Federal Information Security Policy Guideline

Guide pour la sécurisation et la gestion des identités et des accès de base (IAM) & des accès privilégiés (PAM)

21/11/2019

FISPDOC05 V2.1

Remarque importante : Ce document est un guide qui est le résultat d'une collaboration entre des experts en sécurité des informations appartenant aux différents services fédéraux (SPF, OIP, IPSS). Les mesures proposées sont considérées comme recommandations minimales raisonnablement applicables à tous les services fédéraux de manière commune. Elles sont basées sur des normes internationales, des bonnes pratiques en matière de sécurité de l'information et les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont requises pour un service fédéral pour des raisons réglementaires ou pour d'autres raisons formelles et contraignantes, on peut supposer que ces mesures aient la priorité sur les mesures décrites dans ce guide.

FISP Groupe de travail

.be

Table des matières

Contenu de ce document

Orientation du document

Ce document fait partie intégrante de la méthodologie de la sécurité des informations au sein de l'administration fédérale (projet FISP).

Chaque organisation fédérale doit disposer d'une stratégie et de processus concernant Identity & Access Management (IAM).

Objectif de sécurité du document

La présente stratégie est conçue pour fournir des mesures de sécurité des informations concernant Identity & Access Management (IAM) , afin de concrétiser la stratégie de sécurité.

Champ d'application

La présente stratégie n'est pas une description complète du processus concernant Identity & Access Management (IAM) et ne contient pas de descriptions de produits, mais contient suffisamment d'informations permettant de faire de bons choix (stratégiques) et de sensibiliser en ce qui concerne Identity & Access Management (IAM).

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Il s'agit d'une stratégie basée sur les pratiques internationales concernant Identity & Access Management (IAM). Si vous souhaitez appliquer cette directive à votre organisation, vous devez d'abord effectuer une évaluation et vérifier si d'autres restrictions, règles ou pratiques légales s'appliquent à votre organisation. Il est recommandé que vous examiniez pour chaque organisation si les mesures proposées sont techniquement réalisables et s'il existe d'autres mesures de sécurité qui sont plus conviviales pour votre organisation. Adaptez la stratégie de sécurité, en phase avec votre organisation !

Responsabilités

Ce document est destiné au consultant en sécurité des informations (CISO) et au responsable de la protection des données (DPO) de l'institution publique fédérale, aux responsables du traitement de l'information (y compris les sous-traitants de systèmes d'information), au responsable de la sécurité et aux autres parties prenantes dans les domaines connexes (p.ex. le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est le propriétaire de ce document.

Introduction

Identity & Access Management (IAM) concerne l'identification, l'authentification et l'autorisation. Il y a plusieurs raisons d'attirer l'attention sur Identity & Access management (IAM). L'accès non autorisé à des informations critiques provient principalement de l'organisation elle-même. Les organisations doivent prendre conscience que le danger ne vient pas tant de l'extérieur de l'organisation, mais plutôt de l'intérieur même de l'organisation. Il convient donc que les organisations fédérales prennent les mesures de protection nécessaires. Ces mesures de sécurité contribuent également à atteindre des processus d'entreprise efficaces, à gérer les dépenses et les risques, à soutenir/faciliter le business et enfin à respecter la législation et la réglementation. Dans le présent document, les mesures générales concernant IAM sont organisées conformément à la catégorisation proposée des informations par le groupe de travail FISP.

Une référence générale à Privileged Access Management (PAM) sera également abordée dans ce document. Privileged Access Management (PAM) protégera vos données de connexion privilégiées et est intégré à Identity & Access Management (IAM). De cette façon, votre sécurité est plus complète.

Pour le lien avec le Federal Authentication Service (FAS), nous renvoyons au :
https://www.gcloud.belgium.be/fr/service/detail/csam.

Les mesures proposées dans ce document s'appliquent uniquement à la gestion d'accès pour les utilisateurs finaux.

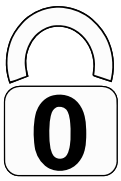
Identity & Access Management (IAM)

Classification des informations - IAM

Mesures générales

Comme indiqué dans l'introduction, IAM concerne l'identification, l'authentification et l'autorisation. Pour les règles relatives à l'identification et à l'authentification, nous renvoyons au règlement d'exécution eIDAS 2015/1502 du 8 septembre 2015. Ce règlement établit les exigences pour chacun des niveaux de sécurité : faible, substantielle et élevée.

Le groupe de travail FISP recommande ensuite d'organiser les mesures concernant IAM conformément à la catégorisation des informations proposée par le groupe de travail FISP.Les mesures proposées sont des mesures cumulées. Cela implique que les mesures de la classe d'informations sous-jacente restent également applicables aux classes supérieures, à l'exception des mesures techniques incompatibles. Par ailleurs, la complexité et la rigueur des mesures évoluent avec le niveau de la classe.

Catégorie	
	• **Identification & Authentification** : aucune requise • **Autorisation** : Aucune autorisation requise

	• **Identification & Authentification** : faible
	• **Autorisation** : Autorisation sur la base de critères techniques ou organisationnels
	  ○ **Technique** : Utilisateurs authentifiés sans appartenance à un rôle d'autorisation.
	  ○ **Organisationnel** : Utilisateurs authentifiés avec attribution à un rôle d'autorisation en fonction de l'appartenance au sein de l'organisation (ou à une partie de celle-ci).

	• **Identification & Authentification** : substantielle
	• **Autorisation** :
	  ○ Enregistrement de l'autorisation via le processus de gestion d'accès (IDM).
	  ○ Autorisation sur la base du groupe fonctionnel. Ce groupe fonctionnel peut être partagé par plusieurs (sous-)applications.
	  ○ La personne à qui l'accès est attribué ne peut pas participer à la validation de l'autorisation concernée.

	• **Identification & Authentification** : substantielle[1]
	• **Autorisation** :
	  ○ Enregistrement de l'autorisation via le processus de gestion d'accès (IDM).
	  ○ Autorisation sur la base du groupe fonctionnel. Ce groupe fonctionnel ne peut pas être partagé par plusieurs (sous-)applications.
	  ○ Validation :
	  ▪ La personne à qui l'accès est attribué ne peut pas participer à la validation de l'autorisation concernée.
	  ▪ Validation avec approbation d'une deuxième personne autorisée par l'organisation.
	  ○ Révision périodique annuelle des accès.

	• **Identification & Authentification** : élevée
	• **Autorisation** :
	  ○ Enregistrement de l'autorisation via le processus de gestion d'accès (IDM).
	  ○ Autorisation sur la base du groupe fonctionnel. Ce groupe fonctionnel ne peut pas être partagé par plusieurs (sous-)applications.
	  ○ Validation :
	  ▪ La personne à qui l'accès est attribué ne peut pas participer à la validation de l'autorisation concernée.
	  ▪ Validation avec approbation de deux personnes autorisées par l'organisation, dont au moins une n'a pas de relation hiérarchique ou fonctionnelle directe avec la personne à qui l'accès est attribué.
	  ○ Révision périodique annuelle des accès.

Privileged Access Management (PAM)

PAM ou Privileged Access Management règle l'accès privilégié aux systèmes et fait partie de l'ensemble plus vaste des technologies IAM, de monitoring et d'autres technologies de sécurité. On ne devrait pas considérer PAM comme (une) solution-outil. Il s'agit en effet d'un ensemble de meilleures pratiques et de solutions techniques, telles que la formation du personnel, la séparation des fonctions, le monitoring/logging de la gestion du système externe ou la création d'un compte personnel pour l'administrateur systèmes afin d'éviter tout lien avec d'autres personnes physiques. Spécifiquement pour les comptes privilégiés, cela peut impliquer que chaque système possède son propre mot de passe complexe ou qu'il existe une stratégie obligatoire de modifier les mots de passe de manière régulière.[2]

[1] S'il n'est pas possible pour l'organisation de répondre aux risques identifiés, avec le niveau actuel " substantiel " pour l'identification et l'authentification, il est recommandé d'appliquer le niveau " élevée ".

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

Gestion documentaire

Historique

Date	·ur		Description des modifications
18/07/2019	BOSA	V0.1	Première version
23/08/2019	BOSA	V0.2	Fusion IAM et PAM Utilisation du règlement d'exécution 2015/1502
30/08/2019	BOSA	V1.0	Traduction
18/09/2019	BOSA	V1.1	Lien d'ajout avec FAS Ajout d'un lien dans les sources L'identification et l'authentification au même niveau Catégorie 3 et 4 ajustées au niveau "High"
7/10/2019	BOSA	V2.0	Adaption de garantie Catégorie 3 adaptée au substantiel avec renvoi à la note de bas de page (à la suite du groupe de travail FISP)
21/11/2019	FISP Workgroup	V2.1	Distribution publique

Approbations

Date	Approbateur(s)	Version
21/11/2019	FISP Workgroup	V2.1

Sources

Ce document a été composé à l'aide des sources suivantes :

- Vo Classification des informations - Mesures minimales - 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
- Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32015R1502)

Lien avec une autre stratégie

Dépendance de documents internes

Réf.	*Titre*
FISPDOC01	*Guide pour la catégorisation des informations*

Positionnement de la stratégie par rapport à la norme ISO 27001

Section	***Objectifs et mesures de référence***	*En relation (X = Oui)*
	Contexte de l'organisation	
	Leadership	
	Planning	
	Appui	
	Opération	
	Évaluation des prestations	
	Améliorations	

Positionnement de la stratégie par rapport à la norme ISO 27002

Section	**Objectifs et mesures de référence**	En relation *(X = Oui)*	Objectifs / Mesures *(détail)*
	Stratégie de sécurité des informations		
	Organisation de la sécurité des informations		
	Sécurité des ressources humaines		
	Asset Management		
	Contrôle d'accès	*x*	
	Code		
	Sécurité physique et écologique		
	Sécurité opérationnelle		
	Sécurité de la communication		
	Achat, développement et maintenance de systèmes d'information		
	Relations avec les fournisseurs		
	Gestion des incidents de sécurité des informations		
	Sécurité des informations dans Business Continuity Management		
	Conformité		