Federal Information Security Policy Guideline

Handleiding voor informatiecategorisatie

21/11/2019

FISPDOC01 V1.3

Belangrijke opmerking: Dit document is een leidraad die het resultaat is van een samenwerking tussen informatiebeveiligingsexperts van de verschillende federale diensten (FOD, OIP, IPSS). De voorgestelde maatregelen worden beschouwd als minimummaatregelen die redelijkerwijs op een gemeenschappelijke manier van toepassing zijn op alle federale diensten. Deze zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de FISP-werkgroep.

Indien strengere maatregelen vereist zijn voor een federale dienst omwille van reglementaire redenen of om andere formele en dwingende redenen, kan men ervan uitgegaan dat deze maatregelen voorrang hebben op de maatregelen die in deze gids worden beschreven.

FISP Werkgroep

.be

Inhoudstafel

Inhoud van dit document

Oriëntatie van het document

Dit document maakt integraal deel uit van de methodologie voor informatiebeveiliging binnen de Federale overheid (FISP project).

Veiligheidsdoel van het document

De resultaten van informatiecategorisatie hebben een belangrijke contributie t.a.v. verschillende processen die bijdragen in het beheer van informatiebeveiliging (bev. risicobeheer van informatie, de keuze van de serviceprovider voor “cloud”- oplossingen, de ontwikkeling van het actieplan voor informatiebeveiliging,..).

Toepassingsgebied

Het beleid “informatiecategorisatie” is van toepassing op alle niet wettelijk geclassificeerde informatie die door de federale overheid (en haar dienstverleners) wordt geraadpleegd, verwerkt, opgeslagen of gepubliceerd. Alle informatie die geclassificeerd is volgens de Wet van 11/12/1998 valt onder een andere specifieke regelgeving en onder de verantwoordelijkheid van de Nationale Veiligheidsoverheid.

Het betreft zowel informatie die de organisatie zelf aanmaakt of informatie afkomstig van, of bestemd voor andere overheden, burgers, bedrijven, partners en derden.

Concreet gaat het over:

- Informatieverwerking waarvoor de organisatie aansprakelijk of verantwoordelijk is:
    - Informatie van de organisaties binnen de federale overheid
- De maatregelen bij verwerking en gebruiken van informatie binnen de organisatie
    - Informatie van andere overheden, burgers, bedrijven, partners en derden

Het beleid “informatiecategorisatie” omvat enkel het opstellen en onderhouden van het categorisatiemodel en niet de toepassing ervan op de aanwezige informatie binnen de gebruiks- en informatieverwerking van de federale overheid.

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Dit is een richtlijn op basis van de internationale praktijken m.b.t. informatiecategorisatie. Indien u deze richtlijn voor uw organisatie wilt toepassen, moet u eerst een beoordeling maken en controleren of andere wettelijke beperkingen, regels of praktijken van toepassing zijn op uw organisatie. Pas het beveiligingsbeleid aan, in lijn met uw organisatie!

Tijdens de Ministerraad van 3 mei 2019 werd een voorontwerp van wet voorgelegd, namelijk de herziening van de wet van 11/12/1198. Indien deze wet wordt aangenomen, wordt het FISP beleid geüpdatet. Het huidige beleid houdt geen rekening met toekomstige wettelijke ontwikkelingen.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van federale overheid, voor de verwerkers van informatie (ook de onderaannemers van informatiesystemen), de veiligheidsofficier en andere belanghebbenden in verwante gebieden (bev. de documentenbeheerder).

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Inleiding

Federale overheden verwerken veel informatie. Die informatie is gevoelig voor risico's op vlak van beschikbaarheid, integriteit en vertrouwelijkheid. Afhankelijk van de gevoeligheid van informatie, dient informatie beschermd te worden volgens een methodologie om de risico's te beheren. Op deze manier kan men de risico's beperken tot een vooraf bepaald aanvaardbaar beschermingsniveau. Het categorisatie schema geeft een eenvoudige en snelle indicatie van het belang van informatie en is daarmee een basis voor risico inschatting.

Deze categorisatiemethode bevordert bovendien de samenwerking tussen de verschillende organisaties die informatie verwerken voor de federale overheid, andere overheden, bedrijven en de burgers. Beheerders die niet bekend zijn met de inhoud en de waarde van data worden op deze manier geholpen voor het implementeren van de nodige veiligheidsmaatregelen.

Dit document geeft uitleg over het belang en de manier waarop data gecategoriseerd kan worden. Er is bewust voor gekozen om geen gebruik te maken van het woord "classificatie" doorheen dit document om zoveel mogelijk verwarring te vermijden met de officieel geclassificeerde gegevens op basis van de wet van 11/12/1998.[1]

Werkingsprincipe

Algemeen

De organisaties van de Federale overheid zouden de beschermingsniveau van informatie, uitgedrukt in categorisatieniveaus, moeten garanderen volgens een intern categorisatieschema in overeenstemming met de specifieke wetgeving terzake, alsook met de internationale regelgeving.

Als de principes beschreven in de wet- en regelgeving afwijken van de principes van het interne categorisatieschema van de federale organisatie, zal de bindende regel altijd van toepassing zijn. Bovendien zullen, in geval van tegenstrijdigheid, wettelijke of juridische principes altijd voorrecht hebben ten aanzien van de principes van het interne categorisatieschema.

Bij het definiëren van een categorisatie is het "laagste" niveau altijd het beoogde doel, omdat enerzijds een te hoge categorisatie automatisch onnodige kosten en complexiteit van processen genereert en aan de andere kant een te hoog niveau het publiek te veel beperkt tot toegang van informatie. Dit zou uiteraard problemen veroorzaken in de processen van de organisatie.

De componenten van een verwerkingsketen kunnen individueel een ander categorisatieniveau hebben, maar de toepasselijke veiligheidsmaatregelen, zijn gebaseerd op het component met de hoogste classificatie.

Controlemaatregelen moeten worden afgestemd op de risico's, op basis van de technische mogelijkheden en de kosten van de te nemen maatregelen. Dit is afhankelijk van de situatie. Hoe gevoeliger de informatie, hoe groter het risico is. Afhankelijk van de context waarin het wordt gebruikt, des te ingewikkelder de vereisten voor informatiebeveiliging. Globaal genomen, als maatregelen de beveiliging en vertrouwelijkheid verhogen tegen lage extra kosten, kunnen ze als "geschikt" worden beschouwd. Maatregelen om de veiligheid en vertrouwelijkheid te verhogen worden niet langer als "geschikt" beschouwd wanneer de kosten van het mitigeren van risico's onevenredig hoog zijn. Het is noodzakelijk dat risico's en beheersmaatregelen in evenwicht zijn.

[1] Zie voor meer informatie hieromtrent het hoofdstuk "Geclassificeerde informatie".

Elke federale organisatie die informatie verwerkt via informatiesystemen, loopt bepaalde risico's omdat deze informatie- en informatiesystemen worden blootgesteld aan interne en externe bedreigingen en problemen. Het uitvoeren van een risicobeoordeling helpt om de risico's voor informatiesystemen en hun belang te identificeren. Dit bepaalt vervolgens de veiligheidsmaatregelen die moeten worden genomen om de risico's tot een aanvaardbaar niveau te brengen. Het voorgestelde interne categorisatieschema kan daarom worden beschouwd als "een vereenvoudigde vorm van risicobeoordeling".

Rollen en verantwoordelijkheden

Alle categorisatie schema's worden voorgesteld door de informatieveiligheidsconsulent (CISO). Het DPO-team zal CISO ondersteunen in het kader van de verificatie van de naleving van de vereisten van de Europese algemene verordening inzake gegevensbescherming. Het voorgestelde schema zal vervolgens gevalideerd worden door het management van de federale organisatie. Management zal bijgevolg ook de verantwoordelijkheid dragen voor de classificatie en zal deze mededelen aan alle belanghebbenden.

Op basis van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtiging, veiligheidsattesten en veiligheidsadviezen, wordt er ook een veiligheidsofficier aangesteld. Deze veiligheidsofficier zal alles wat onder deze wet valt ondersteunen.[2]

Volgende rollen en verantwoordelijkheden werden vastgelegd op basis van een klassiek RACI-model.

	Verantwoordelijke	**voorstellen**	**Ondersteuning**
Categorisatie schema	Management	Chief Information Security officer (CISO)	Data Protection Officer (DPO)

Toepassen van wetten, regelgeving en internationale standaarden

De principes van de wetten, regelgevingen en internationale standaarden moeten gerespecteerd worden onafhankelijk van het, door de instelling gedefinieerde, interne classificatieschema.[3] Men kan dus afwijken van de interne classificatieregels en de daaraan verbonden veiligheidsmaatregelen om tegemoet te komen aan de wet.

Voor informatie afkomstig uit andere landen of van in België gevestigde internationale instellingen waartoe de instelling toegang heeft, moet de instelling handelen "namens de instantie van oorsprong" ("eigenaar" van de informatie). In voornoemde gevallen moet de instelling in functie van het toegekende classificatieniveau van de betrokken informatie de overeenkomstig voorgeschreven beveiligingsmaatregelen toepassen.

Categorisatie van de door de instelling gecreëerde informatie

De federale organisatie zou alle informatie (evenals de informatiemedia), die niet onder de regelgeving of wetgeving met betrekking tot de classificatie valt, moeten categoriseren.

De niet-gecategoriseerde informatie zal worden beschouwd als "categorie 1" zodat deze informatie zonder obstructie binnen het bedrijf kan circuleren en enkel aan het publiek of aan derden kan worden medegedeeld

[2] Zie voor meer informatie hieromtrent het hoofdstuk "Geclassificeerde gegevens".

[3] O.a. de GDPR, de wet van 11/12/1998,..

door een proces van goedkeuring en communicatie te volgen. Aan contractanten of partners mag gecommuniceerd worden indien de informatie van belang is voor de uitvoering van een opdracht en de beveiliging van de informatie kan worden gegarandeerd.

De categorisatie zal het belang van informatie voor het bedrijf weergeven in termen van bedrijfswaarde, kriticiteit, gevoeligheid (vertrouwelijkheid, integriteit, beschikbaarheid), contractuele, wettelijke en regelgevende vereisten. De informatie zou daarom zodanig moeten worden gecategoriseerd dat deze gedurende zijn hele leven binnen het bedrijf voldoende bescherming geniet. Het zal noodzakelijk zijn om een geheimhoudingsverplichting te koppelen aan alle informatie, behalve deze van “categorie 0”.

Er zal een schema worden opgesteld dat uit verschillende categorisaties bestaat en dat indelingsovereenkomsten en criteria voor de reguliere controle van de classificatie bevat. Dit schema zal consistent moeten zijn in de hele onderneming, zodat iedereen de informatie op dezelfde manier categoriseert en dezelfde doelstellingen en maatregelen heeft op het gebied van informatiebeveiliging.

De categorisatie van informatie zal moet worden uitgevoerd door de eigenaar/houder van de informatie of de persoon die de beheerder is van het bedrijfsonderdeel dat verantwoordelijk is voor de informatie. Deze persoon heeft meestal voldoende kennis van de zakelijke gevolgen in het geval van een mogelijk verlies van beschikbaarheid, integriteit en vertrouwelijkheid van dit actief. De eigenaar/houder kent ook de wet- en regelgeving die onderworpen is, evenals de gevolgen van het overtreden van deze informatie.

Labelen van de informatie

De federale organisaties zouden adequate procedures en registers moeten opstellen, valideren, implementeren, communiceren en onderhouden voor de labeling en verwerking van alle informatieverzamelingen, informatiedragers en informatiesystemen in overeenstemming met het interne categorisatieschema. Het omvat zowel de informatie als de overeenkomstige fysieke en elektronische middelen. Er zou bovendien rekening moeten gehouden worden met het gepast labelen van (met het blote oog onzichtbare) metadata. Het label zal het categorisatieschema moeten reflecteren en dient gerespecteerd te worden voor al de informatie die een categorisatie heeft.

Behandelen van informatiemiddelen

Er zouden procedures moeten worden vastgesteld voor het verwerken, opslaan en communiceren van informatie in overeenstemming met hun categorisatie. De volgende aspecten zou men in overweging moeten nemen bij het omgaan met informatiebedrijfsmiddelen:

- beperking van toegang op basis van het categorisatieniveau en gebaseerd op de principes "Need to know" en "Need to have";
- registratie van geautoriseerde ontvangers van informatiemedia;
- bescherming van tijdelijke of permanente kopieën van informatie tot een niveau dat overeenkomt met het beschermingsniveau van de oorspronkelijke informatie;
- het markeren (labeling) van alle kopieën van de informatiemiddelen voor de geautoriseerde ontvanger(s);
- stockeren van ICT bedrijfsmiddelen in overeenstemming met het categorisatieniveau en/of van de productspecificaties van de leverancier.

Overeenkomsten met andere bedrijven waarmee informatie wordt uitgewisseld, zouden procedures moeten omvatten om de categorisatie van informatie te identificeren en om de labels/categorisatieniveaus van de partners te interpreteren. Zelfs als categorisatienamen uit een categorisatieschema van een andere onderneming identiek zijn aan of vergelijkbaar met die van een organisatie van de federale overheid, betekent dit niet dat de toegekende waarde identiek of vergelijkbaar is.

Categorisatie schema

Het beschermingsniveau van informatie wordt uitgedrukt in categorisatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie (B.I.V.).

B.I.V.

Beschikbaarheid

ISO / IEC 27000: “eigenschap van toegankelijkheid en bruikbaarheid op vraag van een geautoriseerde entiteit”

Integriteit

ISO / IEC 27000: “eigenschap van nauwkeurigheid en volledigheid”

Vertrouwelijkheid

ISO / IEC 27000: “de eigenschap dat informatie niet wordt verspreid of bekendgemaakt aan onbevoegde personen, entiteiten of processen”

Categorisatie model

In de context van deze categorisatie zal de informatie voornamelijk worden gecategoriseerd met betrekking tot het aspect vertrouwelijkheid, zoals weergegeven in de onderstaande tabel. De implementatie van de doelstellingen en beveiligingsmaatregelen houdt echter ook rekening met problemen met betrekking tot gegevensintegriteit en beschikbaarheid.

De categorisatieniveaus geven een snelle indicatie van de gevoeligheden en kritieke toestand van de informatie en geven een duidelijk overzicht van de vereiste beschermingsniveaus. Op basis van het vereiste beschermingsniveau kan bepaald worden welke en hoeveel maatregelen geïmplementeerd zouden moeten worden. Indien de categorisatie bijvoorbeeld hoger is dan “1”, moet men extra maatregelen implementeren.

De informatie wordt gekenmerkt door de volgende parameter:

- het type gegevens: volgens de inhoudelijke domeinen waar het gegeven toe behoort.
- gevoeligheid: dit bepaalt in het algemeen de impact van het verlies of de verspreiding van informatie.

Om het gebruik van informatie te vereenvoudigen krijgt elke categorie een unieke code onder vorm van een cijfer <N>. Bovendien passen we een unieke kleurcode toe om de visuele herkenbaarheid te verbeteren. De federale organisaties kunnen de grafische labels verrijken met een context specifieke betekenis.

Categorie	
	Als gevolg van deze **categorie « 0 »** kan de informatie probleemloos worden verspreid. De verspreiding schaadt de belangen van de organisatie van de federale overheid, een dienst of de werking van een groep werknemers niet. **Bestemming**: externe doelgroepen De specifieke vermelding van deze categorie op de informatiedrager is noodzakelijk. Uitzondering is van toepassing wanneer vanwege de aard van de informatiedrager, deze door iedereen kan worden beschouwd als publiek. (bijv. flyers, openbare websites, enz.)

	Deze informatie kan ook via sociale media worden verspreid.
	**Categorie « 1 »** wordt toegewezen wanneer een onjuist gebruik van informatie: • waarschijnlijk invloed heeft op een belang van een dienst of op het in gevaar brengen van het functioneren van een werknemer of een groep mensen, als onderdeel van hun functie binnen de organisatie; • een impact heeft op de privacyrechten van een beperkte groep (uitgedrukt als een percentage) of individuen. Alle informatie die binnen de organisaties van de federale overheid wordt gebruikt en verspreid, die niet door een andere categorie wordt gemarkeerd, worden automatisch beschouwd als categorie 1. **Bestemming**: interne doelgroepen bestaande uit interne werknemers, externe (via een contract), tijdelijke werknemers,.. Deze informatie kan alleen worden uitgewisseld met externe partijen als het bekende partners betreft en alleen indien nodig voor een project en/of partnerschap. De ondertekening van een vertrouwelijkheidsverklaring (NDA) is ook noodzakelijk. Tijdens het, buiten de organisatie, uitwisselen van informatie van “Categorie 1” moet het categorisatieniveau duidelijk visueel gemarkeerd zijn. De informatie kan uiteraard niet via sociale media worden verspreid.
	**Categorie « 2 »** wordt toegewezen wanneer een niet geëigende aanwending van informatie (bijv. vanwege onvoldoende gegevensbescherming): • een van de belangen van de federale organisatie schaden of de werking van de dienst in gevaar brengt; • invloed heeft op de algemene privacyrechten van een groep personen of kwetsbare personen en/of kinderen. **Bestemming**: informatie is voorbehouden aan een beperkte groep medewerkers van de organisatie van de federale overheid of aan goed gedefinieerde partners. Deze informatie kan worden uitgewisseld wanneer dit nodig is voor het uitvoeren van de taken en de missie. De uitwisseling met partners op basis van hetzelfde principe vereist de goedkeuring van het management (hoger niveau) en pas na ondertekening van een vertrouwelijkheidsverklaring (NDA). Het labelen van de informatie is ten alle tijden noodzakelijk. Tijdens het uitwisselen van informatie (b.v. e-mails) van “Categorie 2” moet ook duidelijk worden gemaakt voor wie deze bestemd is (b.v. TLP). Dit zodat de informatie de gepaste beveiligingsmaatregelen kan blijven ervaren.
	**Categorie « 3 »** wordt toegewezen wanneer een niet geëigende aanwending van informatie: • de essentiële belangen van de federale organisaties ernstig kan schaden;

	• een impact heeft op de specifieke privacyrechten van een groep personen of kwetsbare personen en/of kinderen.[4] De gegevens zijn gecategoriseerd als "3" wanneer ongeautoriseerde openbaarmaking, wijziging of vernietiging van dergelijke gegevens kan resulteren in een aanzienlijk risiconiveau voor de federale organisaties. Voorbeelden van gegevens van categorie 3 zijn gegevens die worden beschermd door federale of Europese regelgeving inzake vertrouwelijkheid en gegevens die worden beschermd door vertrouwelijkheids-overeenkomsten. Het hoogste niveau van beveiligingscontroles moet worden toegepast op deze specifieke gegevens. **Bestemming:** Deze informatie moet worden beschermd tegen ongeoorloofde toegang. Alle informatie is voorbehouden aan een beperkte groep medewerkers van de federale organisaties of aan goed gedefinieerde partners. Gegevens categorie 3 zijn "aankondigingstriggers", dat wil zeggen dat er een automatische kennisgeving is aan de betrokken personen voor ongeautoriseerde toegang. Deze informatie mag alleen worden uitgewisseld door diegenen, die naar behoren zijn, geïdentificeerd door de eigenaar van de gegevens en wanneer dit strikt noodzakelijk is voor de uitvoering van de taken en de missie (moet worden geweten). De uitwisseling met partners op hetzelfde principe vereist goedkeuring naast de richting (hoger niveau) van de eigenaar van de gegevens en alleen na ondertekening van een vertrouwelijkheidsverplichting (NDA). Het labelen van de informatie is ten alle tijden noodzakelijk. Tijdens het uitwisselen van informatie (b.v. e-mails) van “Categorie 3” moet ook duidelijk worden gemaakt voor wie deze bestemd is (b.v. TLP). Dit zodat de informatie de gepaste beveiligingsmaatregelen kan blijven ervaren. De eigenaar van het document moet de doelgroep voor deze informatie in het document vermelden. Elke publicatie van dit soort informatie kan als ernstig wangedrag worden beschouwd.
	**Categorie « 4 »** heeft betrekking op geclassificeerde gegevens op basis van de wet van 11/12/1998.[5] Het bevat de gegevens, het materiaal, de technologieën, ... waarvan kennis of gebruik de werking van België, internationale instellingen of bilaterale/multilaterale/internationale overeenkomsten ernstig in gevaar zou kunnen brengen. Met het oog op de regelgevende en wetgevende samenhang, op zowel Europees als nationaal niveau, is dit categorisatieniveau van toepassing op de federale organisaties. De beveiligingsmaatregelen die op de gegevens moeten worden toegepast, moeten voldoen aan de doelstellingen en maatregelen, opgelegd door de instanties die met de juridische kwalificatie zijn belast. De gegevens van categorie 4 zijn "aankondigingstriggers", dit wilt zeggen dat er automatisch kennisgeving wordt gedaan aan de betrokken personen en instellingen voor een toegangsfout.

[4] Art. 10 en 9 van de A.V.G.

[5] Zie voor meer informatie hieromtrent het hoofdstuk “Geclassificeerde gegevens”.

Geclassificeerde gegevens (Wet van 11/12/1998)[6]

De "classificatie" is het proces waarbij men informatie, documenten of gegevens, materieel, materialen of stoffen, in welke vorm ook, een bepaald beschermingsniveau toekent krachtens de wet of door de verdragen of overeenkomsten die België binden, vnl. in relatie tot de volgende nationale en internationale belangen :

- Onschendbaarheid van het nationaal grondgebied & van de militaire defensieplannen;
- Uitwendige veiligheid van de staat & de internationale betrekkingen van België;
- Wetenschappelijk en economisch potentieel van België;
- Veiligheid van de Belgische onderdanen in het buitenland.

De "Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen" (hierna "Wet van 11/12/1998") bepaalt de criteria voor de classificatie, alsmede de bevoegdheden en verantwoordelijkheden van de functionarissen die gemachtigd zijn om ze te gebruiken. Een classificatieniveau wordt toegekend op basis van de inhoud, nooit volgens de aard van de bestemmeling of de hoogdringendheid. Alleen de overheid van oorsprong is bevoegd om te classificeren, het beschermingsniveau te wijzigen en te declassificeren.

Classificatieniveau's

Er zijn 3 classificatieniveaus naargelang de schade die de niet-geëigende aanwending kan toebrengen aan hoger vermelde belangen:

- Schade = "**Vertrouwelijk**"
- Ernstige schade = "**Geheim**"
- Zeer ernstige schade = "**Zeer Geheim**"

Deze markering moet ook duidelijk zichtbaar zijn op elke pagina van de geclassificeerde documenten, samen met het opschrift "Wet van 11/12/1998". De markering "Beperkte Verspreiding" heeft geen wettelijke bescherming, dit duidt enkel aan dat het om gevoelige informatie gaat die niet buiten de doelgroep mag worden verspreid. In de nabije toekomst gaat er wel een vierde (laagste) classificatie bijkomen, de categorie "Restricted" om tegemoet te kunnen komen aan internationale afspraken, verschillende landen en internationale instellingen (EU, NAVO, etc.) hebben namelijk een wettelijke classificatie op het niveau "Restricted".

De tabel hieronder toont bijvoorbeeld de verschillende classificatieniveaus die worden gebruikt in België, de Europese Unie (EU) en de Noord-Atlantische Verdragsorganisatie (NAVO):

Classificatieniveaus				
Nationaal	Zeer Geheim	Geheim	Vertrouwelijk	(Beperkte verspreiding)
NAVO	Cosmic/Focal Top Secret	NATO Secret	NATO Confidential	NATO Restricted
Europa (UE)	EU Top Secret	EU Secret	EU Confidential	EU Restricted

De veiligheidsmachtiging en enkele basisprincipes

Een persoon die toegang tot de geclassificeerde informatie nodig heeft, moet aan vier criteria voldoen:

[6] Op het moment dat dit beleid gecreëerd is, is een voorontwerp van wet voorgelegd aan de ministerraad. Namelijk de herziening van de wet van 11/12/1198. Indien deze wet wordt aangenomen, wordt het FISP beleid geüpdatet. Het huidige beleid houdt geen rekening met toekomstige wettelijke ontwikkelingen.

1. werken voor een bedrijf of administratie dat is geautoriseerd door de Nationale Veiligheidsoverheid (NVO) of is geregistreerd bij de NVO om geclassificeerde informatie te verwerken;
2. geldige individuele veiligheidsmachtiging op het vereiste niveau;
3. demonstreert een 'noodzaak tot kennisname' (de "need to know");
4. een veiligheidsbriefing ontvangen hebben.

Enkele voorbeelden van de niet-geëigende aanwending van geclassificeerde informatie (gevangenisstraffen en geldboetes):

- Raadplegen in een publieke ruimte;
- Meedelen aan personen zonder geldige veiligheidsmachtiging;
- Reproductie zonder akkoord van de overheid van oorsprong;
- Bewaren buiten een geclassificeerde zone;
- Niet naleven van voorwaarden inzake verzending & vernietiging;
- Elke vorm van aanwending met schending van de veiligheidsregels bepaald door de Wet van 11/12/1998.

De Veiligheidsofficier

Elke organisatie die geclassificeerde informatie behandelt moet een veiligheidsofficier (VO) aanduiden, zie art. 13 Wet van 11/12/1998 : « Het personeelslid, houder van een veiligheidsmachtiging, binnen een rechtspersoon die een veiligheidsmachtiging bezit, dat door de leiding van de rechtspersoon wordt aangewezen om te zorgen voor de inachtneming van de veiligheidsregels. De veiligheidsofficieren komen, in de uitoefening van hun opdrachten, onder de bevoegdheid van de NVO».
De veiligheidsofficier is verantwoordelijk tegenover het bestuur en treedt op als tussenpersoon tussen de eigen organisatie, de NVO en de inlichtingendienst.
Deze persoon heeft als voornaamste verantwoordelijkheden :

- Het waken over de naleving van de veiligheidsregels in de rechtspersoon waarbinnen ze zijn aangewezen (richtlijnen NVO).
- Specifiek opgelegde taken in het kader van de procedure tot aanvraag en toekenning van veiligheidsmachtigingen (zie Wet van 11/12/1998).

Documentbeheer

Historiek

Datum	Auteur	Versie	Omschrijving wijzigingen
23/04/2019	BOSA	V.0.1	Eerste draft
29/04/2019	FISP workgroup	V.0.2	1e update na FISP meeting
24/05/2019	FISP workgroup	V.1.0	2e update op basis van opmerkingen van de FISP WG deelnemers
03/07/2019	FISP workgroup	V.1.2	Verbeterde leesbaarheid
21/11/2019	FISP workgroup	V1.3	Publieke verspreiding

Goedkeuringen

Datum	Approver(s)	Versie
21/11/2019	FISP workgroup	V.1.3

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- Informatieclassificatie Vlaamse overheid
- Wet 11/12/1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.
- Verordening (EU) 2016/679 Van het Europees Parlement en de Raad/ 27 April 2016 (GDPR/AVG)
- KSZ data classificatie
- ISO/IEC 27001/2

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Titel*
FISPDOC08	*Algemeen overzicht voor de informatieveiligheid op federaal niveau*

Positionering van het beleid t.o.v. de ISO 27001-norm

Sectie	***Doelstellingen en referentiemaatregelen***	*In relatie (X = Ja)*
	Context van de organisatie	
	Leiderschap	
	Planning	
	Ondersteuning	
	Operatie	
	Evaluatie van de prestaties	
	Verbeteringen	

Positionering van het beleid t.o.v. de ISO 27002-norm

Sectie	**Doelstellingen en referentiemaatregelen**	In Relatie *(X = Ja)*	Doelstellingen / Maatregelen *(Detail)*
	Informatiebeveiligingsbeleid		
	Organisatie van informatiebeveiliging	*X*	
	Human Resources Veiligheid		
	Asset Management		
	Toegangscontrole		
	Geheimschrift		
	Fysieke en ecologische veiligheid		
	Operationele veiligheid		
	Beveiliging van communicatie		
	Aankoop, ontwikkeling en onderhoud van informatiesystemen		
	Relaties met leveranciers		
	Beheer van informatiebeveiligingsincidenten		
	Informatiebeveiliging in Business Continuity Management		
	Conformiteit		