Politique de sécurité de l'information et protection de la vie privée

Réseaux sans fil

(BLD WIREL)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie de sécurité de l'information et protection de la vie privée au sein de la sécurité sociale. Ce document est destiné aux responsables et 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 sécurité sociale (IPSS).

Ce document décrit les directives en matière de sécurité de l'information et de protection de la vie privée en ce qui concerne les réseaux sans fil.

2. Réseaux sans fil sécurisés

Toute organisation souscrit les directives suivantes relatives à la sécurité de l'information et à la protection de la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

1. L'organisation doit gérer et contrôler les réseaux sans fil afin de limiter l'accès au réseau et l'utilisation du réseau et afin de protéger les informations présentes dans les systèmes et applications qui sont envoyées à travers des réseaux sans fil.
2. L'organisation doit respecter les directives qui sont décrites dans l'annexe C de la politique « réseaux sans fil sécurisés »

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2003		V2003	Première version	10/09/2003	1/10/2003
2004		V2004	Deuxième version	11/02/2004	1/12/2004
2017		V2017	Intégration UE GDPR	7/03/2017	7/03/2017

Erreurs et omissions

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

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- ISO, "ISO/IEC 27033:2016 Security techniques - Network security Part 6 securing wireless IP network access", juin 2016, 26 p.
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 p.
- ISACA, "Mobile Computing security audit/assurance program", octobre 2010,23 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le 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/51585.html
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
- https://www.enisa.europa.eu/topics/data-protection
- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Mobile-Computing-Security-Audit-Assurance-Program.aspx
- http://www.cnt-nar.be/CAO-COORD/cao-081.pdf
- https://www.cybersimpel.be/fr

Annexe C: Directives en matière de sécurité de l'information en ce qui concerne les réseaux sans fil

Ces directives doivent être appliquées à tous les réseaux sans fil que l'organisation a sous sa gestion à tous les endroits.

1. Les réseaux sans fil à usage interne donnent directement accès aux systèmes internes de l'organisation.
2. Les réseaux sans fil destinés aux visiteurs donnent uniquement accès à internet.
3. Les réseaux sans fil à usage spécial sont uniquement mis en place suite à une requête spéciale lorsque les deux autres types de réseaux sans fil s'avèrent insuffisants.
4. L'organisation doit disposer d'un processus pour la mise à jour de l'aperçu des réseaux sans fil existants et autorisés, des protocoles de sécurité y afférents et de toutes les mesures de sécurité de l'information y relatives.
5. Le service ICT doit périodiquement contrôler le réseau quant à l'existence de réseaux sans fil non autorisés et l'application des protocoles et mesures de sécurité de l'information implémentées.
6. L'organisation doit disposer de procédures pour la mise en place de réseaux sans fil conformément aux présentes directives de sécurité.
7. Pour les réseaux sans fil qui donnent directement accès aux systèmes internes de l'organisation, il doit être fait usage du chiffrement le plus fort.
8. Pour les réseaux sans fil qui donnent directement accès au réseau interne de l'organisation, le « SSID broadcasting » doit être désactivé.
9. Les algorithmes de chiffrement faibles ou vulnérables ne peuvent pas être utilisés.
10. Les utilisateurs de réseaux sans fil destinés aux visiteurs sur lesquels le chiffrement n'est pas actif sont informés des risques y afférents.
11. Les réseaux sans fil destinés aux visiteurs et les réseaux sans fil qui donnent directement accès aux systèmes internes de l'organisation doivent être logiquement séparés.
12. Les réseaux sans fil destinés aux visiteurs peuvent uniquement donner accès à internet et aux services internet de l'organisation. Un accès direct aux systèmes internes de l'organisation n'est pas autorisé.
13. Les méthodes d'authentification pour l'accès aux réseaux sans fil (hormis les réseaux sans fil pour les visiteurs) doivent être basées sur une authentification forte.
14. Les réseaux sans fil doivent faire l'objet d'un monitoring permettant de détecter tout abus ou toute tentative d'accès non-autorisé.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	**Oui**
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	**Oui**
Cryptographie	
Sécurité physique et environnementale	**Oui**
Protection des processus	
Sécurité de la communication	**Oui**
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

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