|  |
| --- |
| **Modèle de document** |
| **Documentation SIPD étendue pour les partenaires contractuels des offices AI** |
| Office fédéral des assurances sociales |
| 14.10.2024 |

Informations sur le document

|  |  |
| --- | --- |
| Titre : | Documentation SIPD étendue pour les partenaires contractuels des offices AI |
| Date de publication : | 14.10.2024 |
| Enregistré : | 12. décembre 2024 |
| Nombre de pages : | 13  |
| Nom de fichier : | ISDS-Vorlage - Erweiterter Schutz\_Dritte-f.docx |
| Responsable du document : | BSV, DS-ITM |
| Statut : | Finale |
| Vérifié par : | BSV,  | Datum : 31.12.2024 |

Versions

| Version du document | Date | Principales modifications | Responsable |
| --- | --- | --- | --- |
| V0.1 | 14.10.2024 | élaboration | M. BurriM. Moog |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Abréviations et termes

|  |  |
| --- | --- |
| Abréviations | Description |
| CC | caisse de compensation |
| OE | organe d’exécution |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Documents référencés

Certains aspects relatifs à la sécurité sont consignés dans des documents séparés. Les documents suivants sont référencés dans le cadre du présent concept SIPD :

| Titre | Auteur / éditeur | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table des matières

[1. But du document 5](#_Toc184899760)

[2. Résumé 5](#_Toc184899761)

[2.1. Généralités 5](#_Toc184899762)

[2.2. Résumé des risques résiduels 5](#_Toc184899763)

[2.3. Remarques finales 5](#_Toc184899764)

[3. Liste des documents relatifs à la sécurité 5](#_Toc184899765)

[4. Classification d’après l’analyse des besoins de protection 6](#_Toc184899766)

[5. Description du système du point de vue de la sécurité 7](#_Toc184899767)

[5.1. Interlocuteurs et responsabilités 7](#_Toc184899768)

[5.2. Description du système global 7](#_Toc184899769)

[5.3. Description des données à traiter 7](#_Toc184899770)

[5.4. Esquisse de l’architecture et matrice de communication 8](#_Toc184899771)

[5.5. Description de la technologie sous-jacente 9](#_Toc184899772)

[6. Analyse des risques et mesures de protection 10](#_Toc184899773)

[6.1. Risques résiduels 10](#_Toc184899774)

[6.1.1. Risques résiduels élevés (rouge) 11](#_Toc184899775)

[6.1.2. Risques résiduels élevés (jaune) 11](#_Toc184899776)

[6.2. Éléments particuliers à prendre en compte 12](#_Toc184899777)

[7. Rétablissement des activités 12](#_Toc184899778)

[8. Respect, contrôle et approbation des mesures de protection 12](#_Toc184899779)

[8.1. Contrôle de la réception du système 12](#_Toc184899780)

[9. Mise hors service 13](#_Toc184899781)

[10. Abréviations 13](#_Toc184899782)

[11. Annexe 13](#_Toc184899783)

# But du document

Le concept SIPD définit les indications nécessaires pour le maintien et l’amélioration de la sécurité de l’information et de la protection des données. Il récapitule les aspects de la sécurité de l’information et de la protection des données et décrit le système informatique dans son ensemble, documente l’analyse des risques ainsi que les mesures de protection prises.

# Résumé

Le résumé synthétise brièvement le but de l’objet à protéger, les résultats de l’analyse des besoins de protection ainsi que les mesures prises. Il devrait être rédigé de façon à ce que même les personnes ne possédant pas de connaissances techniques approfondies puissent le comprendre. Il résume en outre les risques résiduels supportés par la direction lors de l’approbation du présent concept SIPD.

Il est recommandé de rédiger le résumé après élaboration du document (après la première révision).

## Généralités

Résumé des indications figurant dans le document et concernant l’analyse des risques effectuée, la sécurité de l’information et la protection des données. Il donne une image du potentiel de risque du système examiné.

## Résumé des risques résiduels

Un résumé et une évaluation des risques résiduels doivent être effectués selon le chapitre 6.1**.** La décision d’assumer ou non les risques résiduels appartient au responsable de l’organisation compétente.

## Remarques finales

Remarques finales et conclusions importantes relatives à l’objet informatique à protéger.

# Liste des documents relatifs à la sécurité

Il s’agit de citer les bases légales sur lesquelles s’appuie le projet informatique (à réaliser).

Outre les prescriptions des autorités (lois, ordonnances, directives), les documents internes doivent également être mentionnés.

Certains risques ou dangers peuvent parfois être couverts par des concepts généraux de sécurité ou par des SLA. Ces documents sont énumérés ci-dessous.

|  |  |
| --- | --- |
| Type de document | Titre |
| Loi | [Loi fédérale sur la protection des données (LPD ; RS *235.1*)](https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html) |
|  | [Loi fédérale sur l’archivage (LAr ; RS *152.1*)](https://www.admin.ch/opc/fr/classified-compilation/19994756/index.html)  |
|  |  |
| Ordonnance | [Ordonnance sur la protection des données (OLPD ; RS *235.11*)](http://www.admin.ch/ch/f/rs/c235_11.html) |
|  | Ordonnance sur la transformation numérique et l’informatique (OTNI ; [RS *172.010.58*](https://www.fedlex.admin.ch/eli/cc/2020/988/fr)) |
|  | [Ordonnance sur le traitement des données personnelles et des données des personnes morales lors de l’utilisation de l’infrastructure électronique de la Confédération](https://www.admin.ch/opc/fr/classified-compilation/20111415/index.html) (OTUIC ; RS *172.010.442*) |
|  |  |
| Directive | Directives de l’OFAS (D-SIPD, autres) |
|  |  |
| Stratégie |  |
|  |  |
|  |  |
| Concepts généraux de sécurité |  |
| SLA |  |
| Autres | 🡺 À compléter par l’auteur |

# Classification d’après l’analyse des besoins de protection

La classification de l’objet informatique à protéger doit être réalisée selon l’analyse des besoins de protection.

Les évaluations effectuées lors de l’analyse des besoins de protection permettent aussi d’estimer les éventuelles conséquences financières des besoins en matière de sécurité et de les décrire dans le présent document.

|  |
| --- |
| **Résultat de la classification** |
| **Confidentialité :** | Des données personnelles sont-elles traitées ? Si oui, le risque est-il élevé ? |
| Classification selon les directives internes, par ex. « interne », « confidentiel », etc. |
| Exigences de confidentialité (élevées ou non) |
| **Disponibilité :** | Durée de panne maximale autorisée, par ex. < 2 h, < 8 h, < 12 h, plus de 12 h |
| Perte de données maximale autorisée, par ex. 30 min, 2 h, 24 h |
| Nécessité de la gestion de la continuité des services informatiques (ITSCM), partie intégrante de la gestion de la continuité des activités |
| **Intégrité :**  | L’intégrité est-elle soumise à des exigences particulières ? |
| **Traçabilité :**  | La traçabilité est-elle soumise à des exigences particulières ? |

Résultat de la Schuban : besoin de protection normal ou élevé ?

# Description du système du point de vue de lasécurité

Description condensée des éléments relatifs à la sécurité du système, des applications, des fichiers de données disponibles et traités ainsi que des processus qui s’y rapportent.

## Interlocuteurs et responsabilités

|  |  |
| --- | --- |
| Qui | Nom |
| Personne de contact chez l’OAI |  |
| Personne de contact chez le partenaire contractuel |  |
| DSIO partenaire contractuel |  |
| DSIO de l’OAI |  |
| Autres services |  |

## Description du système global

Description du système dans son ensemble ainsi que des fonctionnalités liées à la sécurité telles que les concepts des rôles, la méthode d’authentification, la sauvegarde, les processus d’assistance et de maintenance (possiblement à distance), le SLA, etc.
Il est aussi possible de faire référence aux documents correspondants (nom, date de création, lieu d’enregistrement, etc.). La description doit être complète et pouvoir être comprise par des personnes non impliquées.

## Description des données à traiter

Description des données et des structures (par ex. base de données utilisée).

Les questions suivantes doivent être clarifiées et exposées lors du traitement de données personnelles :

* Fichier de données annoncé au PFPDT ?

Il s’agit de déterminer si le traitement des données satisfait aux dispositions de la loi fédérale sur la protection des données. Il convient notamment de vérifier si un fichier de données doit être annoncé au PFPDT.

* Un règlement de traitement doit-il être établi ? Consultez à cet égard le [Règlement de traitement](https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/prozesse-methoden/p042-informationssicherheits-und-datenschutzkonzept_ISDS.html) ou l’ordonnance relative à la loi fédérale sur la protection des données (OLPD) ainsi que le document disponible sous le lien suivant : [Guide relatif aux mesures techniques et organisationnelles de la protection des données](https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/mesures-techniques-et-organisationnelles-de-la-protection-des-do.html).
Si oui, renvoyer au document correspondant.
* Existe-t-il une base légale relative au traitement électronique des données ?
* Les données doivent-elles être mises à la disposition des Archives fédérales sous forme électronique ?
* Si les informations sont classifiées, l’OPrI et les [prescriptions de traitement](https://intranet.vbs.admin.ch/de/wissen/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb.detail.document.html/vbs-intranet/de/documents/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb/Bearbeitungsweisungend.pdf.html) doivent être respectées (seulement sur l’intranet et en allemand).
* Si l’objet à protéger est pertinent pour le processus d’audit GRAES, il faut renvoyer au document correspondant.

## Esquisse de l’architecture et matrice de communication

Insérer ici une esquisse de l’architecture et une matrice de communication ou renvoyer au document correspondant tenu à jour.

 



## Description de la technologie sous-jacente

Description des techniques utilisées, telles que plateforme de serveurs, système(s) d’exploitation, environnement système, réseaux utilisés, fonctions cryptographiques, etc. Ces techniques doivent être décrites de manière complète et pouvoir être comprises aussi par des personnes non impliquées. Ou renvoi au document correspondant tenu à jour

# Analyse des risques et mesures de protection

Description des facteurs de risques pertinents (disponibilité, confidentialité, intégrité et traçabilité), liste et évaluation des risques

L’[analyse des risques](https://intranet.ncsc.admin.ch/ncscintra/fr/home/vorgaben-hilfsmittel/sicherheitsverfahren/erhoehter-schutz.html) détaillée doit être effectuée à l’aide du fichier Excel faisant partie du concept. Des remarques sur la façon de le remplir se trouvent dans le document Excel.

Résultats de l’analyse des risques : Les feuilles « Disponibilité », « Confidentialité », « Intégrité », « Traçabilité », « Synthèse » et « Synthèse Radar » sont des graphiques desquels ressort la catégorie du risque évalué.

* Vert : ces risques sont soit inhérents (à l’objet à protéger en tant que tel) ou peuvent être négligés. Ils doivent pouvoir être réduits par des mesures simples.
* Jaune : ces risques ont des conséquences considérables et doivent donc être réduits.
* Rouge : ces risques sérieux ont des conséquences critiques à catastrophiques. Ils doivent impérativement être réduits.

🡺 Les risques qui ne peuvent pas être traités (réduits) ou qui ne peuvent l’être que de manière insuffisante (surlignés en rouge ou en jaune dans la matrice des risques résiduels) doivent être inscrits dans le concept SIPD (chap. 6.1). Il faut les indiquer et informer par écrit le mandant et les responsables des processus d’affaires. La décision d’assumer ou non les risques résiduels connus appartient au responsable de l’unité administrative compétente.

Les risques résiduels doivent aussi être récapitulés brièvement dans le résumé (chap. 2.2).

## Risques résiduels

Il faut insérer ici la grille « Matrice des risques résiduels » provenant de l’analyse des risques.



Il faut fournir dans le tableau qui suit une justification des risques résiduels (surlignés en rouge et en jaune).

|  |  |  |
| --- | --- | --- |
| **N°** | **Risque** | **Justification** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Risques résiduels élevés (rouge)

|  |  |  |
| --- | --- | --- |
| N° du risque | Risque | Évaluation |
|  |  |  |
|  |  |  |
| Mesure(s) |  |
| Degré de mise en œuvre | % | Responsable |  |
| Mise en œuvre |  |
| En attente |  |
| Remarque |  |

### Risques résiduels élevés (jaune)

|  |  |  |
| --- | --- | --- |
| N° du risque. | Risque | Évaluation |
|  |  |  |
| Mesure(s) |  |
| Degré de mise en œuvre | % | Responsable |  |
| Mise en œuvre |  |
| En attente |  |
| Remarque |  |

## Éléments particuliers à prendre en compte

Énumérer les éventuels points pertinents.

# Rétablissement des activités

Un plan d’urgence doit être établi pour les objets à protéger qui soutiennent des processus d’affaires critiques.

Il décrit la planification des cas d’urgence et la prévention des catastrophes de l’objet informatique à protéger afin de garantir le maintien et le rétablissement des activités dans les situations extraordinaires. Une aide est disponible dans le document « P042-Hi03 - Plan d’urgence »[[1]](#footnote-1).

Dans tous les cas, il faut renvoyer aux documents de la BCM au niveau de l’office

# Respect, contrôle et approbation des mesures de protection

Description du règlement d’exécution des révisions et contrôles, annoncés ou non, des activités de sécurité de l’information dans le projet, puis dans l’exploitation.

## Contrôle de la réception du système

Les systèmes, nouveaux ou actualisés, doivent faire l’objet d’un examen et d’un contrôle poussés lors du processus de développement, comprenant la préparation d’une planification approfondie des activités, d’informations sur les tests internes et des dépenses attendues dans différentes conditions. Tout comme pour les projets de développement, ce type d’examens doit tout d’abord être effectué par l’équipe de développement. Ensuite, des examens de réception indépendants doivent être entrepris (pour les projets de développement internes comme pour les projets externalisés) afin de vérifier que le système fonctionne comme prévu (et uniquement comme prévu, voir ISO/IEC 27002:2013, chap. 14.1.1 et 14.1.2). La portée de ces examens doit correspondre à l’importance et à la qualité du système.

Résumé des audits effectués (qui, quand, quoi, résultat).

# Mise hors service

Décrire les points à respecter lors de la mise hors service, tels que la destruction des supports de données, l’annulation des autorisations, l’adaptation des droits d’accès, etc.

# Abréviations

**Définitions, acronymes et abréviations**

|  |  |
| --- | --- |
| Acronymes / Abréviations | Contexte |
| BCM | Gestion de la continuité des activités |
| Concept SIPD | Concept de sécurité de l’information et de protection des données  |
| DSID | Délégué à la sécurité informatique du département  |
| DSIO | Délégué à la sécurité informatique de l’unité d’organisation  |
|  |  |
| NCSC | Centre national pour la cybersécurité |
| OLPD | Ordonnance relative à la loi fédérale sur la protection des données |
| PFPDT | Préposé fédéral à la protection des données et à la transparence |
| RA | Responsable d’application |
|  |  |
| SLA | Service Level Agreement |
| RS | Responsable système |

# Annexe

Ajouter ici les documents complémentaires correspondants tels que, au minimum :

* Analyse des besoins de protection
* Analyse des risques
1. [intranet.ncsc.admin.ch](https://intranet.ncsc.admin.ch/ncscintra/fr/home/vorgaben-hilfsmittel/sicherheitsverfahren/erhoehter-schutz.html) > Directives informatiques & outils > Procédures de sécurité > Protection élevée > P042 - Concept de la sécurité de l’information et de protection des données (SIPD) [↑](#footnote-ref-1)