Federal Information Security Policy Guideline

Globaal overzicht
voor informatiebeveiliging
op federaal niveau

21/11/2019

FISPDOC08 V1.1

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 methodologie voor informatiebeveiliging binnen de Federale overheid (FISP-project).

Veiligheidsdoel van het document

Dit document omschrijft het federale informatiebeveiligingsbeleid.

Toepassingsgebied

Dit beleid voor informatiebeveiliging is toepasselijk voor alle informatie die er circuleert in de federale organisaties.

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Deze informatie mag niet individueel gebruikt worden als referentie documentatie. De lezer van dit document gebruikt dit document niet als vervanger van wetgeving of standaarden, maar als leidraad bij het nemen van de gepaste beveiligingsmaatregen.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent en voor de functionaris voor de gegevensbescherming (FGB of ook wel DPO) van de federale overheidsinstellingen, voor de verwerkers van informatie (ook de onderaannemers van informatiesystemen) en andere belanghebbenden in verwante gebieden (bv. de documentenbeheerder).

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

FISP

FISP (Federal Information Security Policy) is een leidraad voor informatiebeveiliging 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. De adviezen in deze handleiding zijn zodanig opgesteld dat ze voldoende ondersteuning bieden en makkelijk kunnen toegepast worden door de federale instanties.

Het doel van dit beleid is om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen door middel van verschillende adviserende handleidingen. Hierbij is er ook de nodige aandacht voor de identificatie, authenticatie en autorisatie betreffende de toegang tot informatie.

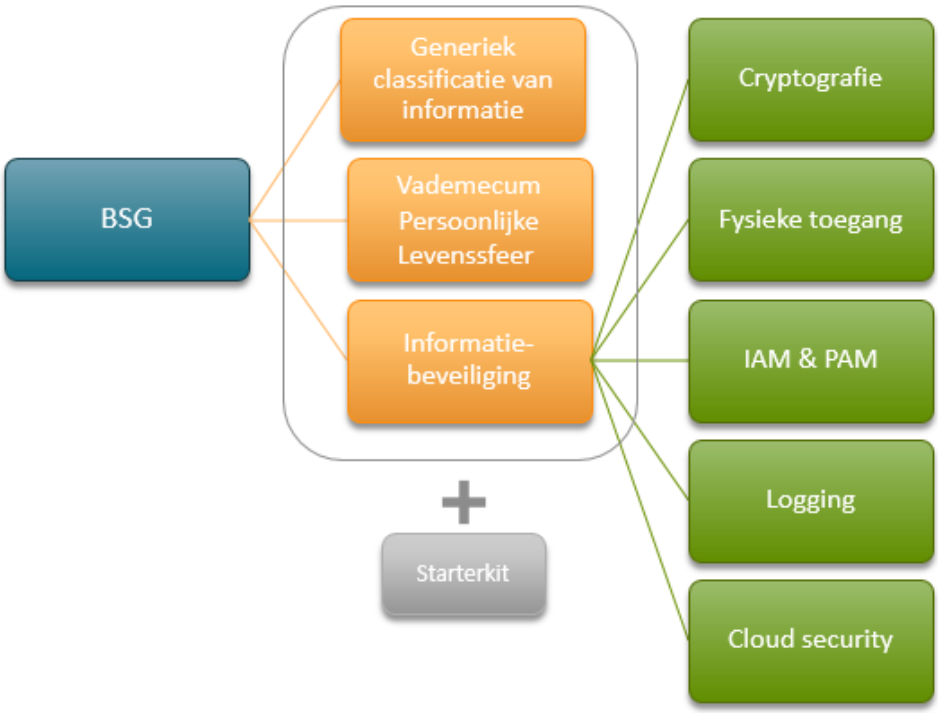
Vervolgens bestaat het informatiebeveiligingsbeleid uit een generieke classificatie van informatie, gekoppeld aan specifieke maatregelen voor elk van deze classificatieniveaus. Bovendien is er ook een vademecum betreffende de bescherming van persoonsgegevens en een starterkit, met enkele globale how-to tips voor het gebruik van de FISP.

Het informatiebeveiligingsbeleid is een aanvulling op de BSG (Baseline information Security Guidelines) geleverd door het Centrum voor Cybersecurity België (CCB) en houdt bovendien ook rekening met bestaande ISO 2700X-normen. Het pakket van voorgestelde maatregelen voor informatiebeveiliging is echter niet compleet, aangezien er beveiligingsobjectieven zijn die nog niet uitvoerig behandeld zijn in deze eerste release van FISP, in vergelijking met de BSG. Het zal aanbevolen zijn om gedurende toekomstige releases van FISP de overige beveiligingsobjectieven te behandelen.

Het is ook belangrijk om te melden dat dit aanbevolen informatiebeveiligingsbeleid, de ondersteuning van het management vereist voor de implementatie in hun specifieke federale organisatie. Informatiebeveiliging maakt immers deel uit van een goed beheer van de organisatie. De betrokkenheid van management bevordert bovendien de ontwikkeling van een veiligheidscultuur en de uitvoering van de voorgestelde beveiligingsmaatregelen.

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.

Organigram van documenten



Beschrijving van de documenten

Naam	*FISP Ref.*	*Inhoud*
Algemeen overzicht voor de informatieveiligheid op federaal niveau	FISPDOC08	Dit is een globaal document dat verwijst naar alle veiligheidsmaatregelen die betrekking hebben op federale informatiebeveiliging.
Handleiding voor informatiecategorisatie	FISPDOC01	Dit document beschrijft hoe de federale organisaties, afhankelijk van de gevoeligheid van informatie, informatie dient te beschermen volgens een methodologie om de risico's te beheren en te beperken tot bepaalde beschermingsniveaus. Deze beschermingsniveaus zijn uitgedrukt in categorisatieniveaus.
Handleiding voor de controle en de beveiliging van de fysieke toegangen	FISPDOC02	Dit document beschrijft de aanbevolen maatregelen om onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van federale organisaties te voorkomen.
Handleiding voor cryptografie	FISPDOC03	Dit document beschrijft de aanbevolen maatregelen met betrekking tot cryptografie. Dit document bevat voldoende informatie om goede (beleid)keuzes te maken en bewustwording te creëren. De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie categorisatie van FISP en met de verschillende data contexten.

Handleiding voor logging en monitoring	FISPDOC04	Dit document beschrijft de aanbevolen maatregelen met betrekking tot logging. De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie categorisatie van FISP. Er wordt bovendien advies gegeven in de maatregelen die men moet nemen voor logbeheer, aanwijzingen over de retentie en beveiliging van audit records, hoe om te gaan met fouten in audit records en audit opvolging, analyse en rapportering.
Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) en de geprivilegieerde toegangen (PAM)	FISPDOC05	In dit document worden de algemene maatregelen met betrekking tot IAM georganiseerd in lijn met de voorgestelde informatie categorisatie van de FISP werkgroep. Een algemene verwijzing naar 'Privileged Access Management' (PAM) komt ook aan bod in dit document.
Handleiding voor de beveiliging in de cloud	FISPDOC06	Dit document beschrijft de bedreigingen, technologische risico's en beveiligingsmaatregelen voor Cloud omgevingen.
Handleiding voor de beveiliging van persoonsgegevens	FISPDOC07	Dit document omschrijft de vereisten om te voldoen aan de informatiebeveiliging zoals vooropgesteld door de Algemene Verordening Gegevensbescherming (AVG). Het bevat bovendien een gestandaardiseerde categorisatie volgens de interpretatie van FISP werkgroep.
Starter kit • **Startgids** • **Glossarium** • **Tabel met rollen- en verantwoordelijkheden (RASCI)**	• FISPDOC09 • FISPDOC10 • FISPDOC11	Dit document is een how-to document voor de verschillende federale overheden, met algemene tips voor de toepassing en implementatie van FISP.

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
22/10/2019	BOSA	V.0.1	Eerste draft
04/11/2019	BOSA	V.02	Update op basis van comments tijdens de FISP meeting
21/11/2019	FISP workgroup	V1.1	Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP FISP workgroup	V.1.1

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- ISO/IEC 27001

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Versie*	*Titel*
		Nihil

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

Sectie	*Doelstellingen en referentiemaatregelen*	*In relatie (X = Ja*
4	*Context van de organisatie*	
5	*Leiderschap*	*x*
6	*Planning*	
7	*Ondersteuning*	
8	*Operatie*	
9	*Evaluatie van de prestaties*	
10	*Verbeteringen*	

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

Sectie	*Doelstellingen en referentiemaatregelen*	*In Relatie (X = Ja)*	*Doelstellingen/ Maatregelen (Detail)*
A5	*Informatiebeveiligingsbeleid*		
A6	*Organisatie van informatiebeveiliging*		
A7	*Human Resources Veiligheid*		
A8	*Asset Management*		
A9	*Toegangscontrole*		
A10	*Geheimschrift*		
A11	*Fysieke en ecologische veiligheid*		
A12	*Operationele veiligheid*		
A13	*Beveiliging van communicatie*		
A14	*Aankoop, ontwikkeling en onderhoud van informatiesystemen*		
A15	*Relaties met leveranciers*		
A16	*Beheer van informatiebeveiligingsincidenten*		
A17	*Informatiebeveiliging in Business Continuity Management*		
A18	*Conformiteit*		