Politique relative à la sécurité et à la confidentialité de l'information

Utilisation d'internet comme moyen d'accès au réseau de la Banque Carrefour de la Sécurité Sociale dans le cadre du traitement de données à caractère personnel par les acteurs du secteur social

(BLD BCSS)

TABLE DES MATIERES

1. Introduction

Le présent document fait partie intégrante de la méthodologie relative à la sécurité et à la confidentialité de l'information dans la sécurité sociale. Il est destiné aux responsables, aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de la sécurité sociale (IPSS).

L'utilisation d'internet comme moyen d'accès au réseau de la Banque Carrefour de la Sécurité Sociale (BCSS) en dehors de l'infrastructure de l'extranet constitue un risque majeur qui doit faire l'objet d'une politique de sécurité stricte et rigoureuse.

Cette politique s'inscrit dans le cadre de la stratégie relative à la sécurité et à la confidentialité du réseau de la sécurité sociale énoncée dans le document "Normes minimales" et approuvée par le Comité Général de Coordination de la Banque Carrefour de la Sécurité Sociale.

Le présent document offre des indications générales concernant l'utilisation d'internet pour accéder au réseau de la BCSS dans le cadre du traitement de données à caractère personnel par les acteurs du secteur social. Cette politique s'applique uniquement aux acteurs du secteur social qui, dans le cadre du traitement de données à caractère personnel, ne sont pas connectés à l'extranet de la sécurité sociale et peuvent démontrer qu'ils sont dans l'impossibilité de s'y connecter.

2. Accès au réseau de la BCSS via internet

Toute organisation souscrit à la politique suivante relative à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité :

2.1. Généralités

L'utilisation d'internet comme moyen d'accès au réseau de la Banque Carrefour de la Sécurité Sociale (BCSS) constitue une exception au principe général de l'accès via l'extranet de la sécurité sociale. Cette utilisation doit faire l'objet d'une demande d'autorisation et de dérogation écrite auprès du fonctionnaire dirigeant de la Banque Carrefour de la Sécurité Sociale.

2.2. Contenu de la demande

La demande d'autorisation et de dérogation doit justifier des motivations à ne pas utiliser l'extranet de la sécurité sociale ou les réseaux privatifs sécurisés ainsi qualifiés par la BCSS et décrire précisément les mesures prises au sein de l'organisation pour réduire les risques de sécurité inhérents à l'usage du protocole Internet.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2004	JMG	V2004	Première version	16/11/2004	16/11/2004
2005	JMG	V2005	Deuxième version	14/02/2005	14/02/2005
2005	JMG	V2005	Troisième version	28/02/2005	28/02/2005
2017		V2017	Intégration EU GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si des erreurs ou des problèmes sont constatés à la lecture du présent document, vous êtes prié en tant que lecteur de transmettre au conseiller en sécurité de la sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'institution une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement à vos données de contact.

Définitions

Dans un souci de cohérence de la terminologie et des concepts utilisés dans tous les documents de politique, toutes les définitions relatives à la sécurité et à la confidentialité de l'information sont centralisées dans un document intitulé "Définitions relatives à la sécurité et à la confidentialité de l'information".

Annexe B : Références

Ci-dessous figurent des documents qui ont servi d'inspiration au présent document.

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 pages
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 pages

Ci-dessous figurent des références aux sites web qui ont servi d'inspiration au présent document.

- https://www.iso.org/fr/isoiec-27001-information-security.html
- https://www.iso.org/fr/standard/54534.html
- https://www.iso.org/fr/standard/54533.html
- http://www.ccb.belgium.be/fr
- https://www.ksz-bcss.fgov.be/fr

Annexe C : Extranet de la sécurité sociale

L'extranet de la sécurité sociale est un réseau IP sécurisé ayant pour fonction l'interconnexion des différentes organisations de la sécurité sociale, ainsi que la fourniture d'un certain nombre de services communs tels que l'interconnexion sécurisée de réseaux hétérogènes, la mise à disposition de proxies HTTP/FTP, l'échange de messages et d'informations, le scanning antivirus du trafic HTTP/FTP/SMTP, l'hébergement de sites web, la gestion et la maintenance de noms de domaines et l'accès à des ressources internes via dial-up ou VPN.

La protection de l'infrastructure répartie sur deux sites et basée sur une sécurité en couches est assurée par des firewalls installés sur chaque connexion entrante, à savoir, d'une part, entre l'institution et le backbone et, d'autre part, entre le backbone et internet et entre le backbone et les réseaux privés ; une gestion centralisée des protections antivirus y est également assurée.

L'extranet de la sécurité sociale s'est doté un système d'IDS (Intrusion Detection System) consolidé par une analyse permanente des logs au travers d'un MSS (Management Security Services).

L'infrastructure et ses composants font l'objet d'audits périodiques.

Annexe D : Conditions d'accès à l'extranet de la sécurité sociale par internet

L'utilisation d'internet comme moyen d'accès au réseau de la Banque Carrefour de la Sécurité Sociale est autorisée sous réserve d'une autorisation explicite et écrite de la Banque Carrefour de la Sécurité Sociale et de la stricte application des exigences suivantes :

1. Niveau autorisation d'accès

- L'autorisation accordée n'est jamais globale ; elle ne porte que sur le système ou la transaction visée lors de la demande.
- Dans le cadre de l'utilisation de données sociales à caractère personnel, la demande précisera distinctement s'il s'agit d'un accès dans le cadre de la communication ou de la consultation de données sociales ; lorsqu'il s'agit d'une consultation, le dossier de demande décrira précisément la finalité recherchée.
- Les transactions ou les systèmes accédés lorsqu'elles contiennent des données sociales à caractère personnel doivent être protégés par un système d'autorisation d'accès au travers du User Management Ambtenaar Fonctionnaire (UMAF).
- Les utilisateurs concernés sont des personnes physiques nommément désignées par le fonctionnaire dirigeant de l'institution.

La gestion de ces autorisations est assurée par un gestionnaire local dûment mandaté à cette tâche par le fonctionnaire dirigeant de l'organisation.

2. Niveau identification / authentification

Le processus d'identification et d'authentification doit appliquer sans restriction le règlement des utilisateurs tel que repris en page d'accueil du portail de la sécurité sociale (https://www.socialsecurity.be).
Le processus d'identification et d'authentification sera fonction du niveau de confidentialité des données traitées par la transaction ou le système concerné ainsi que du cadre de la communication ou de la consultation des données sociales.
L'accès à la transaction ou au système par l'Internet sera activé après un avis favorable de la Banque Carrefour de la sécurité sociale qui précisera dans sa délibération le processus d'identification / authentification à mettre en place.

Dans tous les cas ce processus sera composé au minimum :

- d'une identification par un user ID ;
- d'une authentification par l'usage d'un mot de passe, du token fonctionnaire ou de la carte d'identité électronique.

Dans le cas d'une liaison par transfert de fichier, l'usage d'un certificat pourra être exigé. Le type de certificat sera défini de commun accord avec la BCSS.

3. Traçabilité

L'activation des logs à caractère sécuritaire est obligatoire et doit être conforme au respect de la norme minimale de sécurité énoncée par le groupe de travail "Sécurité de l'information".

4. Restrictions

- L'usage de l'Internet dans le cadre du mode application à application est interdit.
- La disponibilité du réseau Internet n'est pas de la responsabilité du réseau de la Banque Carrefour de la sécurité sociale.
- Seul le protocole HTTPS (encapsulation du protocole HTTP dans SSL) est autorisé.

5. Liaison par transfert de fichier

L'activation de l'échange de données par transfert de fichiers via l'Internet est conditionné par :

- l'autorisation explicite de la Banque Carrefour de la Sécurité Sociale ;
- l'utilisation d'un protocole de transfert sécurisé qualifié par le réseau Banque Carrefour de la Sécurité Sociale ;
- l'utilisation d'un processus d'identification / authentification fort qualifié par le réseau de la Banque Carrefour de la Sécurité Sociale.

Annexe E : Lien avec la norme ISO 27002:2013

Nous renvoyons ici à la (aux) clause(s) principale(s) de la norme ISO 27002:2013 relative à l'objet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Personnel sûr	
Gestion des moyens d'exploitation	
Sécurisation des accès	**Oui**
Cryptografie	**Oui**
Sécurité physique et de l'environnement	
Sécurisation des processus	
Sécurité de la communication	**Oui**
Achats, maintenance et développement de systèmes d'information	
Relations fournisseurs	
Gestion des incidents de sécurité	
Aspects de sécurité de l'information de la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****