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

Sécurité physique

(BLD PHYS)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait partie intégrante des politiques relatives 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).

Il décrit la politique relative à la sécurisation physique et à la sécurisation de l'environnement.

2. Environnement physique sécurisé

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. Espaces sécurisés

Toute organisation doit limiter l'accès aux bâtiments et locaux aux personnes autorisées et contrôler les accès pendant et en dehors des heures de bureau.

a. Les accès doivent être sécurisés (avec des barrières telles que des murs, des portes d'accès dotées de serrures à carte ou du personnel de réception) de manière à protéger les espaces où se trouvent des informations ainsi que des équipements informatiques sensibles ou critiques.

b. Les zones privées d'un bâtiment et les espaces sécurisés doivent être protégés par une sécurisation des accès adaptée, afin de s'assurer que seul du personnel compétent est admis.

c. Une sécurisation physique des bureaux, espaces et installations doit être conçue et réalisée.

d. Toute organisation doit prendre des mesures de prévention, de protection, de détection, d'extinction et d'intervention en cas d'incendie, d'intrusion ou de dégât des eaux.

e. Une protection physique et des consignes doivent être conçus et mis en œuvre pour les travaux réalisés dans des espaces sécurisés.

f. Les points d'accès comme les zones de chargement et de déchargement et autres points où des personnes non autorisées peuvent pénétrer sur le terrain doivent être maîtrisés et si possible isolés des équipements critiques et/ou informatiques, afin d'éviter les accès non autorisés.

2.2. Sécurisation du matériel

L'organisation doit prendre des mesures pour éviter que ses ressources soient perdues, endommagées, volées ou compromises et que ses activités soient interrompues.

a. Le matériel critique doit être placé et protégé de manière à réduire les risques de détérioration et de perturbation en provenance de l'extérieur ainsi que les possibilités d'accès non autorisé.

b. Toute organisation doit disposer d'une alimentation électrique alternative afin de garantir la prestation de services attendue. Le matériel critique doit être protégé contre les pannes de courant et autres perturbations dues à une interruption des équipements d'utilité publique.

c. Les câbles d'alimentation et de télécommunication utilisés pour le trafic de données ou les services informatiques de support doivent être protégés contre l'interception ou la détérioration.

d. Le matériel critique doit être maintenu correctement, de manière à être continuellement disponible et en bon état de fonctionnement.

e. Les équipements, informations et programmes de l'organisation ne peuvent pas être emportés sans accord préalable.

f. Les équipements installés en dehors des sites doivent être sécurisés, en fonction des risques de travaux en dehors du terrain de l'organisation.

g. Toute organisation doit prendre les mesures qui s'imposent afin que toutes les données présentes sur des supports de stockage soient effacées ou rendues inaccessibles avant suppression ou réutilisation.

h. Les utilisateurs doivent s'assurer que les équipements non surveillés sont protégés de manière adéquate.

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
2014		V2014	Quatrième version	30/08/2014	01/09/2014
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 TS 30104:2015 Security Techniques – Physical Security Attacks, Mitigation Techniques and Security Requirements.", mai 2015, 30 pages.
- ENISA, "Technical guideline for minimum security measures", décembre 2011, 22 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
- https://www.iso.org/standard/56890.html
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- https://resilience.enisa.europa.eu/
- http://www.isaca.org/cobit
- https://www.ksz-bcss.fgov.be/fr

Annexe C : Consignes de sécurité physique

Sécurisation physique de l'environnement

1. Les périmètres de sécurité du terrain, la partie publiquement accessible d'un bâtiment, la zone privée d'un bâtiment et les espaces sécurisés doivent être identifiés et définis.
2. La force des périmètres de sécurité des bâtiments, zones et espaces doit être fonction des exigences de sécurité fixées - sur la base d'une analyse des risques - au niveau des ressources d'information (matériel, applications, données) utilisées dans ces bâtiments, zones et espaces.
3. Les bâtiments ou sites comportant des équipements critiques et/ou ICT doivent bénéficier d'une protection physique suffisante.
4. Du personnel d'accueil ou d'autres dispositifs destinés à gérer l'accès physique aux bâtiments ou sites critiques doivent être présents.
5. L'accès à la zone privée d'un bâtiment et aux espaces sécurisés doit être réservé aux personnes autorisées.
6. Sur le plan des services d'utilité publique et de la sécurité, les bâtiments utilisés par l'organisation doivent être aménagés conformément à la législation et à la réglementation nationales, régionales et éventuellement internationales. Ceci est la responsabilité du gestionnaire des bâtiments.
7. Pour les bâtiments, zones et espaces critiques, des systèmes antieffraction doivent être installés conformément aux normes nationales, régionales et éventuellement internationales. Les espaces critiques non occupés doivent toujours être dotés d'un système d'alarme. Le bon fonctionnement des systèmes de sécurité doit être testé régulièrement.
8. Les portes incendie critiques doivent être dotées d'une alarme. Le bon fonctionnement des portes incendie doit être contrôlé et testé conformément aux normes nationales, régionales ou internationales.
9. Les systèmes d'alarme, les systèmes d'alerte incendie, les détecteurs de fumée et les sorties de secours doivent également être testés régulièrement conformément aux normes nationales, régionales ou internationales.
10. L'emplacement et la protection des archives doivent être minutieusement déterminés pour éviter un accès non autorisé aux informations stockées ou leur endommagement par un incendie ou un dégât des eaux.

Protection physique des accès

11. Les visiteurs de l'organisation doivent être enregistrés, avec en outre une indication de la date et de l'heure d'arrivée et de départ.
12. Les visiteurs d'espaces critiques sécurisés doivent détenir une autorisation explicite pour y pénétrer. Un accès ne peut être octroyé qu'à certaines fins autorisées. Les collaborateurs doivent préalablement transmettre des informations sur les visiteurs attendus aux réceptionnistes ou gardiens, pour autant qu'ils soient présents.
13. L'accès aux espaces critiques sécurisés doit être géré et limité aux seules personnes autorisées. Dans ce cas, tous les accès doivent être enregistrés à des fins d'audit.
14. Tous les collaborateurs internes et externes de l'organisation ainsi que les visiteurs doivent porter une forme d'identification de façon visible dans la zone privée d'un bâtiment (bureaux) ainsi que dans les espaces sécurisés.
15. Les collaborateurs de services de support externes ne doivent recevoir un accès aux espaces sécurisés ou aux équipements informatiques sensibles que lorsque l'organisation l'exige.
16. Les droits d'accès aux périmètres sécurisés doivent régulièrement être évalués, actualisés et, si nécessaire, retirés.

Sécurité des bureaux, espaces et installations

17. Les bâtiments, zones, étages et espaces doivent être classifiés sur la base des fonctions critiques qui y sont exécutées.
18. Les équipements critiques doivent être placés dans les bâtiments, zones ou espaces de telle manière qu'ils ne soient pas accessibles au public.
19. Les bâtiments, zones ou espaces dans lesquels sont traitées des informations doivent être le plus discrets possible.
20. Les informations sur les endroits où se trouvent des équipements informatiques sensibles ou critiques ne peuvent pas être publiquement accessibles.
21. Dans les espaces critiques, des dispositifs de surveillance adaptés doivent être utilisés, tels que des caméras.

Protection contre les menaces extérieures

22. Les matériaux dangereux doivent être stockés à bonne distance des espaces critiques.
23. Les supports de sauvegarde doivent être conservés à bonne distance de l'endroit où sont traitées les informations, afin qu'ils ne soient pas endommagés par une catastrophe sur le lieu du traitement.

Travaux dans les zones sécurisées

24. Les enregistrements (vidéo, photo, audio) dans les bâtiments, zones ou espaces critiques doivent être interdits, sauf moyennant l'autorisation explicite et l'encadrement permanent de l'organisation.
25. Seuls les collaborateurs de l'organisation doivent connaître sur une base "need-to-know" l'existence de bâtiments, zones ou espaces sécurisés ou d'activités dans ces bâtiments, zones ou espaces sécurisés.

Zones de chargement et de déchargement

26. L'accès aux zones de chargement et de déchargement doit être réservé à des collaborateurs autorisés détenteurs d'une forme valable et visible d'identification.
27. Les zones de chargement et de déchargement doivent être conçues/aménagées de sorte que des marchandises peuvent être livrées sans que le fournisseur ne doive pénétrer dans d'autres parties du bâtiment.
28. Le cas échéant, les portes extérieures d'une zone de chargement et de déchargement doivent être fermées lorsque les portes intérieures s'ouvrent.
29. À leur arrivée ou leur départ, les ressources d'information doivent être enregistrées suivant les procédures de gestion des ressources.

Placement et protection de matériel

30. Les installations de stockage doivent être protégées contre l'accès non autorisé.
31. Des mesures de contrôle doivent être mises en œuvre pour réduire à un minimum le risque de dangers, comme le vol, l'incendie et le vandalisme.
32. L'organisation doit établir et appliquer des consignes en ce qui concerne la nourriture, les boissons et le tabac dans les data centers placés sous sa gestion.
33. Les conditions environnementales comme la température et l'humidité de l'air doivent être surveillées pour éviter tout impact négatif sur le fonctionnement des équipements de traitement et de stockage de l'information.

Services d'utilité publique

34. Tous les services d'utilité publique comme la distribution d'eau et d'électricité, l'égouttage, le chauffage/la ventilation et la climatisation doivent être calculés en fonction des systèmes qui les supportent.
35. Les installations d'utilité publique doivent être régulièrement inspectées et si nécessaire testées pour garantir leur bon fonctionnement et réduire tout risque de défaillance ou de panne.
36. Une alimentation électrique appropriée satisfaisant aux spécifications du fournisseur du matériel doit être prévue.
37. En support des processus critiques, du matériel UPS (Uninterruptable Power Supply) et/ou un ou plusieurs groupes électrogènes doivent être prévus. Ceux-ci doivent être régulièrement contrôlés et testés de manière à s'assurer qu'ils possèdent la capacité suffisante.
38. Une réserve et une alimentation suffisantes en carburant doivent être prévues pour s'assurer que le groupe électrogène peut continuer à fonctionner durant une longue période.
39. Il faut vérifier si un système d'alarme doit être installé pour détecter les perturbations des installations d'utilité publique.
40. Un éclairage de secours doit être prévu pour le cas où une panne de courant générale se produit.
41. Des dispositifs adaptés doivent être prévus pour pouvoir couper le courant dans les situations d'urgence (ex. arrêt d'urgence ou interrupteur différentiel).
42. La distribution d'eau doit être stable et suffisante (ex. pour la climatisation, l'humidification et les systèmes de lutte contre l'incendie). Pour le refroidissement des data centers, une réserve d'eau doit être prévue pour les situations d'urgence.
43. Le matériel de télécommunication doit être connecté au moins de deux manières différentes aux systèmes du fournisseur de télécommunications.

Sécurisation des câbles

44. Les câbles réseau doivent être protégés contre les écoutes non autorisées ou les détériorations, par exemple au moyen de gaines ou de moulures, et traverser au minimum les espaces publics.
45. Une bonne gestion des câbles doit être appliquée. En outre, des marquages clairement identifiables doivent être apposés sur les câbles et le matériel afin d'éviter les erreurs lors des travaux de maintenance, comme par exemple le patching accidentel de câbles réseau défectueux. L'accès aux panneaux de brassage et espaces de câbles doit être sécurisé.
46. Un aperçu central de tous les patches réalisés doit être tenu pour réduire le risque d'erreurs. Pour les systèmes sensibles ou critiques, il faut prévoir des dispositifs de détection ainsi qu'une inspection physique, pour détecter tout matériel non autorisé relié au câblage.

Maintenance du matériel

47. Le matériel doit être maintenu selon les consignes et la périodicité préconisées par le fournisseur.
48. Seul du personnel de maintenance compétent peut assurer la réparation et la maintenance de matériel.
49. Il faut tenir un aperçu central de toutes les perturbations supposées ou réelles ainsi que de toutes les activités de maintenance préventive et corrective.
50. Des procédures doivent être établies permettant de savoir quand doit être maintenue quelle machine, qui doit effectuer la maintenance et si des informations doivent ou non être supprimées de la machine.

Emport de ressources d'information

51. À moins qu'il existe une politique générale permettant à tous les collaborateurs d'emporter des ressources d'information en dehors des murs de l'organisation, il convient d'en tenir un aperçu central.

Sécurisation du matériel en dehors du terrain

52. Le matériel et les supports en dehors du terrain ne peuvent pas être laissés sans surveillance dans des espaces publics. En déplacement, les ordinateurs portables doivent être transportés tel un bagage à main et doivent être le moins identifiables possible.

53. Les instructions du fournisseur relatives à la protection du matériel doivent être rigoureusement suivies.

Suppression et réutilisation de matériel en toute sécurité

54. Lorsque du matériel comporte des informations sensibles, il faut soit détruire le matériel physiquement, soit détruire ou supprimer les données ou les écraser via des techniques empêchant de récupérer les informations originales.

55. Pour du matériel endommagé contenant des informations sensibles, une évaluation des risques doit être réalisée afin de déterminer la nécessité d'une destruction, d'une réparation ou d'une suppression.

Matériel utilisateurs sans surveillance

56. Tout utilisateur final doit être informé de ses responsabilités concernant la sécurité de l'information et les procédures de protection du matériel sans surveillance des utilisateurs finaux.

57. Le matériel d'utilisateurs finaux qui n'est pas utilisé activement doit être sécurisé par un économiseur d'écran automatique et un mot de passe, la réactivation devant reposer sur l'identification et l'authentification de l'utilisateur.

58. Les utilisateurs finaux doivent :

    - entièrement fermer ou verrouiller les sessions actives lorsque la machine est laissée sans surveillance ou lorsqu'ils terminent leurs tâches/activités ;
    - se déconnecter des applications ou services réseau lorsqu'ils n'en ont plus besoin.

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	**Oui**
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 *****