Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales OFAS
Etat-major de direction DS - IT-Management ITM

Communication eGov n° 053 du 17 décembre 2024

A adresser à : - Organes d'exécution du 1er pilier/AFam
- - Pools informatiques

Objet : - Adaptations des directives D-SIPD et DASP
- Obligation de signaler les cyberincidents et les atteintes aux systèmes d'information

1 Adaptation des directives D-SIPD et DASP

Aucune exigence n'a été modifiée de manière substantielle dans les instructions D-SIPD. Leur rédaction a toutefois été revue de manière à les rendre plus claires et plus compréhensibles. Ces adaptations ont été mises en œuvre en étroite collaboration avec le groupe d'exploitation BEWIA[1] . Entre autres, la validité des rapports d'audit selon ISO 27001 et ISAE 3000 a été redéfinie et les annexes ont été mises à jour dans la D-SIPD. En outre, le nouveau processus de déclaration des cyberincidents a été modélisé selon la norme BPMN .[2]

En ce qui concerne l'utilisation de M365 et le stockage et le traitement de données sensibles chez un fournisseur de services informatiques en nuage, il n'est pas encore possible de faire une nouvelle déclaration, car le sujet n'a pas encore été traité de manière définitive au sein de l'OFAS. Les principes de l'administration fédérale en matière de cloud computing s'appliquent donc comme jusqu'à présent dans la D-SIPD. Au cours du premier trimestre 2025, l'OFAS publiera une information actualisée sur le thème M365 et les clouds publics.

Aperçu des principaux changements :

D-SIPD Directives sur les exigences en matière de sécurité de l'information et de protection des données des systèmes d'information des organes d'exécution du 1er pilier/AFam	• Mapping des exigences sur la norme ISO 27001:2022 (la version en vigueur du 1.1.2024 était basée sur ISO 27001:2013). • Validité des rapports d'audit ISO et ISAE redéfinie en tant que chiffre marginal 1.6. • Répartition du chiffre marginal 2.15 : - 2.15.1 Contrats avec des tiers (en général) - 2.15.2 Principes de cloud computing de l'administration fédérale • Ajout d'un nouveau "Processus de notification des incidents de sécurité" en annexe 2.

[1] BEWIA : Groupe d'exploitation en charge des directives D-SIPD et DASP
[2] BPMN : Business Process Model and Notation (modèle et notation des processus d'entreprise)

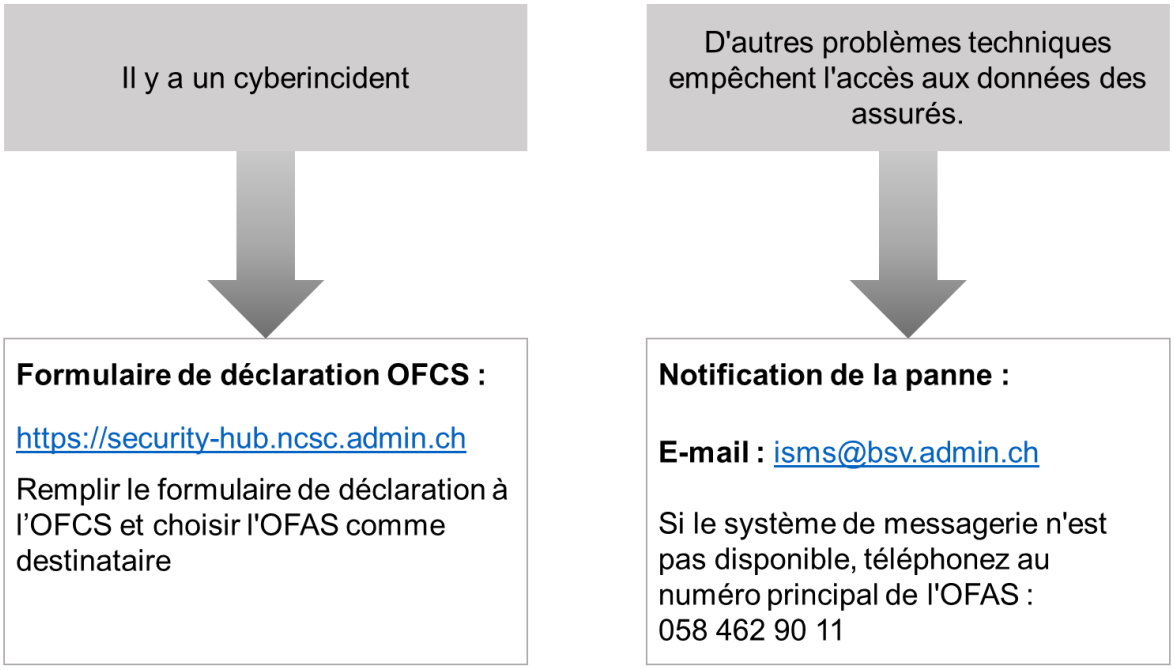
	• Documentation de base SIPD (annexe 3) concernant l'analyse des besoins de protection avec diagramme complété et un exemple de groupes de protection ajouté. • Ajout d'une compilation des exigences relatives aux rôles des organismes d'exécution (annexe 5). • Ajout de liens vers des outils et des modèles (annexe 6)
DASP Directives concernant les audits sur la sécurité de l'information et la protection des données	• Chapitre 2.2 Organismes audités, ajout du chiffre marginal 7 : validité des rapports d'audit ISAE • Chapitre 2.5, chiffre marginal 14 : description du champ d'application de l'audit informatique sur présentation d'un rapport d'audit ISO 27001 / ISAE valable. • Annexe 2 : Questionnaire audit informatique : mapping sur la norme ISO 27001:2022 modifié.

2 Obligation d'annoncer les atteintes au système (Cm 2.3 D-SIPD)

Selon le chiffre marginal 2.3 D-SIPD, les organes d'exécution doivent disposer d'un processus de traitement des incidents liés à la sécurité de l'information. L'obligation d'annoncer selon l'article 141^{septies} du règlement sur l'assurance-vieillesse et survivants (RAVS) s'applique à tous les organes d'exécution du 1er pilier. Il est du devoir de l'OFAS, en tant qu'autorité de surveillance matérielle, d'être informé si les tâches légales peuvent être remplies correctement par les organes d'exécution. Selon la loi sur la sécurité de l'information (LSI), les systèmes d'information des organes d'exécution font partie des infrastructures critiques. Par conséquent, les cyberincidents doivent également être signalés à l'Office fédéral de la cybersécurité (OFCS). La notification d'un cyberincident se fait à l'aide du même formulaire que les notifications à l'OFAS. S'il existe d'autres motifs de perturbation technique (pas de cyberincident) qui entravent ou empêchent l'accès aux données des assurés, ceux-ci doivent être signalés immédiatement à l'OFAS par un canal direct (voir section 3 : "Annonce des perturbations du système en un coup d'œil"). L'OFAS peut ainsi soutenir les organes d'exécution si les assurés s'adressent directement à l'OFAS.

- Selon l'OFCS, le nouveau formulaire de notification des cyberincidents sera disponible à partir du 1er avril 2025 via le "Cyber Security Hub" (https://security-hub.ncsc.admin.ch).
- L'OFAS informera dès que le formulaire sera disponible auprès de l'OFCS. D'ici là, les déclarations à l'OFAS doivent être envoyées par e-mail à isms@bsv.admin.ch.

3 Signaler les perturbations du système en un coup d'œil



Nous vous remercions d'en prendre connaissance.

Secteur État-major de direction – IT Management