Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales OFAS

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 / des allocations familiales (D-SIPD)

Valable à partir du 1er janvier 2024

État au 20 Avril 2026

Remarque

Les annexes au D-SIPD qui ne sont pas pertinentes pour les directives sont répertoriées dans un document séparé, site web de l'OFAS consacré à l'application des assurances sociales, rubrique « eGov/Modèles ») et ne font pas partie des directives. Elles servent à approfondir les connaissances techniques, à illustrer et à soutenir la mise en oeuvre. Seules les directives D-SIPD et leurs annexes pertinentes sont contraignantes.

318.108.08 f D-SIPD

01.24

Suivi des modifications

VERSION	DATE	AUTEUR	REMARQUES
1.0	01.01.2024	OFAS	Version publiée
1.1	15.03.2024	Markus Moog (BSV)	Modifications de la mise en page/formatage
1.2	avril 2024	Michael Jeitziner (IG)	Création du suivi des modifications, mapping contrôle de la norme ISO/IEC 27001:2022, adaptation ch. 2.8.2
1.3	18.04.2024	Markus Moog (BSV) Michael Jeitziner (IG)	Insertion de la table des matières et du n° d'enregistrement. Ajout du texte du ch. 2.14
1.4	24.04.2024	Markus Moog (BSV)	Formatage, suppression de la note de bas de page 6, suppression de l'annexe 3 sur la sécurité de l'information, insertion du tableau d'aide et lien vers les téléchargements
1.5	30.04.2024	Markus Moog (BSV)	Renvois aux ch. et annexes, insertion et lien du tableau d'aide et des modèles
1.6	31.05.2024	Markus Moog (BSV)	Modification du titre 2.13, description des rôles (annexe 5)
1.7	30.07.2024	Markus Burri (BSV) Markus Moog (BSV)	Annexe 3 (nouveau) : analyse des besoins de protection et protection IT de base ; annexe 2 : insertion du nouveau processus d'annonce
1.8	04.11.2024	Markus Moog (BSV)	1.6 : insertion de la validité et du traitement des rapports d'audit selon ISO 27001 et ISAE, insertion du nouveau graphique du processus d'annonce, modification des liens d'aide et des modèles
1.9	11.11.2024	Markus Moog Markus Burri	Annexe 2 : insertion du nouveau processus d'annonce modélisé selon BPMN et d'exemples pour les groupes de protection et attributions (annexe 3), saisie commentaire sur la décision du comité de direction de l'OFAS concernant les services *cloud*, révision de l'ensemble du document
1.9.1	14.11.2024	Markus Moog Markus Burri	2.10.1 : reformulation de l'exemple 2.15.1 : compléter la description, explication que des tiers peuvent être des fournisseurs IT ou d'autres prestataires de services
1.9.2	15.11.2024	Markus Moog Markus Burri	Mise à jour de la description des services *cloud* et de l'avant-propos
2.0	17.12.2024	Markus Moog Markus Burri	Version finale Adoption par la CoCo eGov le 16.12.2024
2.1	24.03.2025	Markus Moog Markus Burri	Précision concernant l'utilisation de Microsoft 365
2.2	12.12.2025	Markus Moog Markus Burri	Adaption et Précision de ch. 2.4, 2.8.2, 2.15.1 Adaptation des annexes 2, 3, 4 et 5
2.3	20.04.2026	Markus Moog Markus Burri	Suppression des annexes (transfert dans un document séparé : eGov/Modèles « Annexes complémentaires D-SIPD »), ajout d'une précision relative à l'externalisation d'objets de protection (ch. 2.17), adaptation de la description des rôles (annexe 2)

Avant-propos

Les présentes directives s'adressent aux organes d'exécution du 1er pilier / des allocations familiales. Elles sont publiées dans la perspective de la révision de la loi sur l'AVS, qui entrera en vigueur le 1er janvier 2024. La surveillance de l'AVS, qui n'avait pratiquement pas changé depuis 1948, sera à l'avenir davantage axée sur les risques. La gouvernance sera renforcée, et les systèmes d'information du 1er pilier seront pilotés de manière adéquate.

À l'automne 2017, le Conseil fédéral avait adopté un projet de révision totale de la loi sur la protection des données. La nouvelle loi reflète l'évolution de la technologie et de la société et renforce les droits que les personnes concernées ont sur leurs données personnelles. Les présentes directives tiennent donc également compte de la loi révisée sur la protection des données et des dispositions d'exécution de la nouvelle ordonnance, qui sont entrées en vigueur le 1er septembre 2023.

Les recommandations du 1er janvier 2022 ont déjà permis aux organes d'exécution de se préparer de manière optimale aux directives de l'OFAS sur les exigences en matière de sécurité de l'information et de protection des données (SIPD). À cette fin, les représentants informatiques des organes d'exécution (projet eAVS/AI Information Security) ont été étroitement associés à l'élaboration des directives.

Les thèmes suivants ont été pris en compte pour le réexamen des recommandations :

- **Documentation de base et élargie de la SIPD** (ch. 2.8.2 et 2.8.3 ou annexes 3 et 4) **:** la compatibilité des exigences avec la nouvelle ordonnance sur la protection des données (OPDo) a été vérifiée.
- **Mandat de tiers / sous-traitance** (ch. 2.15, 2e élément) **:** l'intervention de sous-traitants (art. 9, al. 3, LPD) requiert l'approbation du mandant.
- **Sous-traitant à l'étranger** (ch. 2.15, 3e élément, et annexe 3, let. E) : selon cette recommandation, les données devraient normalement être conservées en Suisse ; les prestations de service pour l'exploitation doivent également être fournies en Suisse, et les exceptions doivent être justifiées. Le traitement de données personnelles par un sous-traitant à l'étranger entraîne une communication de données à l'étranger ; des dispositions complexes de la LPD s'appliquent dans ce cas. L'intervention d'un tiers en tant que sous-traitant à l'étranger est très complexe. Elle requiert de nombreuses clarifications juridiques dans le cas des pays pour lesquels le Conseil fédéral n'a pas déterminé qu'ils garantissent un niveau de protection adéquat au sens de l'art. 16, al. 1, LPD. Le ch. 2.15 contient un renvoi aux restrictions prévues par la LPD, qui doit en fin de compte s'appliquer à tous les organes d'exécution (aucune exception n'est prévue pour les services cantonaux). Des données personnelles ne peuvent être communiquées à l'étranger que si un code de conduite ou une certification garantit un niveau de protection approprié (art. 12, al. 1, OPDo).
- **Services cloud de tiers avec conservation des données en Suisse** Depuis la publication du communiqué eGov 043[1] au début de l'année 2022, plusieurs développements ont eu lieu. Le 15 septembre 2024, le Conseil fédéral a adopté une modification de l'ordonnance sur la protection des données (annexe[2]), dans le cadre du Swiss-U.S. Data Privacy Framework[3] . De plus, les risques liés au «Foreign Lawful Access» (accès aux données par des autorités étrangères, notamment le «CLOUD Act») ont été réévalués. Dans ce contexte, l'OFAS a évalué si l'utilisation de M365 répondait aux exigences de la D-SIPD en matière de traitement et de stockage de données particulièrement sensibles.

Les organes d'exécution sont responsables de la protection de leurs données, néanmoins ils doivent procéder aux évaluations des risques requises par la présente directive (voir ch. 2.15.2).

[1] Communication eGov n° 043 du 01.01.2022

[2] Complément à l'annexe 1 du DSV

[3] Communiqué de presse sur le Swiss-U.S. Data Privacy Framework

Table des matières

Exigences SIPD

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
	1 Objectif, but, objet, principes, champ d'application et références dans le système juridique		
1.1	**1.1 Objectif, but et objet** Compte tenu de la modification de la loi fédérale sur l'assurance-vieillesse et survivants, de la modernisation de la surveillance dans le 1er pilier et de l'optimisation dans le 2e pilier de la prévoyance vieillesse, survivants et invalidité, l'OFAS demande aux organes d'exécution de tenir compte en permanence, dans leurs systèmes d'information, des nouvelles conditions générales décrites ci-après. Un objectif essentiel de la révision de la loi est que les systèmes d'information du 1er pilier disposent de la stabilité et de la capacité d'adaptation nécessaires et qu'ils garantissent la sécurité de l'information et la protection des données. Il est de la responsabilité des organes d'exécution de garantir la réalisation de ces objectifs (cf. art. 49*a*, al. 2, LAVS). La mise en œuvre exacte en termes de portée et de taille de l'organisation SGSI dépend notamment aussi de l'évaluation des risques et de la gouvernance des organes de mise en œuvre. En ce qui concerne la sécurité de l'information et la protection des données, les organes d'exécution doivent en outre satisfaire aux exigences fixées par l'OFAS (art. 49*a*, al. 3, LAVS). Ils doivent les respecter dans la mesure où elles relèvent de leur champ d'application (cf. ch. 1.2). Les présentes directives donnent un aperçu des exigences relatives aux systèmes d'information pour la sécurité de l'information et la protection des données (art. 49*a*, al. 3, en relation avec l'art. 72*a*, al. 2, let. b, LAVS) que doivent respecter les organes d'exécution (tous les chiffres du chap. 2).		
1.2	**1.2 Champ d'application** Les présentes directives relatives aux exigences visées au ch. 2 s'adressent à tous les organes d'exécution de l'AVS, de l'AI, du régime des APG et des PC (cf. art. 66, al. 1, let. a, LAI ; art. 21, al. 2, LAPG ; art. 26, al. 1, let. a, LPC), ainsi qu'à toutes les agences visées à l'art. 65 LAVS. Elles s'appliquent également à l'exécution des allocations familiales (art. 25, let. a, en relation avec l'art. 27, al. 3, LAFam ; art. 25 LFA).		

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
1.3	**1.3 Définition d'un système d'information (SI)** Un système d'information est un outil pour le traitement des données, la communication des données et le profilage (au sens de la LPD) aux fins de l'exécution des tâches[4]. Il contient des éléments techniques et organisationnels. Ces tâches comprennent notamment : - des éléments techniques : matériel informatique, logiciels et composants du réseau ; - de l'application et des volumes de données ; - des éléments organisationnels : processus, tâches, compétences et responsabilités en matière de développement et d'exploitation. Un système d'information est toujours un bien devant faire l'objet d'une protection adéquate. Il s'agit donc d'un objet à protéger (voir ch 2.8).	A.5.9	
1.4	**1.4 Principe du système de gestion de la sécurité de l'information (SGSI)** Les organes d'exécution doivent exploiter un système de gestion de la sécurité de l'information (SGSI) leur permettant de satisfaire aux exigences minimales. Un SGSI est un outil de gestion qui sert à planifier, mettre en œuvre, vérifier et améliorer de manière systématique la sécurité de l'information. Il comprend les règles et les procédures nécessaires et permet de savoir à qui les tâches, les compétences et les responsabilités sont attribuées au sein de l'organisation. Le terme « SGSI » fait implicitement référence à la norme ISO/IEC 27001, qui fait autorité dans le secteur privé et, de plus en plus, dans les administrations publiques. Le SGSI s'appuie sur les normes nationales[5] et internationales[6] et doit au moins satisfaire aux prescriptions suivantes. Il fait l'objet de la vérification par l'organe de révision prévue à l'art. 68*a*, al. 2, let. c, LAVS. L'organe de révision vérifie que le SGSI de l'organe d'exécution répond aux exigences définies dans les présentes directives. Les caisses de compensation pour allocations familiales visées à l'art. 14, let. a, LAFam en sont exclues, sauf disposition contraire dans la loi cantonale sur les allocations familiales.		L'art. 68*a* LAVS ne s'applique pas à la LAFam (contrairement à la LFA). Les règles de la révision des caisses et du contrôle des employeurs relèvent explicitement de la compétence des cantons en vertu de l'art. 17, al. 2, let. i, LAFam. Pour les organes d'exécution de l'AVS qui gèrent également les allocations familiales en tant que tâche déléguée, la révision s'étendra au SGSI, y compris les allocations familiales. Le cas échéant, il est possible d'établir un rapport séparé comme le prévoit le ch. 3604 des Directives sur la remise d'autres tâches aux caisses de compensation (DRAT).

[4] au sens de l'art. 5, let. d à g, LPD

[5] notamment les directives sur la protection informatique de base au sein de l'administration fédérale ou la loi sur la sécurité de l'information LSI

[6] ISO/EC 27001:2022 concernant la sécurité de l'information, la cybersécurité et la protection des données – systèmes de gestion de la sécurité de l'information – exigences et ISO/IEC 27002:2022 concernant la sécurité de l'information, la cybersécurité et la protection de la sphère privée – mesures de sécurité de l'information qui explique les mesures normatives de sécurité de l'information décrites dans ISO/CEI 27001:2022, Annexe A, et émet des propositions en vue de leur mise en œuvre.

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
1.5	**1.5 Sécurité de l'information** La sécurité de l'information est un terme générique, qui couvre des mesures dont le but est d'assurer cette sécurité (du développement du projet jusqu'à la protection des appareils). La sécurité des données et une grande partie de la protection des données appartiennent à la sécurité de l'information. 1. La sécurité des données comprend, d'un point de vue pratique, toutes les mesures permettant de garantir la fiabilité, l'intégrité, la traçabilité et la disponibilité des informations. 2. La protection des données, quant à elle, inclut toutes les mesures visant à éviter un traitement indésirable de données personnelles et ses conséquences. La protection cible la personne et pas les données en soi. Des prescriptions provenant de sources de droit très différentes s'appliquent à la sécurité de l'information et doivent être prises en compte par les organes d'exécution (cf. annexe C1 des annexes complémentaires aux D-SIPD: Aperçu des sources de droit nationales, normes ISO). Les présentes directives se concentrent sur les exigences applicables à un SGSI et ne traitent pas des questions de protection des données telles qu'elles résultent de la relation directe entre un assuré et un organe d'exécution. La circulaire sur l'obligation de garder le secret et sur la communication des données dans le domaine de l'AVS/AI/APG/PC/AFA/AF (COGSC) continue de s'appliquer dans de tels cas. Les présentes directives destinées aux organes d'exécution prennent néanmoins en considération les questions de protection des données, car les exigences en la matière doivent être vérifiées lors de l'élaboration d'une documentation de base du SGSI pour la sécurité de l'information (cf. let. a du ch. 2.8.2). Pour les questions relatives à la conservation des données, il convient en outre de se référer aux Directives sur la gestion, la conservation et la destruction des dossiers dans les domaines AVS/AI/APG/PC/Ptra/AFamAgr/AFam (DGD).		Il s'agit de mesures techniques et organisationnelles. Il ne faut pas les confondre avec les mesures techniques et organisationnelles prévues à l'art. 153*d* LAVS[7], qui doivent uniquement être respectées par les autorités, organisations et personnes autorisées à utiliser le numéro d'assuré AVS en dehors des assurances sociales.

[7] Conformément au message relatif à la modification de la loi fédérale sur l'assurance-vieillesse et survivants (utilisation systématique du numéro AVS par les autorités (FF **2019** 6993)

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
1.6	**1.6 Validité et traitement des rapports d'audit selon ISO 27001 et ISAE 3000 de type 1 et de type 2** Selon cette directive, les rapports d'audit rédigés selon les normes ISO 27001 et ISAE de type 1 ou de type 2 et démontrant la conformité avec les directives D-SIPD sont considérés comme suffisants si au moins une des exigences suivantes est remplie : 1. **Certification ISO 27001 :** les organes d'exécution présentent leur rapport de certification à l'organe de révision. Il n'est pas nécessaire de procéder à un nouvel examen complet si : • Le champ d'application du SGSI certifié englobe toutes les unités organisationnelles et tous les processus d'affaires pertinents des organes d'exécution. • La déclaration d'applicabilité du SGSI n'exclut aucune des mesures de sécurité exigées par les directives D-SIPD. • Lors de l'audit de (re)certification, toutes les mesures de sécurité exigées par les directives D-SIPD ont été vérifiées. 2. **ISAE 3000 de type 1 :** Le rapport d'audit se base sur toutes les conditions fixées dans les directives D-SIPD et se réfère à toutes les exigences fixées par les directives D-SIPD. 3. **ISAE 3000 de type 2 :** Le rapport d'audit (efficacité) est établi avec une certitude suffisante, contrôlé dans le temps et vérifié selon les contrôles définis par les directives D-SIPD.		

	2 Exigences	Norme ISO	Commentaire
2.1	**2.1 Système de gestion de la sécurité de l'information (SGSI)[8]** Chaque organe d'exécution dispose d'un SGSI (cf. ch. 1.4).	4.4	
2.2	**2.2 Structure de base du SGSI de l'organe d'exécution**		
a	Les organes d'exécution fixent dans leur SGSI les thèmes pertinents pour l'exécution de leurs tâches visées aux art. 63 LAVS (RS 831.10) et 57 LAI (RS 831.20) et pour leurs activités dans le cadre de la LAPG (RS 834.1), de la LPC (RS 831.30), de la LFA (RS 836.1) et de la LAFam (RS 836.2).	4.1	
b	Ils identifient les services impliqués et analysent leurs exigences en matière de sécurité de l'information.	4.2	
c	Ils disposent d'une vue d'ensemble actualisée de tous les systèmes d'information et de toutes les activités pertinentes pour l'informatique (cf. inventaire visé au ch. 2.8.1), intégrés dans le SGSI.	A.5.9	
d	Ils déterminent en parallèle les domaines auxquels les exigences ne s'appliquent pas (par ex., les organes d'exécution qui assument des tâches en dehors du champ du 1er pilier / des allocations familiales doivent déterminer quels champs d'application sont exclus). En l'absence de délimitation, le SGSI s'applique à l'ensemble de l'organisation. Par exemple, un établissement d'assurances sociales doit déterminer s'il établit un SGSI pour l'ensemble de l'organisation ou pour chaque organe d'exécution/unité organisationnelle séparément. De même, la Centrale de compensation (CdC) détermine si elle établit un SGSI pour l'ensemble de la CdC ou si les organes d'exécution de la CdC (conformément à l'ordonnance sur la CdC) établissent leur propre SGSI.	4.3	
e	Les organes d'exécution assurent l'actualisation et l'amélioration régulières du SGSI (y c. la gestion de la continuité des activités, cf. ch. 2.17) et de ses composants. Ils vérifient son actualité au moins une fois par année.	4.4 A5.30	
2.3	**2.3 Lignes directrices relatives à la sécurité de l'information** La direction de l'organe d'exécution adopte des lignes directrices relatives à la sécurité de l'information qui s'appuient sur la structure de base du SGSI (ch. 2.2). Elle veille à leur diffusion au sein de l'organe d'exécution et auprès des services externes impliqués, ainsi qu'à leur actualisation régulière. Les lignes directrices relatives à la sécurité de l'information intègrent le principe de séparation des tâches et contiennent les éléments suivants : 1. la définition de l'organisation de la sécurité de l'information et ses interfaces avec les éléments prescrits suivants (art. 66 LAVS) : a. système de contrôle interne (SCI) b. système de gestion de la qualité (en particulier l'amélioration continue)	A.5.1 A.5.3	

[8] Pour mettre sur pied le SGSI, le guide suivant est recommandé :
- ISACA Leitfaden «Implementieren eines ISMS nach ISO/IEC 27001:2022»

	c. système de gestion des risques 2. la réglementation concernant les bonnes pratiques en matière d'information de la direction et des services impliqués (cf. ch. 2.2, let. b et d) ainsi que, le cas échéant : a. du PFPDT conformément à l'art. 24 LPD (en cas de violation de la sécurité des données) ou du responsable de la protection des données prévu par le droit cantonal ; b. de l'OFAS par l'organisation de la sécurité de l'information et la description d'un processus de traitement des incidents liés à la sécurité de l'information (par ex. cf. annexe 1). 3. Il faut prévoir une réglementation de l'information adéquate de l'OFAS (ou des autorités de surveillance compétentes) sur les incidents liés à la sécurité de l'information dans les cas suivants : • Il est nécessaire d'informer le PFPDT ou le responsable cantonal de la protection des données. • Il existe un risque que l'incident nuise au système d'information d'autres organes d'exécution. • L'incident concerne les intérêts des assurés au-delà de quelques cas isolés ou remet en question l'exécution des tâches de l'organe d'exécution. • L'incident peut causer des dommages financiers importants. • L'image de l'assurance peut être sérieusement écornée au-delà d'un cas mineur (par ex. perte ou manipulation de données importante). • Il est possible que le fonctionnement de l'organisation de la sécurité de l'information de l'organe d'exécution ne soit pas assuré dans un futur proche ou ait été entravé par le passé.	A.5.5 A.5.24	Voir Processus d'annonce, annexe 1
2.4	**2.4 Exigences relatives à l'organisation de la sécurité de l'information** L'organisation de la sécurité de l'information prévoit au minimum que l'organe d'exécution désigne une ou plusieurs fonctions responsables de la sécurité de l'information. En règle générale, cela inclut une fonction centrale, telle qu'un(e)·préposé(e) à la sécurité de l'information (PSI), ainsi que d'autres personnes assumant des tâches clés dans la mise en œuvre de la sécurité de l'information. Pour chaque fonction, les responsabilités ainsi que l'attribution à des personnes ou unités concrètes doivent être formellement documentées. Les fonctions ou unités responsables de la sécurité de l'information assument notamment les tâches suivantes : • coordination des aspects liés à la sécurité de l'information au sein de l'organe d'exécution ainsi qu'avec d'éventuels prestataires mandatés (par ex. responsables informatiques, fournisseurs, etc.). • Interlocuteur·trice pour les responsables de la sécurité de l'information des prestataires de services informatiques.	A.5.2	Les désignations courantes pour de telles fonctions sont, par exemple : Chief Information Security Officer (CISO), préposé·e à la sécurité de l'information, Information Security Officer ou responsable SGSI.

	• Point de contact avec l'OFAS en cas d'incidents relatifs à la sécurité de l'information, lorsque les lignes directrices de sécurité de l'organe d'exécution prévoient une notification à l'OFAS (cf. ch. 2.3 ch. 3). • Examen des documentations relatives à la sécurité de l'information (notamment les documentations SIPD, cf. ch. 2.8.2 et 2.8.3) ainsi que des autres éléments de preuve de mise en œuvre. • Information régulière de la direction de l'organe d'exécution sur l'état de la sécurité de l'information au sein de l'organisation. • Émission de recommandations à l'attention de la direction de l'organe d'exécution.		
2.5	**2.5 Exigences applicables aux projets dans le domaine des systèmes d'information** Un projet dans le domaine des systèmes d'information est limité dans le temps. Il implique des objectifs définis et une organisation spécifique, dont le but principal est soit d'introduire ou d'adapter une application, soit de construire ou d'améliorer des infrastructures du système d'information. Les organes d'exécution sont chargés de définir la nécessité d'un projet dans le domaine des systèmes d'information et de réglementer son déroulement. Ils tiennent toujours compte des aspects suivants : 1. La manière de procéder doit suivre une méthode de gestion de projet définie, qui assure la traçabilité lors du pilotage, de la direction et de la réalisation de projets aux caractéristiques et aux degrés de complexité divers. La méthode de gestion de projet utilisée est conforme ou équivalente à la norme suisse de l'association eCH (www.ech.ch). 2. Il convient d'élaborer une documentation relative à la sécurité de l'information et à la protection des données (documentation de base de la SIPD visée au ch. 2.8.2) et, si nécessaire, une documentation élargie de la SIPD visée au ch. 2.8.3.	A.5.8	
2.6	**2.6 Sécurité de l'information pour les appareils mobiles et le travail mobile** Les organes d'exécution définissent : • les conditions générales régissant le travail mobile et l'utilisation d'appareils mobiles pour le personnel concerné ; • l'utilisation professionnelle sûre d'appareils mobiles privés et professionnels, en tenant compte de la possibilité de perte, de vol ou de dégâts. Sont exclues les possibilités d'accès anonyme et personnalisé à des applications conçues sous forme de site Internet public de l'organe d'exécution. Il convient d'assurer une protection équivalente en cas d'utilisation d'appareils privés ; • l'exercice sûr du travail mobile grâce à des mesures de sécurité auxiliaires pour protéger les informations auxquelles les collaborateurs ont accès depuis les appareils mobiles en dehors des espaces de travail ou qui doivent y être traitées ou sauvegardées. Lors du	A.8.1, A.6.7	

	traitement d'informations professionnelles depuis des appareils privés, ceux-ci doivent remplir les mêmes conditions en matière de sécurité des informations et de protection des données que les appareils fournis par les organes d'exécution.		
2.7	**2.7 Sécurité de l'information et personnel**		
2.7.1	**Sécurité du personnel** Les organes d'exécution règlent l'engagement de leur propre personnel et du personnel des tiers mandatés pour la période avant, pendant et après l'engagement de manière à garantir la sécurité de l'information. Il convient de prévoir un processus spécifique pour le contrôle de sécurité du préposé à la sécurité de l'information et des autres rôles clés dans l'organisation de la sécurité de l'information (cf. ch. 2.4), qui permette d'identifier les risques liés à l'intégrité personnelle et de prendre des mesures adéquates. Il est recommandé de contrôler les extraits du registre des poursuites et du casier judiciaire tous les cinq ans.	A.6.1, A.6.2, A.6.3, A.6.4, A.6.5	
2.7.2	**Information et formation** Les organes d'exécution veillent à ce que le personnel engagé soit informé au moins une fois par année sur les obligations en matière de sécurité de l'information et qu'il y soit sensibilisé.	A.5.4, 6.3, 6.4	
2.7.3	**Changement de situation** Les droits d'utilisateur du personnel engagé concernant l'accès (cf. ch. 2.11.1) aux systèmes d'information et les autorisations (cf. ch. 2.9) doivent être tenus à jour. Ils doivent être immédiatement adaptés aux changements de situation lorsque l'engagement, le mandat ou une convention d'utilisation sont modifiés ou prennent fin. Il convient de mettre en place un processus pour gérer les comptes inutilisés.	A.6.5	
2.8	**2.8 Objets du SI à protéger : inventaire, documentation de la SIPD et autres exigences**	A.5.9, A.5.10	
2.8.1	Les organes d'exécution disposent d'un **inventaire** de tous les systèmes d'information (cf. ch. 2.2, let. c). Celui-ci est mis à jour régulièrement. Un système d'information est toujours un bien devant faire l'objet d'une protection adéquate. Il s'agit donc d'un objet à protéger.	A.5.9	
2.8.2	**Documentation de base de la SIPD** 1. Tout projet dans le domaine des systèmes d'information (ch. 2.5) doit faire l'objet d'une analyse préalable de la sécurité de l'information et de la protection des données. L'examen préalable des risques selon l'annexe C5 des annexes complémentaires aux D-SIPD ou des modèles cantonaux/internes peuvent être utilisés comme modèles. 2. La documentation de base de la SIPD doit couvrir au moins les thèmes suivants en lien avec la sécurité de l'information et la protection des données : a. clarification du cadre juridique de la protection des données, en particulier en ce qui concerne la conformité légale du traitement des données au regard de la LPD et, le cas échéant, d'autres lois	A.5.10, A.5.12, 5.13	Aides et modèles voir annexe C5 des annexes complémentaires aux D-SIPD

	cantonales sur la protection des données et d'autres dispositions de lois sur les assurances sociales (voir guide à l'annexe C2 des annexes complémentaires aux D-SIPD) ; b. classification de l'objet à protéger selon la disponibilité (y c. évaluation de l'objet à protéger en lien avec la classification en tant qu'application essentielle) ; c. classification de l'objet à protéger selon la confidentialité ; d. classification de l'objet à protéger selon l'intégrité et la traçabilité (en ce qui concerne les accès aux données en mode écriture) ; e. lieu de conservation des données ; f. description de l'objet à protéger ; g. clarification des règles d'inscription dans le registre d'activités ou d'annonce au PFPDT (art. 12, al. 4, LPD). Les organes d'exécution qui sont des organismes cantonaux clarifient l'inscription dans un registre cantonal, conformément à la loi cantonale de protection des données ; h. clarification de la nécessité d'une analyse d'impact relative à la protection des données personnelles visée à l'art. 22 LPD ; i. attribution à un groupe de protection. 3. Si, sur la base de l'analyse visée au point 2, il est établi que des données personnelles sensibles ou d'autres données soumises à des exigences particulières de confidentialité sont traitées avec l'objet à protéger, il faut élargir la documentation de base de la SIPD visée au ch. 2.8.3. 4. Que ce soit sous l'angle qualitatif ou quantitatif, la documentation de base de la SIPD suit le modèle de l'annexe C2 des annexes complémentaires aux D-SIPD.		
2.8.3	**Documentation élargie de la SIPD** La documentation élargie de la SIPD doit être élaborée lorsque des données personnelles sensibles sont traitées avec l'objet à protéger, c'est-à-dire lorsque leur traitement peut entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (ch. 2.8.2, point 3). Elle doit englober au moins les thèmes suivants : a. résumé des événements pertinents de la documentation de base de la SIPD ; b. Description du système du point de vue de la sécurité b.1 interlocuteurs / responsabilités ; b.2 description de l'ensemble du système ; b.3 description des données à traiter (règlement du traitement avec définition des rôles et gestion des supports de données) ; b.4 esquisse d'architecture / matrice de communication ;	A.5.10, A.5.12, 5.13	

	b.5 description de la technologie sous-jacente ; c. analyse de risque, mesures de protection et risque résiduel (le cas échéant avec prise de position du PFPDT) ; d. rétablissement de l'activité / plan d'urgence (prévision des catastrophes, crises) ; e. Respect / contrôle / adoption des mesures de protection f. Mise hors service La documentation élargie de la SIPD doit s'inspirer du modèle proposé dans l'annexe C3 des annexes complémentaires aux D-SIPD, que ce soit sous un aspect qualitatif ou quantitatif.		
2.8.4	**Actualisation de la documentation de la SIPD** Les systèmes d'information existants (en exploitation) doivent disposer d'une documentation de la SIPD (ch. 2.8.2 et 2.8.3) qui corresponde aux relations effectives.		Modifications des systèmes d'information voir ch. 2.14
2.8.5	**Responsable de l'application** Les organes d'exécution désignent un responsable de l'application pour chaque système d'information utilisé individuellement ou en commun. Celui-ci fixe, avec le préposé à la sécurité de l'information, les exigences de sécurité pour le système d'information. Le responsable de l'application répond de la mise en œuvre des mesures de sécurité.	A.5.9	
2.9	**2.9 Gestion de l'accès aux systèmes d'information** Les organes d'exécution gèrent l'accès à leurs systèmes d'information. Le modèle de gestion de l'accès contient au moins a. une gestion des utilisateurs avec une identification univoque ; b. un modèle d'autorisation selon les fonctions ou les tâches des utilisateurs ; c. des processus d'octroi, de mutation et de retrait de comptes d'utilisateur et des autorisations ; et assure que d. l'ensemble des accès aux systèmes d'information (y c. les processus automatisés avec accès machine-to-machine) soient protégés par une authentification correspondant au degré de protection nécessaire et, si besoin, par des mesures cryptographiques adéquates (ISO A.8.24) conformément à la matrice d'accès (cf. aussi ch. 2.13.2) ; e. les utilisateurs reçoivent uniquement les droits d'accès aux systèmes d'information nécessaires pour l'exécution de leurs tâches ; f. une journalisation des accès soit opérée conformément à l'art. 4 OPDo (voir annexe C2, ch. 7 des annexes complémentaires aux D-SIPD) ; g. le responsable de l'application contrôle au moins une fois par an l'exactitude et la pertinence des droits d'accès.	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5	

2.10	**2.10 Cryptographie**		
2.10.1	Les procédures et méthodes cryptographiques mises en place par les organes d'exécution doivent correspondre à l'état de la technique. En cas d'utilisation de systèmes de cryptage asymétriques, les certificats doivent être établis par une autorité de certification reconnue, en fonction du cas d'application et des exigences juridiques correspondantes. Les certificats reconnus par SAS pour des signatures électroniques, conformément à l'ordonnance sur la signature électronique (OSCSE ; RS 943.032)[9]. La solution choisie doit être décrite dans la documentation de la SIPD (ch. 2.8.2 ou 2.8.3). Les organes d'exécution garantissent la gestion sécurisée et la validité des clés cryptographiques.	A.8.24	
2.11	**2.11 Protection physique**		
2.11.1	**Dispositif de sécurité pour les locaux** Les organes d'exécution possèdent un dispositif de sécurité pour protéger physiquement leurs systèmes d'information. Ils doivent prévoir diverses mesures garantissant une protection individuelle adéquate des objets à protéger, en tenant compte des résultats du contrôle de la SIPD (ch. 2.8.2 ou 2.8.3) en ce qui concerne les groupes de protection (cf. ch. 2.8.2, point 2, let. i). Les mesures de protection à prévoir dans le dispositif de sécurité doivent porter sur les points suivants : • périmètre de sécurité physique (situation de l'environnement et mesures architecturales) ; • gestion de l'accès physique ; • protection des bureaux, locaux et installations ; • protection contre les menaces externes et environnementales.	A.7.1, A.7.2, A.7.3, A.7.5	
2.11.2	**Mesures pour les appareils et les équipements** Les organes d'exécution et leurs fournisseurs (cf. ch. 2.15.1) disposent de mesures documentées visant à protéger les appareils et les équipements contre la perte, les dégâts, le vol ou la mise en danger. Les mesures à prévoir pour les appareils doivent porter sur les points suivants : • emplacement et protection des appareils et des équipements ; • dispositifs d'alimentation ; • sécurité du câblage ; • maintenance des appareils et des équipements ;	A.7.7 - A.7.14, A.8.1	

[9] voir le site de l'OFCOM

	• retrait des valeurs ; • sécurité des appareils, équipements et valeurs en dehors des locaux ; • élimination sûre ou réutilisation des appareils et des équipements ; • appareils d'utilisateurs sans surveillance ; • directives pour un environnement de travail propre et verrouillages des écrans.		
2.12	**2.12 Mesures de sécurité opérationnelle** Les organes d'exécution et leurs fournisseurs (cf. ch. 2.15) disposent de mesures documentées permettant d'assurer la sécurité opérationnelle. Les mesures à prévoir doivent porter sur les points suivants : A. Procédures et responsabilités opérationnelles • procédures opérationnelles documentées ; • gestion des modifications ; • gestion des capacités ; • séparation des environnements de développement, de test et d'exploitation. B. Protection contre les logiciels malveillants par des mesures adaptées C. Sécurité des données D. Enregistrement et surveillance • enregistrement des événements ; • protection des informations enregistrées ; • activités des administrateurs et des utilisateurs ; • synchronisation des horloges. E. Gestion des logiciels pour l'installation des logiciels sur les systèmes en exploitation F. Vulnérabilités techniques • gestion des vulnérabilités techniques ; • restriction d'installation de logiciels. G. Contrôle de l'intégrité en cas de besoin de protection accru (cf. annexe C2, let. D des annexes complémentaires aux D-SIPD) H. Contrôle des systèmes d'information Ainsi que des mesures pour les audits de systèmes d'information, afin de minimiser les effets négatifs de l'activité de contrôle. En effet, les activités de contrôle comme le test d'intrusion et les tests de prévention de crise peuvent avoir des conséquences négatives sur les systèmes d'information, les données et les utilisateurs. C'est pourquoi des mesures correspondantes, dont une planification détaillée, la communication, etc., doivent être prévues pour atténuer ces conséquences.	A.5.37, A.8.6, A.8.31, A.8.32 A.8.7 A.8.13, A.8.15, A.8.17 A.8.19 A.8.19 A.8.8 A.8.34	

2.13	**2.13 Gestion des réseaux et de la communication**		
2.13.1	**Documentation de l'architecture** Les organes d'exécution disposent d'une documentation de l'architecture qui porte sur l'environnement de leurs systèmes d'information. Celle-ci renseigne sur • les topologies de réseaux propres et externes sous-jacentes des réseaux utilisés dans le cadre de leur inventaire de valeurs (cf. ch. 2.8.1) ; • les topologies de réseaux sous-jacentes, y compris ses composants actifs et leurs configurations.		
2.13.2	**Matrice d'accès** Les organes d'exécution disposent d'une matrice d'accès contraignante, qui détermine la façon dont les personnes et les processus automatisés (machines/logiciels) peuvent accéder aux systèmes d'information exploités dans les différentes zones du réseau (cf. ch. 2.13.3) ou la façon dont elles doivent être authentifiées et éventuellement autorisées (cf. ch. 2.10, cryptographie).		
2.13.3	**Sécurité et documentation du réseau** 1. Les organes d'exécution doivent prévoir des directives relatives à la sécurité du réseau et définir les responsabilités en matière de gestion des réseaux et de connexions entre les réseaux. 2. Les organes d'exécution disposent, pour les réseaux relevant de leur responsabilité, d'un règlement d'utilisation qui définit au moins les points suivants : • raccordement d'appareils de communication externes ; • règlement des connexions entre réseaux ; • accès à distance. 3. Les organes d'exécution doivent assurer la protection des données en lien avec le 1er pilier à l'aide d'une structure réseau adéquate (par ex. zonage et segmentation), d'une construction adaptée et d'une bonne configuration. 4. Les organes d'exécution protègent les réseaux relevant de leur responsabilité contre les attaques et les accès non autorisés. 5. Pour les réseaux qui ne relèvent pas de la responsabilité des organes d'exécution et dont l'utilisation ne peut pas être contractuellement réglée (Internet), il faut mettre en œuvre des mesures de sécurité. 6. Il convient de documenter les structures du réseau et les responsabilités.	A.8.20 - A.8.22 A.5.14, A.6.6 A.8.21	

2.13.4	**Transfert protégé d'informations** 1. Concernant le transfert d'informations, les organes d'exécution prennent des mesures qui garantissent que les données soient suffisamment protégées conformément aux exigences de protection et de sécurité des données (sécurité de l'information, ch. 2.8.2 / 2.8.3), indépendamment du fait qu'ils utilisent un réseau propre, un réseau régi par un contrat ou un réseau externe pour l'échange de données (cf. ch. 2.10 Cryptographie). 2. Les organes d'exécution veillent à ce que les collaborateurs (cf. ch. 2.7.2) connaissent les différents niveaux de protection (cf. ch. 2.8.2 et 2.8.3) en cas de transfert de données et qu'ils utilisent des moyens de transfert correspondants (par ex. courrier électronique crypté). 3. Concernant l'échange de données électroniques notamment des données personnelles sensibles (selon la LPD) entre les organes d'exécution et la Centrale de compensation (CdC), il existe plusieurs solutions techniques : 1 Réseau sedex : voir les directives de l'OFAS sur la plateforme informatique d'échange de données entre caisses de compensation AVS et offices AI (318.106.07 PED). 2 Transmission cryptée (par ex. Incamail, que tous les organes d'exécution ont adopté comme norme commune via l'association eAVS/AI). 3 Envoi directement depuis l'application au lieu d'un e-mail.	A.5.14, A.6.6	
2.14	**2.14 Modifications des systèmes d'information** Les organes d'exécution s'assurent que la sécurité fait partie intégrante des systèmes d'information durant l'ensemble de leur cycle de vie. Il convient de prendre en considération les exigences de sécurité spécifiques qui dérivent de la sécurité de l'information et de la protection des données (cf. ch. 2.5, 2.8.2 et 2.8.3). La documentation de la SIPD (ch. 2.8.2 ou 2.8.3) doit être actualisée en cas de modification. Si aucune modification n'a été apportée au système d'information, l'actualité de la documentation de la SIPD doit être vérifiée au moins une fois tous les cinq ans. Les exigences qui, selon le ch. 2.5, s'appliquent aux nouveaux projets sont également valables pour les modifications des systèmes d'information. Cela permet de s'assurer que les exigences de sécurité sont prises en compte lors du développement des systèmes d'information. Il convient en outre de respecter les exigences énoncées au ch. 2.12, let. A, 4e élément, concernant la séparation des environnements de développement, de test et d'exploitation, et de garantir la protection des données utilisées pour les tests. Si les organes d'exécution ne sont pas eux-mêmes responsables de la mise en œuvre des modifications de leurs systèmes d'information, les exigences doivent être communiquées aux tiers chargés des modifications et le respect de ces exigences doit être surveillé et contrôlé.	A.5.8, A.8.26 A.8.25, A.8.27, A.8.29 - A.8.32 A.8.33 A.8.30	

2.15	**2.15 Contrats avec des tiers**		
2.15.1	• Si les organes d'exécution concluent des contrats avec des tiers pour la fourniture de prestations qui impliquent un potentiel accès à des données relevant du droit des assurances sociales ou qui concernent le traitement de telles données, ils fixent contractuellement l'ensemble des règles de protection (devoir de confidentialité, traitement des données, etc.) et les exigences applicables aux prestations. Ils précisent également dans le contrat les mesures de contrôle correspondantes et, pour les tiers qui ne sont pas contrôlés par les organes d'exécution, les peines conventionnelles prévues en cas de violation de ces dispositions. Ces contrats peuvent être aussi bien des relations avec les fournisseurs dans le domaine IT que des prestations ne relevant pas du domaine IT. En outre, les organes d'exécution s'assurent, au moyen d'une clause contractuelle appropriée, qu'ils soient habilités à faire des audits auprès de leurs prestataires, sauf dans les cas prévus au chapitre 2.2, ch. 7 DASP, où un audit externe distinct auprès de tiers n'est pas nécessaire. • En principe, un contrat avec un tiers doit prévoir que ce dernier l'exécutera lui-même et que l'organe d'exécution doit pouvoir s'opposer à tout transfert éventuel (partie ou total) des engagements. Même en cas de transfert des engagements, il faut s'assurer par des accords que les exigences minimales seront pleinement respectées. • Si l'OFAS a conclu un contrat-cadre avec un prestataire de services actif auprès des offices AI, les offices concernés appliquent les mêmes exigences en matière de sécurité de l'information (SIPD) que celles prévues dans ce contrat-cadre. • Les prestations relatives à l'exploitation doivent être réalisées sur le territoire national. Il est nécessaire de déclarer et de justifier les prestations relatives à l'exploitation réalisées à l'étranger. • Il convient de garantir en tout temps qu'aucune donnée personnelle d'assurés n'est traitée à l'étranger, sauf si ce traitement est lié à un échange international de données réglementé sur le plan légal (par ex. art. 32, al. 3, LPGA ou CIBIL ([Accords bilatéraux Suisse-UE. Convention AELE. Circulaire sur la procédure pour la fixation des prestations dans l'AVS/AI/PC]). • Outre le respect des dispositions légales en matière de protection des données, les prestataires des organes d'exécution doivent signer une convention de confidentialité s'ils ont accès aux données du 1er pilier/IPFam	A.5.19 - A.5.21	Indications sur : - Heures de service exigées - Exigences Disponibilité Les organes d'exécution déterminent le besoin de protection des données qui doivent être traitées par des tiers et, si nécessaire, établissent l'évaluation préalable des risques et l'AIPD. Sur la base de la documentation ainsi établie, les tiers potentiels documentent la manière dont ils respectent les prescriptions en matière de protection des données concernant l'organe d'exécution (protection de base et, le cas échéant, documentation élargie de la SIPD).

2.15.2	Lors de l'utilisation de M365, qui implique la conclusion d'un contrat avec la société Microsoft en tant que tiers, les points suivants doivent être pris en compte :
	
	• En principe, les données M365 ne peuvent être stockées dans le cloud que sous forme chiffrée. Grâce à la fonction de chiffrement mise en place par défaut par Microsoft, qui correspond aux normes industrielles en vigueur, M365 peut être utilisé sans mesures supplémentaires.
	
	• Lors de l'initialisation, il est impératif que les organes d'exécution choisissent un tenant (espace de stockage) situé en Suisse.
	
	• Une authentification multifacteur (MFA[10]) doit être mise en place pour tout accès depuis l'extérieur de l'organisation et via Internet.
	
	• Chaque organe d'exécution doit s'assurer que les risques potentiels ont été analysés, évalués et que des mesures appropriées ont été prises. Cela concerne en particulier le traitement et le stockage de données personnelles sensibles, qui nécessitent les actions suivantes :
	  • Réalisation d'une analyse des besoins de protection
	  • Réalisation d'un examen préliminaire des risques
	  • Réalisation d'une analyse d'impact sur la protection des données (si cela est exigé à la suite de l'examen préliminairedes risques)
	  • Mise en place des mesures de protection informatique de base
	  • Réalisation d'une analyse des risques et d'un concept SIPD (si requise selon l'analyse des besoins de protection)
	
	Les détails relatifs aux analyses et évaluations figurent dans les annexes C2 et C3 des annexes complémentaires aux D-SIPD.
	
	Si les mesures de protection mises en place et les actions d'atténuation des risques permettent le traitement et le stockage des données dans le cloud, celles-ci peuvent être gérées et stockées via les applications M365. Le traitement et le stockage de données classifiées selon les articles 18, 19 et 20 de l'OSI, restent soumis aux principes applicables aux solutions cloud[11] de l'administration fédérale, conformément à l'article 2 OSI (voir Annexe C2 complémentaires aux D-SIPD let. I Attribution à un groupe de protection).
	
	De plus, les réglementations cantonales peuvent restreindre l'utilisation de M365, indépendamment de la présente directive.
	
	L'utilisation de Microsoft Exchange Online est possible dans le cadre des limitations décrites ci-dessus, telles que l'analyse et l'évaluation
		A 5.23	

[10] Microsoft MFA : https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

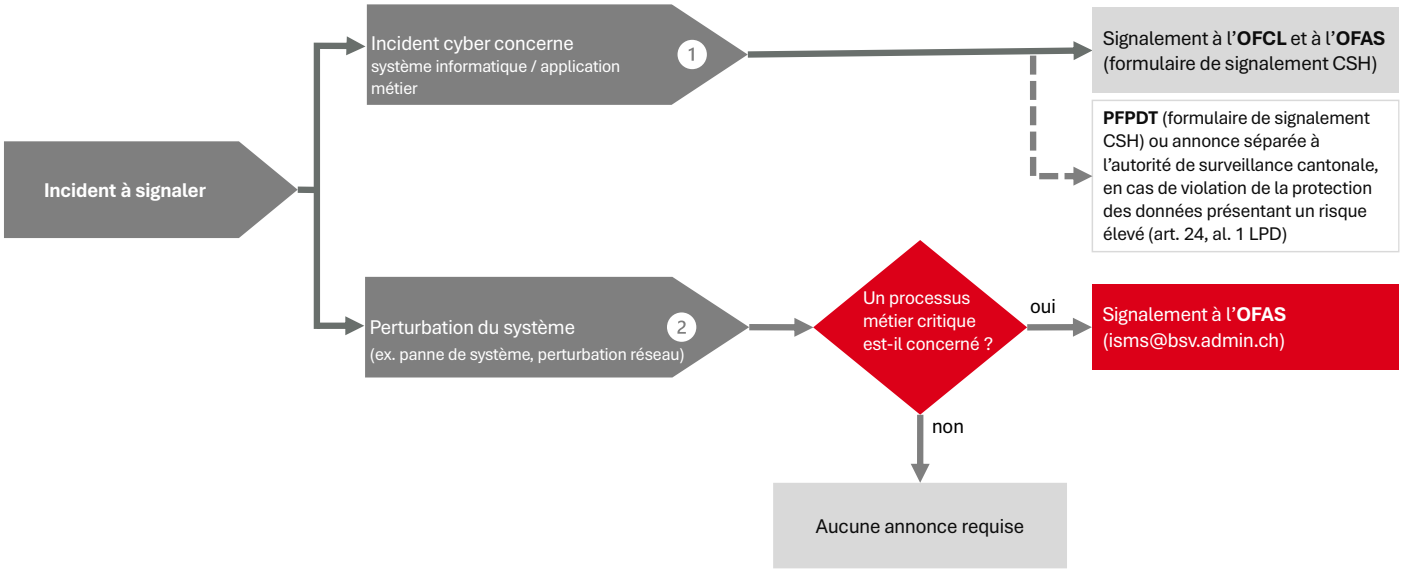
[11] Informatique en nuage : https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

	pour les données personnelles sensibles. L'accès à Exchange Online depuis l'extérieur de l'organisation ou via Internet doit impérativement être sécurisé par une solution MFA (authentification multifacteur). Pour l'envoi de données sensibles, il est en outre impératif d'utiliser une technologie de cryptage de pointe (indépendamment de l'application utilisée, par exemple IncaMail ou équivalent). La dépendance aux services cloud de Microsoft ainsi qu'à d'autres services cloud comporte des risques. Les entités responsables doivent élaborer une **stratégie de sortie** et documenter les mesures nécessaires afin de garantir leur capacité d'action en cas d'urgence (par exemple, en cas d'indisponibilité des services cloud de Microsoft).		
2.16	**2.16 Gestion des incidents relatifs à la sécurité de l'information** Le préposé à la sécurité de l'information des organes d'exécution s'assure que les notifications concernant des incidents de sécurité en lien avec les systèmes d'information sont adéquatement traitées, documentées et évaluées, afin de réduire la probabilité d'occurrence ou les conséquences de futurs incidents.Il dispose d'un plan de réaction et de communication pour les incidents de sécurité, ce qui permet de garantir que les personnes compétentes prennent les mesures appropriées.	A.5.24 - A.5.28, A.6.8	
2.17	**2.17 Maintien de la sécurité de l'information (gestion de la continuité des activités)** Les organes d'exécution disposent - conformément au besoin des objets du SI à protéger (cf. ch. 2.8.2 et 2.8.3) - de procédures de redémarrage testées pour maintenir et restaurer l'exploitation des systèmes TIC critiques à protéger en cas de perturbationset de catastrophes. Si l'organe d'exécution a confié l'exploitation d'un ou plusieurs objets protégés à des prestataires externes, le prestataire concerné est responsable du respect du chiffre 2.17. Dans ce cas, l'organe d'exécution vérifie l'existence des procédures BCM du prestataire concerné	A.5.29, A.5.30, A.8.14	
2.18	**2.18 Conformité aux directives** Les organes d'exécution veillent à ce que les lacunes liées aux systèmes d'information identifiées grâce à leur système de contrôle interne, à leur gestion de la qualité ou à leur gestion du risque (cf. aussi ch. 2.3) soient comblées, indépendamment du fait qu'elles aient déjà été découvertes lors d'une révision prévue par le droit de la surveillance.	A.5.31-A.5.34, A.5.35, A.5.36, A.8.8	

Annexe 1 : Obligation de signalement des cyberincidents et perturbations du système

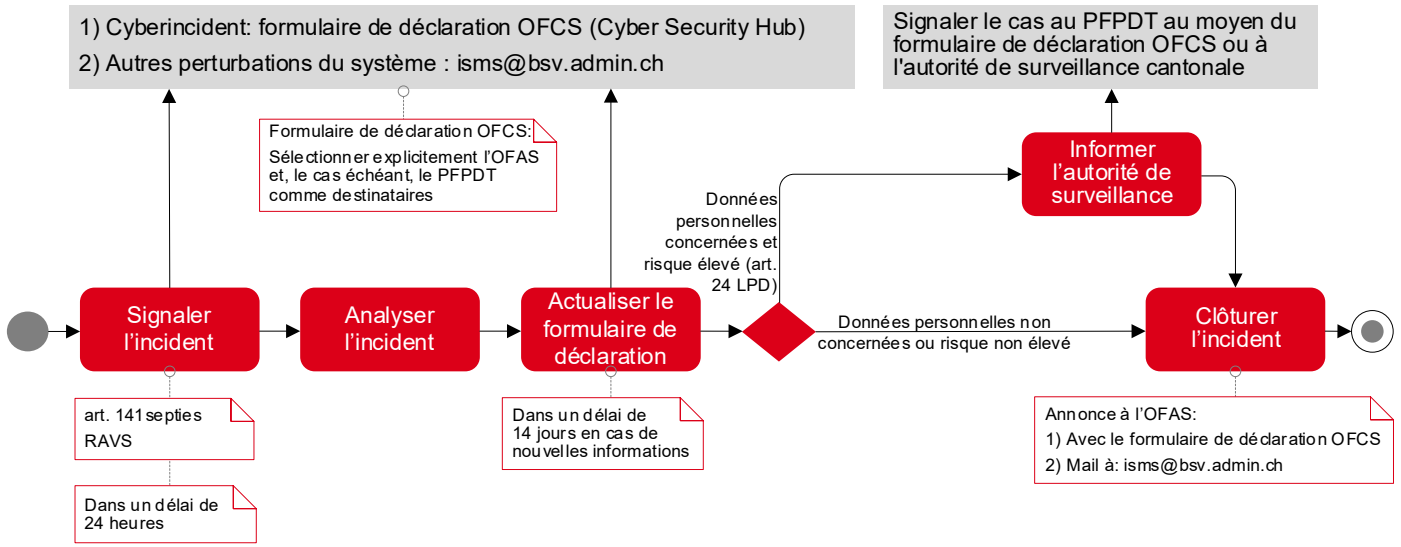
A.2.1 Aperçu de l'obligation de signaler

Conformément à l'art. 141septies RAVS, une distinction est faite entre les cyberincidents et les perturbations du système. Les perturbations du système (p. ex. pannes ou dysfonctionnements du réseau) qui affectent un processus opérationnel critique (au sens du ch. 2.8.2, let. b) doivent être signalées à l'OFAS par courriel à l'adresse isms@bsv.admin.ch. Le formulaire de signalement de l'OFCS[12] est exclusivement réservé aux cyberincidents.



A.2.2 Signalement d'un cyberincident

Les cyberincidents doivent être signalés à l'OFAS à l'aide du formulaire de l'OFCS.



[12] Site web du NCSC (OFCS) avec lien du formulaire de signalement: https://www.ncsc.admin.ch/ncsc/fr/home.html

Annexe 2 : Exigences relatives aux rôles des organes d'exécution

#	Abréviation	Mission	Description
1	CD	Comité de direction/ Direction de l'organe d'exécution	Le comité de direction / la Direction de l'organe d'exécution adopte des lignes directrices relatives à la sécurité de l'information qui s'appuient sur la structure de base du SGSI (ch. 2.2). Elle veille à leur diffusion au sein de l'organe d'exécution et auprès des services externes impliqués, ainsi qu'à leur actualisation régulière.
2	PSI/CISO	Préposé à la sécurité de l'information ou d'autres désignations courantes pour ces postes sont par exemple « Chief Information Security Officer » (CISO), « Information Security Officer » ou « Responsable SGSI ».	Il est entre autres l'interlocuteur de l'OFAS pour les incidents relatifs à la sécurité de l'information pour lesquels les lignes directrices édictées par l'organe d'exécution prévoient une information à l'OFAS (ch. 2.3, point 3).
3	RA	Responsable d'application	Les organes d'exécution désignent un responsable de l'application pour chaque système d'information utilisé individuellement ou en commun. Celui-ci fixe, avec le préposé à la sécurité de l'information, les exigences de sécurité pour le système d'information. Le responsable de l'application répond de la mise en œuvre des mesures de sécurité.
4	CDP	Chef de projet	Dirige les projets correspondants dans le domaine des systèmes d'information
5	ARS	Administrateur du réseau/système	Gère le réseau et/ou les infrastructures du serveur, mise en œuvre de mesures techniques de sécurité
6	CPD	Conseiller à la protection des données	(art. 25 et art. 26 al. 2 let. a ch. 2 OLPD). Est impliqué lors de l'établissement de la documentation élargie de la SIPD (si des données personnelles sensibles sont traitées avec l'objet protégé)

Liste des abréviations

Abréviation	Terme	Lien
AI	Assurance-invalidité	
AIPD	Analyse d'impact relative à la protection des données personnelles	https://sozialversicherungen.admin.ch/fr/f/20762
Al.	Alinéa	
APG	Allocations pour perte de gain	
ARS	Administrateur du réseau/système	
Art.	Article	
AVS	Assurance-vieillesse et survivants	
BCM	Gestion de la continuité des activités	
CA	Certificate Authority, organisme de certification	
CC	Caisse de compensation	
CdC	Centrale de compensation	
CDP	Chef de projet	
ch.	Chiffre	
CIBIL	Circulaire sur la procédure pour la fixation des prestations dans l'AVS/AI/PC	https://sozialversicherungen.admin.ch/fr/d/6399/download
COGSC	Circulaire sur l'obligation de garder le secret et sur la communication des données dans le domaine de l'AVS/AI/APG/PC/AFA/AF	https://sozialversicherungen.admin.ch/fr/d/6435
CPD	Conseiller à la protection des données	
DGD	Directives sur la gestion, la conservation, l'archivage et la destruction des documents dans les domaines AVS/AI/APG/PC/Ptra/AFamAgr/AFam	https://sozialversicherungen.admin.ch/fr/d/6921/download
DRAT	Directives sur la remise d'autres tâches aux caisses de compensation	https://sozialversicherungen.admin.ch/fr/d/6956/download
eAVS/AI	Association des organes d'exécution de l'AVS et de l'AI	https://www.eahv-iv.ch/fr/
eCH	Association de développement de normes dans la cyberadministration	https://www.ech.ch/fr
ISACA	Information Systems Audit and Control Association	https://www.isaca.ch/de/
ISO	Organisation internationale de normalisation	
ISO 27001	ISO/IEC 27001 Technologies de l'information – procédures de sécurité informatique – systèmes de management de la sécurité de l'information – exigences (avec annexe 1 normative concernant les objectifs et mesures de références, qui dérivent de la norme ISO/IEC 27002)	
ISO 27002	ISO/IEC 27002 Technologies de l'information – procédures de sécurité informatique – guide des mesures de sécurité de l'information	
LAFam	Loi fédérale sur les allocations familiales ; RS *836.2*	https://www.fedlex.admin.ch/eli/cc/2008/51/fr
LAI	Loi fédérale sur l'assurance-invalidité ; RS *831.20*	https://www.admin.ch/opc/fr/classified-compilation/19590131/index.html
LAPG	Loi sur les allocations pour perte de gain ; RS *834.1*	https://www.fedlex.admin.ch/eli/cc/1952/1021_1046_1050/fr

Abréviation	Terme	Lien
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants ; RS *831.10*	https://www.fedlex.admin.ch/eli/cc/63/837_843_843/fr
LFA	Loi fédérale sur les allocations familiales dans l'agriculture ; RS *836.1*	https://www.fedlex.admin.ch/eli/cc/1952/823_843_839/fr
LPC	Loi fédérale sur les prestations complémentaires à l'assurance-vieillesse, survivants et invalidité ; RS *831.30*	https://www.fedlex.admin.ch/eli/cc/2007/804/fr
LPD	Loi fédérale sur la protection des données ; RS *235.1*	https://www.fedlex.admin.ch/eli/cc/2022/491/fr
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales ; RS *830.1*	https://www.fedlex.admin.ch/eli/cc/2002/510/fr
LSI	Loi du 20 décembre 2020 sur la sécurité de l'information	https://www.fedlex.admin.ch/eli/fga/2020/2696/fr
O	Ordonnance	
OAMal	Ordonnance du 27 juin 1995 sur l'assurance-maladie ; RS *832.102*	https://www.admin.ch/opc/fr/classified-compilation/19950219/index.html
OFCS	Office fédéral de la cybersécurité	https://www.ncsc.admin.ch/ncsc/fr/home.html
OPDo	Ordonnance sur la protection des données , RS *235.11*	https://www.fedlex.admin.ch/eli/cc/2022/568/fr
OTNI	Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale ; RS *172.010.58*	https://www.fedlex.admin.ch/eli/cc/2020/988/fr
PC	Prestations complémentaires	
PCE	Personne de confiance	
PFPDT	Préposé fédéral à la protection des données et à la transparence	https://www.edoeb.admin.ch/edoeb/fr/home.html
PSI	Préposé à la sécurité de l'information (au sens des présentes directives)	
RA	Responsable d'application	
RAVS	Règlement sur l'assurance-vieillesse et survivants ; RS *831.101*	https://www.admin.ch/opc/fr/classified-compilation/19470240/index.html
SAS	Service d'accréditation suisse	https://www.sas.admin.ch/sas/fr/home.html
SCI	Système de contrôle interne	
SCSE	Loi sur la signature électronique ; RS 943.03	https://www.admin.ch/opc/fr/classified-compilation/20131913/index.html
SGQ	Système de gestion de la qualité	
SGR	Système de gestion des risques	
SGSI	Système de gestion de la sécurité de l'information	
SI	Système d'information	
SIPD	Sécurité de l'information et protection des données	
TI	Technologie de l'information	