld, voor het deelaspect *digitale dienstverlening* werd het ProgrammaBureau Digitale Dienstverlening (PBDD) aangeduid.

Deze organisatorische eenheden worden daarbij ondersteund door de CISO en de Functionaris voor gegevensbescherming (Data Protection Officer/DPO). Doel van het beveiligingsproces is het inzichtelijk maken van de (rest)risico's voor een bepaald proces, datastroom of informatiesysteem zodat de Departementsvergadering op basis hiervan tot een weloverwogen besluit kan komen.

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.

De organisatorische eenheden rapporteren over de voortgang, actualiteit en de effectiviteit van de maatregelen aan de DV. Vanuit het beveiligingsproces kan hierop worden ingegrepen door verbetervoorstellen in te dienen.

5.3 Raakvlakken

5.3.1 Bedrijfscontinuïteitsbeheer (BCM)

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

Elke organisatie moet voor alle kritieke processen en essentiële informatiesystemen een continuïteitsplan opstellen, waarin activiteiten, maatregelen en belangrijke gegevens van de processen van de organisatie worden beschreven, die tot doel hebben de onderbrekingstijd tot een aanvaardbaar niveau te beperken. DCJM maakt voor elke (bedrijfskritische) toepassing een informatieclassificatie op waarbij de Beschikbaarheid wordt geëvalueerd. De informatieclassificaties worden centraal bijgehouden en regelmatig herzien.

Locatie van de Informatieclassificaties: Informatieveiligheid > 0225 InformatieClassificatieRaamwerk (ICR)

De Bedrijfscontinuïteit die wordt ondersteund door toepassingen, wordt uitvoerig behandeld in Business Continuity Management – partim ICT

5.3.2 Projectmanagement

In projecten wordt, voorafgaand aan de ontwikkeling of aankoop een Informatieclassificatie en een daarbijhorende risicoanalyse opgemaakt.

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.

5.3.3 Incident beheer

DCJM werkt een procedure uit m.b.t. incidentbeheer, deze procedure wordt gepubliceerd op het intranet van DCJM en bevat minimaal:

a) Hoe omgaan met incident (identificeren, indijken, elimineren en herstellen en post-incident activiteiten)
b) Monitoren, detecteren, analyseren en rapporteren van gebeurtenissen en incidenten
c) Loggen van incidenten
d) Hoe omgaan met forensisch bewijsmateriaal
e) Evalueren van en beslissen over gebeurtenissen en welke beslissingen nemen
f) Hoe kwetsbaarheden op vlak van informatieveiligheid en/of privacy evalueren
g) Escaleren van incidenten
h) Hoe vanaf incidenten een normale situatie herstellen
i) Wat, hoe en wie communiceren naar medewerkers van de organisatie en andere belanghebbenden.

Incidenten die een risico vormen voor andere entiteiten binnen de VO worden gemeld Cyber response team van de Vlaamse overheid (Vo-CRT).

5.4 Verwerken van Persoonsgegevens

Een informatieveiligheidsbeleid dient rekening te houden met een correcte verwerking van persoonsgegevens. Het beleid moet voldoen aan de minimale vereisten die worden opgelegd door de Europese wetgeving inzake verwerking van persoonsgegevens. De maatregelen die worden uitgewerkt binnen het informatieveiligheidsbeleid dienen te voldoen aan de minimale technische en organisatorische maatregelen (TOM) die gepaard gaan met de bescherming van persoonsgegevens. Om te bepalen welke deze TOM zijn, kan een Gegevensbeschermingseffectbeoordeling (GEB) worden uitgevoerd. In bepaalde gevallen is de uitvoering van een GEB verplicht. De DPO ondersteunt de toepassingseigenaar bij het uitvoeren van een GEB.

Er zijn 2 richtlijnen om te bepalen of en wanneer een GEB vereist is:

- Artikel 35, lid 3 van AVG

- De lijst van de VTC (https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-dpia)

6 Evaluatie, verantwoording, toetsing, toezicht

6.1 Evaluatie

Het beleid, de betrouwbaarheidseisen en de maatregelen worden op DCJM-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 Rapportering

Het departement werkt actief mee om het Informatieveiligheidsbeleid op de werkvloer uit te rollen en rapporteert hierover, via de verandermanager, aan het Stuurorgaan Informatie en ICT.

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

Wat betreft de verwerking van persoonsgegevens, jaarlijks rapporteert de Functionaris voor gegevensbescherming aan de Informatieveiligheidscel 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 dat zij informatie alleen delen met anderen die deze informatie nodig hebben voor hun werkzaamheden, 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. Iedere medewerker informeert zichzelf (door o.m. het volgen van de aangeboden opleidingen, het volgen van de intranetberichten, deelname aan activiteiten omtrent informatieveiligheid, …) over het Informatieveiligheidsbeleid.

Leidinggevenden zien erop toe dat medewerkers die door hen worden aangestuurd de aangeboden opleidingen volgen, zich informeren over het informatieveiligheidsbeleid. Leidinggevenden doen dit in de eerste plaats door zelf het voorbeeld te geven.

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 intranet bevat de basisinformatie die steeds toegankelijk is voor de medewerkers van het departement en regelmatig geactualiseerd wordt. Informatieveiligheid maakt eveneens een standaard onderdeel uit van de introductieopleiding voor nieuwe medewerkers.

De leidinggevenden verlenen actief hun medewerking aan en ondersteunen deze activiteiten. Daarnaast is de leidinggevende 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.