Ligne directrice: sécurité de l'information et vie privée

Clean desk et clear desk

(BLD CLEAR)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie de sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, 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 responsabilités du collaborateur en ce qui concerne le maintien de contrôles physiques efficaces d'accès aux informations disponibles au sein de l'organisation. A savoir, comment le collaborateur doit-il gérer, en toute sécurité, les informations physiques et les outils informatiques mis à sa disposition, afin de garantir une protection optimale des informations de l'organisation. Quelles sont les mesures de protection à prendre sur le poste de travail afin de se protéger contre des accès non autorisés aux informations.

Le « Clean desk » n'est pas équivalent au « Clear desk »:

- En effet, la directive du « Clean desk » exige que tout sur le bureau soit rangé et conservé en un endroit sûr. Ce qui permet de partager des bureaux physiques avec plusieurs collaborateurs (« flexdesk »).
- La directive du « Clear desk » revient à dire que tout ne doit pas nécessairement être enlevé du bureau. Mais il est par contre obligatoire que toute information à caractère sensible ne soit pas sujette à un accès non autorisé. Toute donnée sensible ne peut pas demeurer sans surveillance sur le bureau.

2. Clean desk & Clear desk

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

2.1. Accès à l'information

Tout collaborateur joue un rôle crucial pour empêcher tout accès illicite aux informations sensibles. Ceci est valable tant au niveau de l'accès aux systèmes d'information et d'applications qu'au niveau de l'accès physique aux locaux ou aux documents. La collaboration de l'ensemble des collaborateurs est essentielle à la sécurité de l'information et à la vie privée.

Un système d'accès (physique ou logique) a été implémenté afin d'éviter tout accès non autorisé à l'organisation. L'accès est sécurisé par un dispositif d'accès précis. L'utilisateur peut obtenir des informations confidentielles et sensibles durant l'exécution de ses tâches journalières et les placer autre part où le dispositif d'accès ne fonctionne plus ou n'est pas applicable.

L'utilisateur demeure responsable des informations, sous quelque forme que ce soit. L'utilisateur doit donc veiller à la bonne protection de celles-ci. Dès que les informations ne sont plus utilisées par l'utilisateur, ce dernier doit aussi veiller à leur archivage ou à leur destruction.

2.2. Rapports, évaluation et campagne de sensibilisation

Pour ces normes minimales, les aspects suivant devront être exécutés:

- Tout collaborateur est régulièrement sensibilisé à l'importance de l'accès aux informations. Une campagne de sensibilisation ou une session d'information relative à la sécurité de l'information et à la vie privée doit être organisée, validée, communiquée et suivie au moins une fois par an.
- Une évaluation annuelle relative au respect de la présente politique dans la pratique est organisée une fois par an (au moyen d'une enquête interne).

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2013		V2013	Eerste versie	31/01/2013	01/02/2013
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

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 détaillant la politique à suivre, 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 normes minimales 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”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- http://www.iso.org/iso/iso27001
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.isaca.org/cobit
- https://www.enisa.europa.eu/topics/data-protection
- https://www.sans.org/security-resources/policies/general/pdf/clean-desk-policy
- http://ccb.belgium.be/nl/work
- https://www.safeonweb.be/nl
- https://www.safeinternetbanking.be
- https://www.cybersimpel.be/nl

Annexe C: Directives relatives au clean desk & clear desk

L'application de la politique « Clean Desk, du bureau propre et de l'écran vide » permet de réduire le risque d'accès non autorisé ou d'endommagement des supports, papiers ou autres, et des moyens de traitement de l'information.

Les normes minimales relatives à la sécurité de l'information et à la vie privée visent à appliquer une protection appropriée sur le lieu de travail du travailleur.

- Améliorer la propreté au sein de l'institution.
  - Lorsque les bureaux sont rangés ou tous les espaces de travail sont libres de papier et de désordre, les collaborateurs se sentent plus à l'aise en terme de confort et les invités ont une impression positive de l'institution.
- Améliorer la protection de données confidentielles.
  - Une grande partie de l'information traitée par l'institution est confidentielle et doit être protégée contre des accès non autorisés.
  - Les documents contenant des informations sensibles que l'on souhaite imprimer doivent immédiatement être enlevés des imprimantes. Il est éventuellement possible de protéger l'impression de documents au moyen d'un code personnel.
  - Tous les documents contenant des informations sensibles (p.ex. données confidentielles, informations relatives au client, ...) doivent être rangés de sorte qu'ils soient uniquement accessibles aux collaborateurs compétents.
  - Les documents contenant des informations sensibles qui ne doivent plus être conservés et que le travailleur souhaite détruire, doivent être détruits d'une manière sécurisée. Les supports contenant des informations sensibles qui ne doivent plus être conservés doivent être détruits de la sorte que la confidentialité des informations reste garantie.
  - Les locaux d'archives dans lesquels sont archivés des documents confidentiels doivent toujours être fermés à clé.
- Améliorer la productivité.
  - Un bureau rangé augmentera la productivité car moins de temps sera perdu lors de la recherche de documents.
  - L'application de cette politique permet de partager les bureaux entre plusieurs collaborateurs (« flexdesk »).

Dans la pratique

Les directives du « Clean desk » encouragent l'application de trois règles de base:

1. Quand le collaborateur est présent à son bureau: le collaborateur tâche de garder uniquement sur son bureau les documents dont il a besoin pour la journée.
2. Quand le collaborateur quitte temporairement son bureau: si le collaborateur est fréquemment attendu à des réunions, il doit vérifier s'il n'y a pas de données confidentielles présentes sur son bureau qui pourraient être sans surveillance. Si tel est le cas, il doit les mettre en lieux sûrs. Par ailleurs, il doit également s'assurer de mettre son ordinateur en mode veille, sécurisé par un mot de passe en cas de longue absence.
3. Quand le collaborateur quitte son bureau: il lui incombe de s'assurer que tous les documents sensibles sont placés dans un lieu sûr tel qu'une armoire fermée à clé et que son bureau est rangé avant de quitter l'institution. Une deuxième clé doit par conséquent être mise à la disposition d'un autre service ou collaborateur afin de permettre l'accès aux documents en cas de besoin. C'est la responsabilité des utilisateurs de prendre les mesures de protection nécessaires au sein de leur bureau. Les responsables du traitement doivent vérifier que leurs collaborateurs respectent cette politique.

Quelques conseils pratiques pour un bureau rangé et à l'abri de tout risque:

- Inscrivez le rangement du bureau et des papiers dans votre agenda à des intervalles réguliers.

- En cas de doute concernant la conservation d'un papier ou d'un document, il est généralement préférable de tout simplement le jeter.
- Vérifiez régulièrement que les affaires se trouvant sur le bureau sont encore nécessaires.
- Rangez toujours le bureau avant de le quitter le soir.
- Fermez les armoires d'archives à clé à la fin de la journée de travail.
- Rangez toujours les ordinateurs portables dans un endroit sûr, conformément à la norme minimale relative aux ordinateurs portables.
- Utilisez des destructeurs de papier pour les documents sensibles qui ne sont plus nécessaires et que vous souhaitez détruire.
- Les médias sur lesquels sont enregistrées des informations sensibles tels les CD, les DVD, les disques durs externes ou les clés USB doivent aussi être rangés dans un lieu sûr et doivent être enlevés des postes de travail.
- Envisagez de scanner les documents ou papiers et de les conserver sous format électronique et de détruire par la suite, en toute sécurité, les papiers ou documents.
- A la fin de la réunion, effacez les tableaux et supprimez les feuilles avec annotations du tableau à feuilles papier.
- Il est interdit de noter sur papier les user ID et les phrases de passe complètes.

Accès à l'information

Les médias doivent être gérés minutieusement par l'utilisateur : papiers imprimés, courrier postal, clés USB, disques backup, fichiers partagés, post-it, PC, tablette, … .

Par exemple, l'utilisateur peut imprimer des données provenant d'une application protégée par la carte d'identité électronique; dans ce cas, la version imprimée de ces données n'est plus protégée par ce moyen.

Cela signifie que

- les documents contenant des informations sensibles sont de préférence imprimés suite à l'introduction d'un code de sorte qu'ils ne traînent pas sans surveillance sur l'imprimante. Imprimez uniquement les documents qui sont strictement nécessaires (aussi bon pour la consommation d'encre et pour l'environnement).
- Toute clé USB peut être utilisée pour transférer des documents d'un système à l'autre. En cas de transfert de données sensibles, la clé USB doit idéalement être complètement chiffrée et les données stockées sur celle-ci doivent être immédiatement supprimées après transfert. Une alternative consiste à enregistrer les informations sensibles dans un fichier ZIP protégé par un mot de passe.
- Tout backup sur tout type de média (SD drive, CD, DVD, disque dur externe, …) doit être localisé dans un environnement physiquement sécurisé et ne peut jamais être laissé sans surveillance.
- Un système de destruction est à la disposition de l'ensemble des collaborateurs pour la suppression de documents confidentiels. Il va de soi que tout document confidentiel en fin de vie doit être détruit par ce système.
- Aucune donnée à caractère personnel ne peut être transmise sous forme visible par e-mail. En cas d'envoi de fichiers sensibles par e-mail, veillez à ce que ceux-ci soient correctement chiffrés avant envoi.
- Dans le cas de répertoires partagés contenant des informations sensibles dédiées à un certain public, ces répertoires doivent être clairement configurés au niveau des droits d'accès.
- Il est strictement interdit de laisser des données sensibles sans surveillance sur une imprimante ou un bureau.

Annexe E: 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	
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 *****