Federal Information Security Policy Guideline

Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) & de geprivilegieerde toegangen (PAM)

21/11/2019

FISPDOC05 V2.1

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 minimum aanbevelingen 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).

Iedere federale organisatie dient te beschikken over een beleid en processen inzake Identity Access Management (IAM).

Veiligheidsdoel van het document

Dit beleid is geschreven om informatiebeveiligingsmaatregelen met betrekking tot Identity Access Management (IAM) aan te reiken, zodat invulling gegeven kan worden aan het beveiligingsbeleid.

Toepassingsgebied

Dit beleid is geen volledige procesbeschrijving voor Identity Access Management (IAM) en bevat geen productbeschrijvingen, maar bevat wel voldoende informatie om goede (beleid)keuzes te maken en bewustwording te creëren met betrekking tot Identity Access Management (IAM).

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Dit is een beleid op basis van de internationale praktijken m.b.t. Identity Access Management (IAM). 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. Het is aangeraden om een afweging te maken per organisatie of de voorgestelde maatregelen technisch haalbaar zijn en of er andere beveiligingsmaatregelen zijn die gebruiksvriendelijker zijn voor uw organisatie. Pas het beveiligingsbeleid aan, in lijn met uw organisatie!

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 (bv. de documentenbeheerder).

Eigenaar

De eigenaar van dit document is de FISP werkgroep.

Inleiding

Identity Access Management (IAM) gaat over identificatie, authenticatie en autorisatie. Er zijn verschillende redenen om aandacht te geven aan Identity & Access management (IAM). Ongeautoriseerde toegang tot kritische informatie, vindt zijn oorsprong vooral binnen de organisatie zelf. Organisaties moeten zich bewust worden dat het gevaar niet zozeer van buiten de organisatie komt maar dus meer vanuit de organisatie zelf. Het is dus aangewezen dat de federale organisaties de nodige beschermingsmaatregelen nemen. Deze beveiligingsmaatregelen dragen ook bij aan het bereiken van efficiënte bedrijfsprocessen, het beheren van kosten en risico's, het ondersteunen/ faciliteren van business en tot slot om te voldoen aan wet- en regelgeving. 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. Privileged Access Management (PAM) zal uw privileged logingegevens beschermen en wordt geïntegreerd met Identity & Access Management (IAM). Op deze manier is uw beveiliging meer compleet.

Voor meer informatie betreffende de 'Federal Authentication Service' (FAS) verwijzen we naar de volgende link:
https://www.gcloud.belgium.be/nl/service/detail/csam

De maatregelen die voorgesteld worden in dit document zijn alleen van toepassing op het toegangsbeheer voor eindgebruikers.

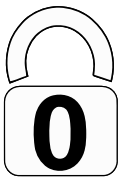
Identity Access Management (IAM)

Informatieclassificatie - IAM

Algemene maatregelen

Zoals in de inleiding aangegeven gaat IAM gaat over identificatie, authenticatie en autorisatie. Voor de regels met betrekking tot identificatie en authenticatie verwijzen we naar de eIDAS uitvoeringsverordening 2015/1502 van 8 september 2015. Deze verordening vermeldt de vereisten voor elk van de betrouwbaarheidsniveaus, laag, subtantieel en hoog.

De FISP werkgroep beveelt vervolgens aan om de maatregelen met betrekking tot IAM te organiseren in lijn met de informatie categorisatie zoals voorgesteld door de FISP werkgroep. De voorgestelde maatregelen zijn gestapelde maatregelen. Dit impliceert dat de maatregelen van de onderliggend informatieklasse ook op de bovenliggende klassen van toepassingen blijven, met uitzondering van onverenigbare technische maatregelen. Bovendien evolueert de complexiteit en sterkte van de maatregelen mee met de stijging van de klasse.

Categorie	
	• **Identificatie & Authenticatie**: Niet vereist • **Autorisatie**: Geen autorisatie vereist

	• **Identificatie & Authenticatie**: laag
	• **Autorisatie**: Autorisatie op basis van technische of organisatorische criteria
	  ○ **Technisch**: Geauthentiseerde gebruikers zonder het lidmaatschap tot een autorisatie rol.
	  ○ **Organisatorisch**: Geauthentiseerde gebruikers met toekenning tot autorisatie rol op basis van het lidmaatschap binnen de organisatie (of een deel ervan).

	• **Identificatie & Authenticatie** : substantieel
	• **Autorisatie**:
	  ○ Autorisatie registratie via toegangsbeheerproces (IDM).
	  ○ Autorisatie op basis van functionele groep, deze functionele groep mag gedeeld worden door meerdere (deel) applicaties.
	  ○ De persoon die de toegang ontvangt mag niet deelnemen aan de validatie van de betrokken autorisatie.

	• **Identificatie & Authenticatie** : Substantieel[1]
	• **Autorisatie**:
	  ○ Autorisatie registratie via toegangsbeheerproces
	  ○ Autorisatie op basis van functionele groep, deze functionele groep mag niet gedeeld worden door meerdere (deel-)applicaties.
	  ○ Validatie:
	  ▪ De persoon die de toegang ontvangt mag niet deelnemen aan de validatie van de betrokken autorisatie.
	  ▪ Validatie met goedkeuring van een door de organisatie geautoriseerd tweede persoon.
	  ○ Jaarlijkse periodieke herziening van de toegangen

	• **Identificatie & Authenticatie**: Hoog
	• **Autorisatie**:
	  ○ Autorisatie registratie via toegangsbeheerproces (IDM)
	  ○ Autorisatie op basis van functionele groep, deze functionele groep mag niet gedeeld worden door meerdere (deel-)applicaties
	  ○ Validatie:
	  ▪ De persoon die de toegang ontvangt mag niet deelnemen aan de validatie van de betrokken autorisatie.
	  ▪ Validatie met goedkeuring van twee door de organisatie geautoriseerd personen, waarvan minimaal één zonder directe hiërarchische of functionele relatie met de persoon die de toegang ontvangt.
	  ○ Jaarlijkse periodieke herziening van de toegangen

Privileged access Management (PAM)

PAM of 'Privileged Access Management' regelt de geprivilegieerde toegang tot systemen en maakt deel uit van het grotere geheel van IAM, monitoring en andere security technologieën. Men mag het niet zien als (één)tool oplossing. Het is echter een verzameling van best practices en technische oplossingen zoals het maken van opleiding voor personeel, functiescheiding, monitoren/logging van het extern systeem beheer of het creëren van een eigen account van systeemadministrator zodat er geen link is met andere fysieke personen. Specifiek voor geprivilegieerde accounts kan dit zijn dat ieder systeem een eigen complex wachtwoord heeft of dat er een policy is om wachtwoorden op een regelmatige wijze te veranderen.[2]

[1] Indien het voor de organisatie niet mogelijk is om tegemoet te komen aan de geïdentificeerde risico's, met het huidige niveau 'substantieel' voor de identificatie en authenticatie, is het aangeraden om niveau 'hoog' toe te passen.

[2] https://www.smalsresearch.be/download/research_reports/management_summary/Privileged%20Account%20Management%20(PAM).pdf

Documentbeheer

Historiek

Datum	*Auteur*	*ersie*	*Omschrijving wijzigingen*
18/07/2019	BOSA	V0.1	Eerst draft
23/08/2019	BOSA	V0.2	Fusie IAM en PAM Gebruik van uitvoeringsverordening 2015/1502
30/08/2019	BOSA	V1.0	Vertaling naar Frans
18/09/2019	BOSA	V1.1	Toevoeging link met FAS Link in source toegevoegd Identificatie en Authenticatie op hetzelfde niveau gebracht Categorie 3 en 4 aangepast naar level “Hoog”
7/10/2019	BOSA	V2.0	De vrijwaring is aangepast Categorie 3 aangepast naar substantieel met verwijzing naar voetnoot (n.a.v. de FISP WG)
21/11/2019	FISP Workgroup	V2.1	Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP Workgroup	V2.1

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- Vo Informatieclassificatie – Minimale maatregelen – IAM https://overheid.vlaanderen.be/sites/default/files/media/Digitale%20overheid/Stuurorgaan%20VIIB/20180703_6_63b_SVIIB_Bijlage_Informatieclassificatie_1.pdf
- ISO/IEC 27002 https://www.iso.org/standard/54533.html
- https://www.smalsresearch.be/download/research_reports/management_summary/Privileged%20Account%20Management%20(PAM).pdf
- UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32014R0910&from=NL)

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Titel*
FISPDOC01	*Handleiding voor informatiecategorisatie*

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		
	Human Resources Veiligheid		
	Asset Management		
	Toegangscontrole	*x*	
	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		