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

Sécurité de la gestion des accès des portails

(BLD PORTAL)

TABLE DES MATIERES

1. INTRODUCTION 3

2. SECURITE DE LA GESTION DES ACCES DES PORTAILS 3

ANNEXE A : GESTION DU DOCUMENT 4

ANNEXE B : REFERENCES 4

ANNEXE C : LIEN AVEC LA NORME ISO 27002:2013 5

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).

Cette politique décrit les modalités d'accès pour les personnes désignées comme gestionnaires ou co-gestionnaires des droits d'accès au portail de la sécurité sociale. Octroyer des droits d'accès signifie donner accès à tout ou partie des systèmes d'information des organisations impliquées dans le développement de ces portails, notamment :

- gérer un compte utilisateur sur le portail de la sécurité sociale ;
- gérer un rôle de co-gestionnaire en tant que gestionnaire ;
- gérer les accès aux différentes applications et transactions ;
- gérer les accès aux environnements.

La fonction de gestionnaire ou co-gestionnaire est une mission de confiance nécessitant une grande honnêteté et un strict respect des obligations de la fonction.

2. Sécurité de la gestion des accès des portails

Toute institution 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.

Toute organisation qui souhaite utiliser les services et applications du portail de la sécurité sociale au profit de ses utilisateurs est tenue de désigner au moins un gestionnaire d'accès. La fonction de gestionnaire ou de co-gestionnaire des portails est attribuée par la personne chargée de la gestion journalière de l'organisation, suivant une procédure déterminée.

À défaut, le conseiller en sécurité de l'information (CISO) est le gestionnaire de l'organisation ; il est l'intermédiaire privilégié entre l'organisation et le service de sécurité de la Banque Carrefour de la Sécurité Sociale (BCSS). Outre le respect, le conseiller en sécurité de l'information doit amener les collaborateurs à lire et appliquer les règlements relatifs à l'utilisation des systèmes d'information des portails.

La fonction de gestionnaire ou de co-gestionnaire comprend au minimum les éléments suivants :

1. Le rôle de gestionnaire ou de co-gestionnaire est nominatif et ne peut pas, même temporairement, être cédé à un tiers.
2. L'octroi des accès aux portails et à leurs services au profit des utilisateurs de l'organisation est une procédure déterminée et validée par la personne chargée de l'administration journalière.
3. L'octroi de droits d'accès individuels aux utilisateurs de l'organisation doit obligatoirement être limité aux applications nécessaires à l'exécution de leurs tâches spécifiques.
4. La communication ou la modification de comptes utilisateur s'effectuent suivant une procédure déterminée.
5. Lors de la rupture de la mission d'un collaborateur en qualité de gestionnaire ou de co-gestionnaire, le conseiller en sécurité de l'information agréé de l'organisation doit immédiatement prendre toutes les mesures nécessaires pour supprimer les accès de ce collaborateur et assurer le suivi de sa succession. En outre, le conseiller en sécurité de l'information agréé doit formellement informer le service de sécurité de la BCSS avec ratification formelle par la personne chargée de l'administration journalière de l'organisation.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2003	JMG	V2003	Première version	12/12/2003	12/12/2003
2004	JMG	V2004	Deuxième version	02/04/2004	02/04/2004
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
- ISO, "ISO/IEC 29146:2016 Security techniques – A framework for access management", juni 2016, 35 blz.
- ISO, "ISO/IEC 24760:2011 Security techniques – A framework for identity management", December 2012, 20 blz.
- ISACA, "COBIT 5 for Information Security", Mei 2012, 220 blz.

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
- https://www.iso.org/fr/standard/45169.html
- https://www.iso.org/fr/standard/57914.html
- http://www.isaca.org/cobit
- https://www.ksz-bcss.fgov.be/fr
- http://www.ccb.belgium.be/fr
- https://www.safeonweb.be/fr

Annexe C : 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**
Cryptographie	
Sécurité physique et de l'environnement	
Sécurisation des processus	
Sécurité de la communication	
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 *****