ISMS

(Information Security Management System)

Politique de File Transfer : directives pour l'échange de fichiers et de documents entre des institutions publiques de la sécurité sociale (IPSS) et des partenaires autorisés.

Version control : Doc. Réf. : 2014.0012					
Release	Status	Date	Written by	Edited by	Approved by
FR_1.00	Final	14/12/2013	Frank Souffriau		Staff Extranet

TABLE DES MATIÈRES

1. Introduction

L'échange de documents à des fins professionnelles est soumis à une série de mesures de sécurité. Conformément aux normes de sécurité minimales de la Banque Carrefour de la sécurité sociale, toute institution doit prendre les mesures de sécurité adéquates afin de se prémunir contre les risques liés à l'échange de documents professionnels. Par échange, il y a lieu d'entendre :

- l'envoi de documents à des institutions de sécurité sociale et à des partenaires autorisés;
- la réception de documents en provenance d'institutions de sécurité sociale ou de partenaires autorisés ;
- la consultation de la liste de documents échangés.

2. Scope

La présente directive comprend les conditions d'utilisation et les directives pour l'utilisation d'une « passerelle électronique » sécurisée pour l'échange de documents (électroniques) professionnels entre les divers groupes-cibles. La présente directive est applicable à toutes les institutions de sécurité sociale.

L'utilisation de la "passerelle électronique" (dans le contexte duquel il est fait référence aux applications reprises dans l'annexe 9.2) est plutôt autorisée en cas exceptionnel et ne sert pas à remplacer les flux d'échange classiques via la BCSS.

3. Groupe-cible (GC)

La présente directive est applicable à toutes les IPSS et à leurs partenaires autorisés, à savoir des entités identifiables à l'aide d'un numéro BCE et ayant une qualité de "professionnels" (cf. UAM BCSS).

- **(GC-1)** L'échange mutuel de documents entre des acteurs du réseau primaire est autorisé moyennant le respect des conditions d'utilisation (voir le point 4).
- **(GC-2)** L'échange mutuel de documents entre des acteurs du réseau primaire et leur réseau secondaire sera évalué au cas par cas (avec éventuellement une restriction dans le temps).
- **(GC-3)** L'échange mutuel de documents entre des acteurs du réseau primaire et des organismes qui ne font pas partie du réseau de la sécurité sociale (tels que SPF ou Communautés), mais qui sont connectés à l'extranet de la sécurité sociale est autorisé moyennant le respect des conditions d'utilisation (voir le point 4).
- **(GC-4)** L'échange mutuel de documents entre des acteurs du réseau secondaire sera également évalué au cas par cas (avec éventuellement une restriction dans le temps).
- **(GC-5)** L'échange mutuel de documents entre des acteurs du réseau primaire et une société privée est autorisé moyennant le respect des conditions d'utilisation (voir le point 4).
- **(GC-6)** L'échange mutuel de documents entre des acteurs du réseau secondaire et une société privée sera évalué au cas par cas.
- **(GC-7)** L'échange mutuel de documents entre deux sociétés privées n'est pas autorisé.
- **(GC-8)** L'échange mutuel de documents entre deux services d'une même entité n'est pas soutenu. Il appartient dès lors à l'entité d'organiser l'échange de documents entre ses services.

4. Conditions d'utilisation

- **Toute** demande d'utilisation de l'application « FILEEXCHANGE » (Ref. tableau de synthèse 9.2 , p 6) doit être soumise à l'approbation de la BCSS. Pour ce faire, il y a lieu de remplir et signer le formulaire "**Demande d'autorisation pour un flux d'échange de documents**". Ce formulaire peut être obtenu par envoyer un e-mail vers security@ksz-bcsss.fgov.be.
- La taille (Mb) des fichiers à échanger est limitée en fonction de la solution utilisée, comme indiqué dans le tableau de synthèse 9.2.
- Il y a lieu d'utiliser le système d'identification et d'authentification propre à la solution utilisée, comme indiqué dans le tableau de synthèse 9.2.
- Dans la mesure où il est fait usage du système UAM géré par la BCSS, les qualités utilisées doivent relever de la catégorie « professionnels ».
- Les documents échangés seront supprimés 3 mois après la date d'échange.

5. Directives

Ci-après figurent les directives à respecter afin de garantir la sécurité de l'information lors de l'échange de documents professionnels entre des institutions et des partenaires autorisés.

Cette directive est liée aux normes minimales et doit effectivement être appliquée par l'institution. L'utilisateur final doit être sensibilisé aux risques liés à l'échange de documents professionnels (sensibles).

Il appartient aux institutions de sécurité sociale d'adapter la politique de sécurité à leur situation spécifique et au volume des ressources de l'entreprise à protéger.

5.1. Généralités

1. La politique de sécurité de l'information de l'institution reste intégralement applicable dans ce contexte.
2. La présente directive vaut pour tous les utilisateurs concernés par l'échange de documents professionnels.
3. L'utilisation de la solution de "file transfer" doit être limitée à des fins professionnelles dans le cadre de la fonction exercée par l'utilisateur. Cette solution ne peut être utilisée à des fins privées.
4. Le niveau de sécurité requis pour l'échange de documents dépend de la nature et de la sensibilité des données / informations auxquelles il est potentiellement donné accès.
5. Le niveau de sécurité du traitement et de l'enregistrement des documents doit être proportionnel à la nature et à la sensibilité des données.
6. L'institution doit avoir la garantie que les partenaires autorisés avec lesquels des documents sont échangés disposent d'un niveau de sécurité similaire à celui de l'institution.
7. L'institution s'engage à sensibiliser les utilisateurs aux bonnes pratiques et à attirer leur attention sur leur responsabilité lors de l'échange de documents professionnels.
8. L'institution s'engage à respecter la vie privée de l'utilisateur.
9. Toute partie concernée par l'envoi, tant le destinataire que la personne intermédiaire ou l'expéditeur, doit prendre les mesures adéquates, dans les meilleurs délais, pour le traitement des messages de suivi.
10. Toute anomalie ou lacune lors de l'envoi électronique de documents doit être signalée dans les meilleurs délais aux parties concernées (destinataire, intermédiaire, expéditeur).
11. L'échange de documents professionnels, nécessaire à l'application et à l'exécution de la sécurité sociale, doit être protégé au moyen d'un système d'identification, d'authentification et d'autorisation.

12. Des mesures adéquates doivent être prises lorsque des données à caractère personnel sont enregistrées sur des supports susceptibles de quitter le périmètre sécurisé de l'institution.

5.2. Organisation

1. Le service compétent de l'institution est responsable de la mise en œuvre correcte de la directive de sécurité en matière d'échange de documents professionnels.
2. Le support par l'institution concerne uniquement les ressources mises à la disposition par l'institution. Ce support peut être confié à un tiers.
3. L'institution aura toujours la possibilité de bloquer l'accès aux documents de l'institution (données présentes sur les systèmes et/ou ressources de l'institution) et d'effacer des données.

5.3. Directive de sécurité

1. Comme précisé au point 5.1, le niveau de sécurité requis dépend de la nature et de la sensibilité des documents. Toute partie concernée par l'envoi, tant le destinataire que l'intermédiaire ou l'expéditeur, doit prendre les mesures adéquates lors de l'échange de documents.
2. L'échange de documents entre des institutions de sécurité sociale et leurs partenaires autorisés doit être protégé au moyen de mesures de gestion adéquates.
3. Les policies de sécurité au sein de la sécurité sociale doivent être respectées, notamment les policies dans les domaines suivants, conformes aux normes ISO 27002:
    - l'organisation de la sécurité,
    - la classification et la gestion des ressources,
    - la sécurité physique et la sécurité de l'environnement,
    - la gestion opérationnelle,
    - la sécurité d'accès logique,
    - le développement et la maintenance de systèmes,
    - la gestion de la continuité,
    - le respect des policies.

6. Sanctions

Le non-respect de la présente directive donnera lieu à une sanction conformément au règlement en vigueur au sein de l'institution.

7. Propriétaire du document

Le maintien, le suivi et la révision de la présente directive relèvent de la responsabilité du service Sécurité de l'information de la BCSS.

8. Références

Les références utilisées sont :

- les normes de sécurité minimales 2011 de la BCSS
- la norme ISO 27002 : 2005.

9. Annexes

9.1. Lien avec la norme ISO 27002

Ci-après nous indiquons les principales clauses de la norme ISO 27002 qui ont un rapport avec l'objet de la présente directive.

Norme ISO 27002	
Directive de sécurité	Oui
Organisation de la sécurité de l'information	Oui
Gestion des ressources d'entreprise	Oui
Exigences de sécurité relatives au personnel	Oui
Sécurité opérationnelle	Oui
La protection de l'accès logique	Oui
Sécurité d'accès logique	Oui
Maîtrise des incidents de sécurité	Oui
Protection de l'information dans le cadre de la continuité de l'entreprise	Oui

9.2. Tableau de synthèse des solutions recommandés pour l'échange de documents entre des institutions de sécurité sociale et de partenaires autorisés

Nom de l'application	**« Secure FTP »**	**« ISSFTP »**	**« ELARA »**	**« FILEEXCHANGE »**
Group Cible (GC) (voir le Chapitre 3 de ce document)	GC-3, GC-4, GC-5 et GC-6	GC-1 et GC-2	GC-3 et GC-2	GC-2, GC-4, GC-5 et GC-6
Protocole	SFTP	FTP	FTP	HTTPS
Identification	Clé publique/Clé privée + UserID /Password	User ID/Password	User ID/Password	WebApp sécurisée par le UserManagement
Couche de sécurité	1.2	2.1	2.1	1
Capacité	Peut contenir 1.000.000 fichiers (chiffres indicatifs) 80 GB	Peut contenir 1.000.000 fichiers (chiffres indicatifs) 80GB	Peut contenir 700.000 fichiers (chiffres indicatifs) 40GB	10 MB par envoi
SLA	NON	NON	NON	NON
Buts	Echange de fichiers de données	Echange de fichiers de données	Echange de fichiers de données	Echange ponctuel de documents et de données