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

Respect

(BLD COMPLY)

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).

Le présent document décrit les politiques relatives au respect des exigences légales, réglementaires, statutaires et contractuelles de la sécurité et de la confidentialité de l'information. Il décrit en outre les politiques relatives à la vérification de la conformité de l'implémentation de la sécurité et de la confidentialité de l'information avec les attentes de la direction de l'organisation.

2. Respect

Toute institution souscrit aux politiques suivantes relatives à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité.

1. L'organisation doit périodiquement mener un audit de conformité concernant l'état de la situation de la sécurité et de la confidentialité de l'information comme décrit dans les politiques[1].
2. L'organisation doit éviter la violation de toute disposition légale, réglementaire, statutaire ou contractuelle relative à la sécurité et à la confidentialité de l'information.
3. L'organisation doit s'assurer que la politique de sécurité et de confidentialité de l'information est implémentée conformément aux attentes de la direction.
4. L'organisation doit prévoir une procédure disciplinaire formelle pour les travailleurs qui violent la politique de sécurité et de confidentialité de l'information.

1 Suivant les bonnes pratiques d'application, un tel audit devrait être organisé une fois par an au moins. Il n'est pas exclu que le conseiller en sécurité d'une organisation réalise un audit auprès d'une autre organisation du même réseau. Si l'institution de gestion d'un réseau secondaire n'a pas une vue claire sur l'état de la situation de la sécurité et de la confidentialité de l'information de l'un de ses membres, elle peut demander au Comité sectoriel de réaliser un audit de conformité.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2003		V2003	Première version	10/09/2003	01/10/2003
2004		V2004	Deuxième version	11/02/2004	01/12/2004
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
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 pages

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

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

Annexe C : Consignes concernant le respect

Identification de la législation et de la réglementation applicables ainsi que des exigences statutaires et contractuelles

- Des responsabilités et des contrôles spécifiques doivent être définis et documentés.
- Le conseiller en sécurité doit veiller à ce que les tendances en évolution soient intégrées dans le développement ou l'adaptation de politiques et procédures.

Droits de propriété intellectuelle (Intellectual Property Rights of IPR)

- Le software qui supporte des applications business opérationnelles doit soit être développé dans l'organisation, soit être acheté/loué auprès d'un tiers connu et fiable (développeur software).
- Il n'est pas autorisé d'utiliser un software publiquement disponible (également connu sous l'appellation shareware ou freeware), excepté sur la base d'une évaluation par le service ICT et en concertation avec le conseiller en sécurité.
- Le software de tiers, utilisé par l'organisation, ne peut pas être copié, excepté moyennant une autorisation explicite dans le contrat de licence et l'approbation de la direction ou pour des raisons de continuité.
- Le software que l'organisation met à disposition ne peut pas être copié sur un moyen de stockage, transféré vers un autre ordinateur, ni être mis à la disposition de parties externes à l'organisation sans l'accord explicite du service ICT.
- Une sensibilisation aux politiques destinées à protéger l'IPR (software, documents, droits de conception, trademarks, brevets et licences de code source) doit être entretenue, et les ressources sur lesquelles repose l'IPR doivent être identifiées.
- Le matériel de preuve de la "propriété" des licences doit être conservé.
- Des contrôles doivent permettre de vérifier si le nombre maximal d'utilisateurs autorisé défini dans le contrat de licence est respecté.
- Il faut s'assurer que seuls des logiciels autorisés et des produits sous licence sont utilisés.
- Une politique doit être établie pour la cessation ou le transfert de software.
- Il faut une conformité avec les conditions générales de vente pour le software ainsi que pour les informations obtenues via des réseaux publics.
- Sauf autorisation par la législation sur le copyright, les livres, articles, rapports ou autres documents ne peuvent être copiés ni en tout ni en partie.

Protection des documents de l'organisation

- Pour la protection de documents d'entreprise, il faut tenir compte de la classification correspondante sur la base du schéma de classification de l'organisation.
- Les documents doivent être catégorisés selon leur type. Il peut s'agir de documents comptables, de logs de transaction, de logs d'audit, de procédures opérationnelles, chacun avec les données correspondantes sur la période de rétention.
- Les données doivent être stockées et traitées conformément aux spécifications du fournisseur.
- En cas de stockage sur des supports électroniques, des procédures doivent être prévues pour garantir l'accès aux données durant toute la période de rétention, même lors d'un changement de technologie.
- Un schéma de rétention doit indiquer la période de rétention des données.
- Le système de stockage doit assurer l'identification des données et des périodes de rétention ainsi que la destruction adéquate des données à la fin de la période de rétention.
- Des consignes doivent exister concernant la rétention, le stockage, le traitement et la destruction des données.

Protection des données et confidentialité des données à caractère personnel

- Un délégué à la protection des données (DPO) doit être désigné pour accompagner les dirigeants, utilisateurs et prestataires de services dans leurs responsabilités individuelles et les procédures à suivre dans le cadre de la protection des données à caractère personnel (confidentialité).
- Des mesures techniques et organisationnelles doivent être implémentées pour protéger les données à caractère personnel.

Prescriptions pour l'utilisation de mesures de gestion cryptographiques

- Un avis juridique doit être recueilli à propos des limites concernant l'importation ou l'exportation de hardware et de software pour l'exécution de fonctions cryptographiques et l'utilisation du chiffrement.

Évaluation indépendante de la sécurité et de la confidentialité de l'information

- La direction peut demander une vérification indépendante par un audit interne ou une partie spécialisée externe afin de garantir l'adéquation et l'efficacité de l'approche de la sécurité et de la confidentialité de l'information pour l'organisation.
- Si les objectifs relatifs à la sécurité et à la confidentialité de l'information ne sont pas réalisés ou si la conformité avec les politiques de sécurité et de conformité de l'information n'est pas atteinte, des actions correctives doivent être entreprises.

Respect de la politique et des procédures de sécurité de l'information

- Les dirigeants doivent préciser comment vérifier la conformité avec la politique de sécurité de l'information dans leurs domaines de responsabilité.
- En cas de non-conformité, les dirigeants doivent :
  - identifier les causes de la non-conformité
  - évaluer la nécessité d'entreprendre des actions pour garantir le respect
  - entreprendre des actions correctives appropriées
  - vérifier l'efficacité des actions correctives et identifier les écarts ou les lacunes
  - enregistrer les résultats des actions correctives mises en œuvre

Vérification de la conformité technique

- La conformité technique doit être garantie par des outils automatisés qui génèrent des rapports techniques, lesquels doivent ensuite être interprétés par un spécialiste technique.
- Des tests d'intrusion ou des évaluations des lacunes des systèmes d'information doivent être planifiés, documentés et exécutés exclusivement par des collaborateurs autorisés et compétents.

Mesures disciplinaires

- Les politiques de sécurité et de confidentialité de l'information doivent être portées à la connaissance du personnel de l'organisation. Le personnel doit pouvoir facilement accéder aux politiques et doit en outre être sensibilisé à ses obligations en matière de sécurité et de confidentialité de l'information.
- Le non-respect des politiques et des procédures y afférentes - qui ont été portées à la connaissance du personnel - peut conduire à des sanctions, voire à des poursuites judiciaires.
- Tout collaborateur invité à exécuter une activité contraire à cette politique doit au plus vite introduire une réclamation écrite ou orale auprès du dirigeant du service ou auprès de tout autre dirigeant, ou encore auprès du conseiller en sécurité.

Annexe D : 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	
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	**Oui**

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