LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

Juillet 2023

Charte
de bonne conduite
en matière de sécurité de l'information numérique

1 PROTECTION
de l'information

2 ACCÈS
aux systèmes d'informations de l'État

3 UTILISATION
et sécurité des ressources informatiques

4 RÉAGIR
en cas d'événements de sécurité

5 SENSIBILISATION

SOMMAIRE

PRÉAMBULE

La présente charte a pour objet de préciser les consignes de sécurité de base relatives à l'utilisation des systèmes d'information non classifiés[1] de l'État.

Cette nouvelle version a été élaborée par le Haut Commissariat à la Protection Nationale dans sa fonction d'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et le CTIE.

Elle s'applique à l'ensemble des utilisateurs des réseaux et systèmes d'information non classifiés, installés et exploités par les administrations et services de l'État.

L'ANSSI a également rédigé une Politique générale de la sécurité de l'information de l'État luxembourgeois dont les documents sont téléchargeables et consultables sur le site Extranet de l'ANSSI

anssi.extranet.etat.lu

ou le site Internet du Haut-Commissariat à la protection nationale

hcpn.gouvernement.lu

1. PROTECTION DE L'INFORMATION

La confidentialité et le secret professionnel sont des principes fondamentaux qui méritent une attention toute particulière dans le contexte des technologies de l'information et de la communication.

L'utilisateur veille à protéger les informations de l'État afin d'éviter une divulgation accidentelle ou non autorisée, une mauvaise utilisation, une altération ou une destruction inappropriée.

Il est interdit à tout utilisateur de tenter d'accéder à des informations auxquelles il n'est pas autorisé ou qui ne sont pas utiles à l'accomplissement de ses missions et fonctions. En particulier, l'utilisateur ne doit pas accéder ou tenter d'accéder à des données personnelles d'autres utilisateurs, sauf autorisation explicite.

Il est interdit de donner accès ou de mettre à disposition d'un tiers, sauf autorisation explicite, toute information professionnelle non publique (p. ex. photographies, vidéos, captures d'écrans ou par un copier/coller d'informations).

LES PRINCIPALES CYBERMENACES

Une « cybermenace » désigne toute circonstance, action ou tout événement potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes.

Nous invitons chaque utilisateur à consulter les recommandations de sécurité détaillées portant sur les principales cybermenaces sur le site Extranet de l'ANSSI (https://anssi.extranet.etat.lu). La consultation régulière du site du GOVCERT, (www.govcert.lu), qui attire votre attention sur les attaques « phishing » actuelles et comment les détecter, est également recommandée.

Remarque : La sécurité des informations classifiées est régie par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité et ne fait pas objet de la présente charte.

1. La sécurité des informations classifiées est régie par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité et ne fait pas objet de la présente charte.

1.1 Sites de stockage en ligne

Le stockage d'informations professionnelles non publiques dans des applications ou sites en ligne privés (Google Drive, OneDrive, iCloud, Dropbox, etc.) est strictement interdit.

1.2 Politique du bureau propre

Afin de réduire les risques d'accès non autorisés, de perte et d'endommagement des informations en dehors de la surveillance de l'utilisateur (pendant ou en dehors des heures de travail), il est très fortement préconisé aux utilisateurs d'adopter une politique de « bureau propre ». Ainsi, tous les utilisateurs sont invités à ranger les supports d'information contenant des informations professionnelles non publiques lorsqu'ils quittent leur poste de travail.

1.3 Déplacement national

Lors d'un déplacement national, l'utilisateur est appelé à faire preuve de vigilance quant aux équipements informatiques et aux informations qu'il transporte.

Il s'assure notamment :

- que les données professionnelles non publiques soient accédées via des connexions sécurisées, plutôt qu'à partir d'un stockage local. En cas de déplacement dans un lieu sans connexion Internet fiable, l'utilisateur est autorisé à conserver temporairement les données essentielles à son besoin métier sur son ordinateur portable ;
- de recourir systématiquement au chiffrement des données professionnelles non publiques emportées (p. ex. utilisation de portables avec disques chiffrés ou utilisation de clés USB chiffrées) ;
- que les informations et équipements soient conservés en sécurité (p. ex. ne pas laisser l'ordinateur portable de manière visible dans une voiture) ;
- d'éviter la connexion à des périphériques externes ou à des réseaux non sécurisés, non dignes de confiance.

1.4 Déplacement à l'étranger

En sus des mesures applicables en cas de déplacement national, les consignes suivantes sont applicables :

- en cas de perte ou de vol de matériel, prévenir au plus vite l'instance gestionnaire des incidents de sécurité et établir une déclaration dans un commissariat de police du pays dans lequel l'incident s'est produit ;
- en cas d'inspection par les autorités locales, prévenir au plus vite l'instance gestionnaire des événements et des incidents de sécurité et agir selon les instructions communiquées ;
- au retour, demander à son responsable informatique en cas de suspicion, notamment si le matériel a été inspecté par les autorités locales ou s'il a été branché à des réseaux peu fiables, une analyse du matériel et changer les mots de passe.

2. ACCÈS AUX SYSTÈMES D'INFORMATION DE L'ÉTAT

L'utilisateur ne peut accéder aux systèmes d'information de l'État que dans la limite des droits d'accès accordés par le biais du processus de gestion des accès. L'utilisateur ne doit pas s'octroyer ou essayer de s'octroyer lui-même des droits d'accès ou des privilèges.

L'utilisateur ne dispose sur les systèmes d'information de l'État que des droits d'accès strictement nécessaires à l'accomplissement de ses missions, en application du principe du « moindre privilège ». En pratique, l'utilisateur doit signaler tout accès non nécessaire (p. ex. suite à un changement des attributions de l'utilisateur ou un changement de service) afin que les droits non nécessaires puissent être supprimés.

2.1 Identifiants et mots de passe

L'utilisateur reçoit personnellement un identifiant (dans le contexte IAM : « nom d'utilisateur » ou IAM ID) et un mot de passe. Cet identifiant et ce mot de passe sont strictement personnels, confidentiels et incessibles. Chaque utilisateur est donc responsable de l'usage qui en est fait.

Les règles de sécurité suivantes sont applicables :

- les informations d'identification ont un caractère confidentiel et ne doivent pas être partagées avec d'autres personnes. Les utilisateurs ne doivent en aucun cas permettre à une autre personne (collègue ou autre) d'accéder à un système ou une application avec leurs identifiants ;
- les systèmes d'authentification mis en œuvre sont à respecter et il est strictement interdit d'essayer de les contourner ;
- il est strictement interdit de tenter d'utiliser ou d'accéder à un système / application avec les identifiants d'un autre utilisateur ;
- les mots de passe doivent être choisis avec soin, p. ex. minuscules, des majuscules, des chiffres et des caractères spéciaux, absents des dictionnaires et sans lien avec l'utilisateur, sa famille ou son entourage (p. ex. date de naissance) ;
- les mots de passe doivent être mémorisés. Ils ne doivent ni être notés sur un support accessible par un tiers (mémo adhésif, papier libre, etc.), ni stockés en clair sous format électronique (fichier, messagerie électronique, etc.) ;
- en cas de compromission réelle ou suspectée d'un mot de passe il y a lieu de le changer immédiatement ;
- la réutilisation des mêmes mots de passe personnels pour accéder aux systèmes d'information de l'État et pour accéder à des comptes privés est interdite ;
- la mémorisation de mots de passe dans les navigateurs Internet n'est pas autorisée ;
- l'utilisation de gestionnaires de mots de passe en ligne est interdite ;
- pour l'utilisateur qui, dans le contexte de sa mission, a besoin de se connecter à de multiples applications internes, respectivement à des applications et sites en ligne, l'utilisation d'un coffre-fort numérique (p. ex. Keepass) assurant le stockage sécurisé et chiffré des mots de passe est recommandée. En cas d'utilisation d'un tel coffre-fort numérique, il est impératif que le mot de passe de celui-ci respecte les règles énoncées dans la présente charte.

BIEN CHOISIR SON MOT DE PASSE

Le mot de passe doit être robuste et complexe afin que personne ne puisse le deviner. Il devrait comporter au minimum 12 caractères , mélangeant les minuscules, majuscules, chiffres et caractères spéciaux. Le cas échéant, l'utilisation de moyens mnémotechniques est recommandée pour construire le mot de passe, afin que ce dernier soit facilement mémorisable.

Le mot de passe ne devrait pas contenir d'information en lien avec l'utilisateur, sa famille ou son entourage, ou qui pourrait être facilement accessible par un tiers (p. ex. sur les réseaux sociaux), telle une date de naissance, le nom de proches, des identifiants, des mots du dictionnaire ou équivalents.

2.2 Connexion au réseau de l'État

Pour assurer la sécurité des systèmes d'information de l'État, l'accès au réseau de l'État est réservé aux équipements autorisés, gérés et mis à disposition aux utilisateurs par les services compétents. La connexion au réseau de l'État d'équipements privés ou visiteurs (tels qu'ordinateurs personnels, tablettes, imprimantes, smartphones, ou autres périphériques), qu'elle soit filaire ou sans fil, est interdite.

Cette restriction ne s'applique évidemment pas aux réseaux dédiés à la connexion de terminaux personnels ou visiteurs.

2.3 Accès distant et télétravail

L'accès à distance aux ressources informatiques internes de l'État est réservé aux personnes en ayant le besoin métier.

L'utilisateur devant se connecter à des ressources informatiques à distance pour des besoins professionnels doit :

- avoir reçu une autorisation formelle de la part de sa hiérarchie ;
- réaliser l'accès à distance uniquement avec le matériel fourni et spécifiquement configuré à ces fins ;
- veiller à ce que le matériel fourni pour le télétravail ou l'accès à distance ne soit pas utilisé par un tiers (équipement personnel) ;
- ne pas contourner ou tenter de contourner les mesures et dispositifs de sécurité permettant d'assurer une connexion sécurisée à distance ;
- veiller à protéger la confidentialité des informations qu'il imprime.

L'utilisateur accédant au VPN de l'État est personnellement responsable de l'utilisation qu'il en fait.

CAS PARTICULIER DU TÉLÉTRAVAIL

Le télétravail permet à l'utilisateur (ci-après « le télétravailleur ») de réaliser régulièrement son activité professionnelle en dehors de son lieu de travail habituel.

Le télétravailleur est soumis aux mêmes obligations en matière de sécurité de l'information que l'utilisateur travaillant sur site. Le télétravailleur est également tenu de prévoir un espace dédié à ses activités professionnelles qui garantit la confidentialité des informations accédées (p. ex. lors de l'utilisation d'outils de vidéoconférence à domicile). Il doit être particulièrement attentif aux règles décrites dans la section « Postes de travail et ordinateurs portables ».

3. UTILISATION ET SÉCURITÉ DES RESSOURCES INFORMATIQUES

Les ressources informatiques mises à disposition par l'État (p. ex. accès à Internet, postes de travail, ordinateurs portables, imprimantes, téléphones, tablettes, logiciels ou applications) sont destinées à l'activité professionnelle des utilisateurs.

Une utilisation privée est tolérée, dans la mesure où elle :

- ne constitue pas un abus ;
- ne perturbe pas les tâches professionnelles ;
- n'enfreint ni les lois ou réglementations en vigueur, ni la présente charte ;
- ne porte pas atteinte à la sécurité et au bon fonctionnement des systèmes d'information de l'État ;
- ne peut ternir l'image de l'État.

L'usage privé des ressources informatiques peut être limité par une administration ou un service de l'État, notamment dans un souci de bon usage des ressources (p.ex. sécurité ou performance) .

Il est strictement interdit de tenter de modifier, de modifier ou de contourner les paramètres et dispositifs de sécurité informatique (p. ex. désactivation du logiciel antivirus, modification des droits d'accès ou suppression des traces d'audit générées par les systèmes).

L'utilisateur ne doit pas tenter d'analyser ou d'exploiter des vulnérabilités sur les ressources informatiques de l'État (p. ex. à l'aide d'outils de « scan de vulnérabilités » ou de « hacking »).

Un équipement de l'État ne doit pas être sorti des locaux de l'État, sauf autorisation préalable et à l'exception des équipements autorisés. Les équipements autorisés incluent les équipements mobiles fournis par l'État et prévus pour être utilisés en dehors des locaux de l'État (p. ex. ordinateurs portables, smartphones, tablettes ou supports de stockage amovibles).

L'utilisateur fait un usage responsable et écologique des ressources informatiques, en veillant notamment à limiter l'impression de documents ainsi qu'en éteignant les postes de travail, ordinateurs portables et appareils mobiles en cas d'absence prolongée (sauf consigne contraire).

La perte ou le vol d'un équipement informatique doit être notifié comme un événement de sécurité par l'utilisateur concerné selon les modalités décrites dans la section « Réagir en cas d'événement de sécurité ».

3.1 Postes de travail et ordinateurs portables

Les postes de travail et ordinateurs portables sont des éléments clés du système d'information de l'État. La modification de la configuration et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système d'information en place.

Ainsi, il importe de respecter les consignes suivantes :

- l'utilisateur devrait éviter de stocker les données professionnelles sur les disques locaux (p. ex. disques C : ou D :). A défaut, l'utilisateur doit s'assurer qu'elles sont sauvegardées sur les serveurs de l'État ;
- la connexion filaire (p. ex. USB) ou sans fil (p. ex. Bluetooth) des appareils mobiles non gérés par l'État (i.e. tout appareil privé) aux postes de travail et ordinateurs portables de l'État est interdite, sauf autorisation préalable. La recharge électrique d'un appareil mobile privé par l'intermédiaire d'un poste de travail, ordinateur portable ou écran est interdite ;
- la connexion de supports de stockage amovibles privés (p. ex. cartes SD, clés USB, disques amovibles, CD/DVD), ne provenant pas de source sure, aux postes de travail et ordinateurs portables de l'État n'est pas autorisée ;
- l'utilisateur ne doit pas utiliser les postes de travail ou les ordinateurs portables de l'État pour sauvegarder ou synchroniser le contenu de leur appareil mobile, tel que des fichiers multimédias, à moins que ce contenu ne soit nécessaire à leurs besoins professionnels ;
- il est interdit de modifier la configuration matérielle en retirant ou en installant des composants (p. ex. graveur, disque dur supplémentaire ou lecteur DVD), sauf autorisation préalable ;
- l'utilisateur doit permettre l'installation des mises à jour de sécurité sur son poste de travail ou ordinateur portable dans les meilleurs délais ;
- sauf raison professionnelle justifiée, il est interdit de modifier la configuration logicielle des postes de travail en retirant des programmes, en installant des programmes téléchargés depuis Internet ou reçus par courrier électronique ou en provenance de toute autre source ;
- les postes de travail sont à verrouiller lorsque l'utilisateur quitte son poste, même momentanément, en activant le blocage d'accès (sous Windows : par exemple en appuyant sur ⊞ + L) ;
- en cas de prise en main à distance de son poste de travail, il est recommandé à l'utilisateur de rester présent devant son poste de travail pendant l'intervention, fermer les applications et fichiers contenant des informations personnelles ou professionnelles non publiques et de s'assurer que la prise en main est bien terminée en fin d'intervention ;
- avant de connecter un support de stockage amovible sur un équipement de l'État, l'utilisateur doit avoir une assurance raisonnable qu'il ne présente pas de logiciels malveillants (virus, vers, rançongiciel, etc.). Pour ce faire, il est recommandé d'utiliser des outils dédiés à la vérification de l'absence de virus (p. ex. boitiers « GoviClean » ou outil d'analyse antivirus en ligne « MultiAV » fournis par le GOVCERT).

CAS PARTICULIER DES ORDINATEURS PORTABLES

En sus des règles relatives aux postes de travail, les ordinateurs portables en déplacement sont soumis aux règles suivantes :

- il est fortement recommandé de désactiver toutes les connexions sans fil dès qu'elles ne sont plus requises à des fins professionnelles (WiFi, Bluetooth, etc.) ;
- l'utilisateur est personnellement responsable de son ordinateur portable et doit prendre les mesures de protection adéquates pour minimiser les risques de vols et d'endommagements. Les ordinateurs portables ne doivent pas être laissés sans surveillance dans les lieux publics et ne doivent pas être visibles lorsqu'ils sont laissés sans surveillance dans un véhicule ;
- les données professionnelles non publiques devraient être accédées via des connexions sécurisées plutôt qu'à partir d'un stockage local. Si cela n'est pas possible, l'utilisateur charge uniquement les données essentielles à son besoin métier sur son ordinateur portable ;
- les ordinateurs portables ne doivent pas être utilisés dans des emplacements où des personnes mal intentionnées pourraient avoir une vue directe de l'écran. L'utilisation de filtres de confidentialité est fortement recommandée ;
- l'utilisateur doit éteindre son ordinateur portable lors d'un déplacement en dehors des locaux de l'État ;
- en cas d'utilisation d'un réseau WiFi ou filaire (Ethernet), inconnu ou non sécurisé, la connexion directe à Internet est interdite. L'utilisateur doit utiliser le client VPN professionnel. Si la connexion VPN ne réussit pas, le réseau concerné ne doit pas être utilisé.

3.2 Messagerie électronique

Les consignes suivantes sont à considérer, respectivement à respecter dans le cadre de l'utilisation de la messagerie électronique :

- l'utilisateur doit être conscient du fait que l'acheminement, l'authenticité et l'intégrité des messages véhiculés par Internet ne sont pas garantis ;
- l'utilisateur doit faire preuve d'une extrême vigilance lorsqu'ils reçoivent un message provenant d'Internet avec un fichier attaché ou contenant un lien vers un autre site, surtout si celui-ci est un expéditeur externe au réseau de l'Etat. Il ne doit également pas répondre à l'expéditeur et ne pas activer des liens ou ouvrir des pièces jointes qui lui paraissent suspects. Les messages électroniques peuvent notamment servir de vecteur à la transmission de code malveillant (virus, rançongiciels, chevaux de Troie, etc.) ;
- les comptes de messagerie professionnels et personnels sont obligatoirement séparés. Les données professionnelles doivent obligatoirement être envoyées par l'intermédiaire d'un compte de messagerie professionnel. L'utilisateur doit également éviter d'utiliser son adresse e-mail personnelle dans un contexte professionnel ;
- le transfert de courriers électroniques à caractère professionnel d'une adresse professionnelle vers une adresse personnelle est strictement interdit ;
- la diffusion de messages qui peuvent porter atteinte à la réputation de l'État est strictement interdite ;
- l'utilisateur est appelé à vérifier soigneusement la liste des destinataires avant chaque envoi, et ce particulièrement lors d'envoi de données à caractère confidentiel ou sensible ;
- en cas de transmission d'informations à caractère confidentiel à des destinataires externes, il est recommandé d'utiliser un système d'échange de fichiers électroniques (p. ex. « One-Time-Exchange » (« OTX »)),qui permet d'échanger des fichiers électroniques avec des tiers via un canal sécurisé, ou de procéder à un chiffrement adéquat des informations ;

- il est recommandé à l'utilisateur d'activer la fonction de notification automatique en cas d'incapacité de gérer le courrier électronique pendant une durée prolongée (Out of Office).

3.3 Accès Internet

Pour des raisons de sécurité, l'accès à certaines catégories de sites n'est pas autorisé[1] (hacking, jeux, chat, sites à caractère pornographique, violent ou raciste, etc.). Les accès à Internet sont protégés par des mesures de sécurités génèrant automatiquement des traces des activités réalisées. Ces traces peuvent être enregistrées et conservées pour pouvoir notamment détecter et remédier aux pannes, dysfonctionnements, actions illicites ou usages présumés anormaux ceci en conformité avec la législation en vigueur.

L'accès Internet est régi par les consignes et recommandations suivantes :

- toute transmission interne ou externe d'informations à caractère indécent, obscène, profanateur, menaçant, frauduleux ou illégal est interdite ;
- le « téléchargement illicite » de logiciels ou de contenu protégé par droit d'auteur (musique, vidéo, etc.) est interdit ;
- il est de bonne pratique de référencer dans les publications les sources des informations recherchées sur Internet ;
- la publication d'informations professionnelles non publiques dans des forums ou autres sites est soumise à autorisation préalable ;
- la souscription à des abonnements payants sous le nom et l'adresse de l'État est soumise à autorisation préalable et engagement comptable selon les procédures usuelles ;
- les outils de traduction et de conversion de documents en ligne ne doivent pas être utilisés sur des informations à caractère confidentiel ;
- même si l'accès à un site n'est pas bloqué, l'utilisateur doit faire preuve de vigilance lorsqu'il télécharge un contenu ;
- il est interdit d'utiliser tout type de réseau superposé tel que Tor ou de services « peer-to-peer » (p. ex. Torrent) sur les équipements de l'État.

3.4 Supports de stockage amovibles

Les supports de stockage amovibles (p. ex. cartes SD, clés USB, disques amovibles, CD/DVD) utilisés pour des raisons professionnelles sont régis par les consignes et recommandations suivantes :

- les supports de stockage amovibles contenant des informations professionnelles non publiques doivent être protégés lorsqu'ils sont laissés sans surveillance (p. ex. conservation dans une armoire verrouillée) ;
- l'utilisateur ne doit pas prêter son support de stockage amovible à un tiers ou laisser un tiers non autorisé y accéder ;
- les informations à caractère confidentiel et/ou sensible doivent être chiffrées ou protégées adéquatement par mot de passe, dès lors qu'elles sont stockées sur un support de stockage amovible. Il est recommandé de faire recours à des clés USB incluant une fonctionnalité de chiffrement ;
- l'utilisateur ne doit pas connecter un support de stockage amovible utilisé à des fins professionnelles à un équipement privé ;
- après usage, l'utilisateur efface toutes les données professionnelles non publiques sur le support de stockage amovible (i.e. clés USB ou disques amovibles).

1. Cette interdiction ne vaut pas pour les services et utilisateurs qui ont besoin de tels accès dans le contexte de leur mission.

3.5 Appareils mobiles

Les règles de sécurité suivantes sont applicables aux appareils mobiles (p. ex. smartphones ou tablettes), professionnels ou privés « Bring Your Own Device », utilisés pour accéder aux ressources internes de l'État :

- l'utilisateur doit protéger son appareil mobile par un code de verrouillage, mot de passe ou fonction biométrique. Il ne doit pas prêter son appareil mobile et ne pas laisser un tiers non autorisé y accéder ;
- l'utilisateur doit appliquer systématiquement les mises-à-jour de son appareil mobile, sauf contre-indication de son service informatique;
- l'utilisateur ne doit pas activer des fonctionnalités de partage dont la sécurité est douteuse (p. ex. bluetooth, nearby share, tethering ou airdrop) ;
- l'utilisateur accède aux données essentielles à son besoin métier via des connexions sécurisées et se retreint autant que possible de télécharger ces données sur son appareil ;
- si l'utilisateur soupçonne qu'un accès non autorisé aux données de l'État a eu lieu par l'intermédiaire de son appareil mobile, il signale l'incident à l'instance gestionnaire des événements et des incidents de sécurité[2] ;
- le débridage (en anglais « jailbreak ») ou l'installation de logiciels / firmware conçus pour avoir accès à des fonctionnalités non standardes sont interdits, sauf autorisation préalable ;
- l'installation de logiciels ne doit se faire qu'à partir des magasins d'applications officiels (p. ex. « Google Play Store » ou « Apple App Store »). L'installation de logiciels piratés ou de contenus illégaux est interdite ;
- l'utilisateur ne doit pas charger son appareil mobile sur une station de charge publique USB ou USB-C (présente par exemple dans les gares, aéroports ou centre commerciaux).

3.6 Utilisation de réseaux sans-fil dans un contexte professionnel

Chaque utilisateur est responsable de son utilisation du WiFi. Cet usage ne doit pas nuire à la sécurité de l'information de l'État.

En cas de connexion à un tel réseau, il y a lieu :

- d'utiliser l'accès VPN (la connexion directe à Internet étant interdite). Si la connexion VPN ne réussit pas, le réseau WiFi ne doit pas être utilisé ;
- de désactiver le réseau sans-fil à la fin d'utilisation ;
- d'éviter au maximum l'utilisation de réseaux WiFi qui ne sont pas gérés par l'État (WiFi publics).

3.7 Imprimantes

L'utilisateur veille à protéger la confidentialité des informations qu'il imprime.

2 Cf. « Réagir en cas d'événement de sécurité de l'information »

4. RÉAGIR EN CAS D'ÉVÉNEMENT DE SÉCURITÉ

Doit être considéré comme événement de sécurité de l'information, tout occurrence identifiée de l'état d'un système, d'un service ou d'un réseau, indiquant une faille possible dans la politique de sécurité, un échec des mesures de sécurité ou une situation inconnue jusqu'alors, et pouvant relever de la sécurité.

Voici quelques exemples d'événements de sécurité :

- divulgation non autorisée d'information professionnelle non publique ;
- perte ou vol de matériel informatique ;
- présence d'un logiciel malveillant sur le poste de travail d'un utilisateur ;
- ouverture par un utilisateur d'une pièce jointe ou activation d'un lien frauduleux provenant d'un message de type hameçonnage (en anglais « phishing ») ;
- changement non autorisé apporté à un système d'informations ;
- accès non autorisé ou tentative d'accès non autorisée ;
- découverte d'une vulnérabilité ou d'une faille de sécurité.

L'utilisateur est tenu de signaler tout événement de sécurité dans les plus brefs délais à l'instance gestionnaire des évenements et des incidents de sécurité désignée par son administration ou service de l'État. L'utilisateur concerné doit alors agir selon les instructions communiquées par l'instance gestionnaire des événements et des incidents de sécurité.

Si l'instance gestionnaire des évenements et des incidents de sécurité n'est pas joignable (p. ex. en dehors des heures de travail usuelles), l'utilisateur concerné peut contacter le GOVCERT.LU et agir selon les instructions qui lui seront communiquées.

L'utilisateur veille à protéger la confidentialité des informations relatives à un événement de sécurité.

5. SENSIBILISATION

L'ensemble du personnel de l'État est invité à suivre régulièrement des séances de sensibilisation (proposées par l'INAP, organisées par l'entité ou proposées par ailleurs) en matière de sécurité de l'information numérique.

Nous invitons chaque utilisateur à consulter les sites suivants qui proposent des supports de sensibilisation et de formation à la sécurité de l'information numérique

anssi.extranet.etat.lu

www.govcert.lu

lhc.lu

www.nc3.lu

www.cybersecurity.lu

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information