ANSSI.lu

Agence nationale de la sécurité
des systèmes d'information
Luxembourg

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

Historique

Version	Date	Auteur	Commentaire
1.0	29.06.2017	ANSSI/CTIE	Version finale

Table des matières

1 Protection de l'information 3
1.1 Ingénierie sociale 3
1.2 Réseaux sociaux 4
1.3 Sites de stockage en ligne 5
1.4 Politique du bureau propre 5
1.5 Déplacement national 5
1.6 Déplacement à l'étranger 5
2 Accès aux systèmes d'information de l'État 6
2.1 Identifiants et mots de passe 6
2.2 Connexion au réseau de l'État 7
2.3 Accès à distance par VPN 7
3 Utilisation et sécurité des ressources informatiques 7
3.1 Postes de travail 7
3.2 Messagerie électronique 8
3.3 Accès Internet 8
3.4 Ordinateurs portables 9
3.5 Supports de stockage amovibles (clés USB, disques amovibles, CD/DVD) 9
3.6 Appareils mobiles (smartphones, tablettes) 10
3.7 Réseaux sans-fil (WiFi) 10
3.8 Imprimantes 11
4 Réagir en cas d'incidents de sécurité 11
5 Sensibilisation 11

Préambule

La présente charte a pour objet de préciser les consignes de sécurité de base relatives à l'utilisation des systèmes d'information de l'État par l'ensemble des utilisateurs. Sont visés les équipements et moyens informatiques et téléphoniques ainsi que les services internet. Elle a été élaborée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et le CTIE.

La charte a été approuvée par le Conseil du gouvernement dans sa séance du 2 juin 2017. L'ANSSI a également rédigé une politique de sécurité de l'Information de l'État luxembourgeois dont les documents sont téléchargeables et consultables sur le govspace du CTIE (https://govspace.msp.etat.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.

Tout utilisateur est invité à vérifier le degré de confidentialité de l'information professionnelle qu'il traite puisqu'il est responsable de l'usage qu'il en fait.

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.

1.1 Ingénierie sociale

Le terme d'ingénierie sociale désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique répandue consistant à obtenir des informations internes ou confidentielles par téléphone, courrier électronique, courrier traditionnel ou contact direct de la part de certaines personnes cibles travaillant pour l'organisation visée.

L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la crédulité des personnes cibles en se faisant souvent passer pour une personne de la même organisation, un technicien, un supérieur, etc.

De nombreuses attaques cyber incluent une composante d'ingénierie sociale qui vise à convaincre la personne ciblée à fournir des informations ou à effectuer une action spécifique.

Il est recommandé à l'ensemble des utilisateurs des équipements, moyens et services de l'État de faire attention à ce type de pratique, de faire preuve de prudence, de vigilance et d'une saine méfiance et de respecter les consignes minimales suivantes :

- de vérifier, si possible, l'identité des interlocuteurs non connus personnellement, en leur demandant des informations précises (p.ex. nom et prénom, société, numéro de téléphone) ;
- de s'interroger sur la criticité des informations demandées ;
- de vérifier éventuellement les informations fournies.

Attaques par hameçonnage ciblé (Spear phishing)

Des attaques ciblées et rusées de type « Spear phishing » sur les utilisateurs des systèmes d'information de l'État sont régulièrement observées et constituent une menace importante. Ces attaques consistent à falsifier l'adresse de messagerie de l'expéditeur ou le sujet, le corps respectivement la signature du message et ont pour but de duper le destinataire en vue de l'inciter à ouvrir une pièce jointe malveillante ou un lien.

Malgré le fait que les stations de travail de l'État soient protégées par des mécanismes de protection performants, il importe que tous les utilisateurs adoptent les bons réflexes et essaient de repérer les e-mails suspects. A cette fin, l'utilisateur peut se laisser guider par les questions suivantes :

- est-ce qu'il est crédible que l'expéditeur envoie l'e-mail ?
- est-ce que l'adresse de l'expéditeur est bien celle qu'il utilise généralement ?
- est-ce que l'objet de l'e-mail est crédible ?
- est-ce que le contenu de l'e-mail est en adéquation avec l'expéditeur et l'objet ?
- est-ce qu'il est crédible que l'expéditeur envoie un document attaché ?

En cas de doute, il est important :

- de ne pas ouvrir l'e-mail, respectivement les pièces jointes ou les liens et de ne pas répondre à l'e-mail reçu ;
- de contacter l'expéditeur par téléphone ou par e-mail en utilisant l'adresse bien connue et de demander confirmation.

En cas de doute non levé ou d'attaque confirmée il y a lieu d'informer l'instance gestionnaire des incidents de sécurité[1].

1.2 Réseaux sociaux

L'utilisation des réseaux sociaux doit se faire selon les règles de bonne conduite et d'éthique. L'utilisateur naviguant sur les sites de réseaux sociaux (Facebook, Twitter, etc.) doit être conscient des risques associés à cette pratique. Les principes fondamentaux suivants sont impérativement à respecter :

- **Assurer la confidentialité** : l'utilisateur s'engage à ne publier aucune information professionnelle non publique ;
- **Être responsable** : l'utilisateur est personnellement responsable de toutes les activités qu'il conduit sur le site et est donc tenu responsable de toute information publiée (message, commentaire, contenu multimédia, etc.) ;
- **Respecter autrui** : l'utilisateur s'engage à ne pas publier des propos intolérants, hostiles, haineux ou autres propos diffamatoires. L'utilisateur s'engage également à être courtois.

[1] Soit le Helpdesk de l'entité si cette fonction existe, sinon le responsable informatique. Si aucune de ces fonctions n'est définie, alors la notification doit être faite au GovCERT. Il revient au Helpdesk respectivement au responsable informatique d'évaluer l'impact de l'incident. En cas d'incident d'envergure, notamment s'il y a un risque d'impact sur des tiers, l'incident est à notifier sans délai au GovCERT.

1.3 Sites de stockage en ligne

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

1.4 Politique du bureau propre

Afin de réduire les risques d'accès non autorisés, de perte et d'endommagement des informations en dehors des heures de travail, il est recommandé aux utilisateurs d'adopter une politique de « bureau propre ». Ainsi, chacun est invité à ranger les supports d'information contenant des informations professionnelles non publiques lorsqu'il quitte son poste de travail.

1.5 Déplacement national

Lors d'un déplacement national, l'utilisateur fait preuve de vigilance quant aux équipements informatiques et aux informations qu'il transporte. Il s'assure au minimum :

- que les informations soient sauvegardées sur un autre support d'information restant dans les locaux de l'entité ;
- que seules les informations nécessaires dans le cadre de la mission soient emportées ;
- que les informations professionnelles emportées non publiques soient protégées adéquatement (p.ex. utilisation de clés USB chiffrées, utilisation de portables avec disques chiffrés, etc.) ;
- que les équipements et les informations soient conservés en sécurité (p.ex. ne pas laisser l'ordinateur portable de manière visible dans une voiture, etc.) ;
- d'éviter la connexion à des périphériques externes ou à des réseaux non sécurisés, non dignes de confiance.

1.6 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[1] 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 incidents de sécurité [1];
- au retour, demander 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.

[1] Soit le Helpdesk de l'entité si cette fonction existe, sinon le responsable informatique. Si aucune de ces fonctions n'est définie, alors la notification doit être faite au GovCERT. Il revient au Helpdesk respectivement au responsable informatique d'évaluer l'impact de l'incident. En cas d'incident d'envergure, notamment s'il y a un risque d'impact sur des tiers, l'incident est à notifier sans délai au GovCERT.

2 Accès aux systèmes d'information de l'État

2.1 Identifiants et mots de passe

Les utilisateurs reçoivent 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 sont confidentielles 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 sont à choisir avec soin. Un bon mot de passe est composé d'au moins 8 caractères de 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.

  Il ne faut en aucun cas utiliser :

  - un mot du dictionnaire (même tiré d'un dictionnaire d'une langue étrangère),
  - un prénom,
  - l'identifiant,
  - une quelconque information liée à la personne, la famille ou l'entourage (prénom, date de naissance, nom des enfants, nom des animaux domestiques, etc.).
- ne jamais demander à un tiers de générer un mot de passe ;
- les mots de passe doivent être mémorisés et ne doivent pas être notés ou 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 les utilisateurs qui, dans le contexte de leur mission, ont besoin de se connecter à de multiples applications internes, respectivement à des applications et sites en ligne, l'utilisation d'un coffre-fort numérique 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.

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 d'équipements privés ou d'équipements visiteurs (ordinateurs personnels, tablettes, imprimantes, smartphones, périphériques, etc.), qu'elle soit filaire ou sans fil, au réseau de l'État est interdite.

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

2.3 Accès à distance par VPN

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

Les utilisateurs devant se connecter à des ressources informatiques à distance pour des besoins professionnels doivent :

- avoir reçu une autorisation formelle de la part de leur 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.

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

3 Utilisation et sécurité des ressources informatiques

Les équipements, moyens et services mis à disposition par l'État sont destinés 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 pas la loi ou la réglementation ou la présente charte et qu'elle ne porte pas atteinte à la sécurité et au bon fonctionnement des systèmes d'information de l'État.

3.1 Postes de travail

Les postes de travail 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 :

- les postes de travail sont utilisés à des fins professionnelles et en aucun cas à des fins qui pourraient ternir l'image de l'État ;
- il est strictement interdit de tenter de modifier, de modifier ou de contourner les paramètres de sécurité informatique (p.ex. désactivation du logiciel antivirus, modification des droits d'accès ou suppression des traces d'audit fournies par les systèmes) ;

- il est interdit de modifier la configuration matérielle en retirant ou en installant des composantes (p.ex. graveur, disque supplémentaire, lecteur DVD, CD-ROM, modem, etc.) ;
- il est interdit de modifier la configuration logicielle des postes de travail en retirant des programmes ou en installant des programmes téléchargés depuis Internet ou reçus par courrier électronique ou en provenance de toute autre source ;
- les postes de travail sont verrouillés lorsque l'utilisateur quitte son poste, en activant le blocage d'accès (sous Windows : ⊞ + L ou CTRL + ALT + DELETE) ;
- il est recommandé d'éteindre le poste de travail hors des heures de service.

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 ;
- les utilisateurs doivent faire preuve d'une extrême vigilance lorsqu'ils reçoivent un e-mail provenant d'Internet avec un fichier attaché ou contenant un lien vers un autre site, surtout si celui-ci est de provenance inconnue ou douteuse. Les messages électroniques peuvent servir de vecteur à la transmission de code malveillant (virus, rançongiciels, chevaux de Troie, etc.) ;
- le transfert de courriers électroniques à caractère professionnel d'une adresse professionnelle vers une adresse privée est strictement interdit ;
- la diffusion de messages qui peuvent porter atteinte à la réputation de l'État est strictement interdite ;
- en cas de transmission d'informations confidentielles à des destinataires externes, il est recommandé de procéder à un chiffrement adéquat des informations ;
- en cas de réception de messages à caractère violent, raciste ou pornographique, l'utilisateur avertit son responsable informatique ;
- la propagation de chaînes de lettres est interdite ;
- 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 génèrent des traces au niveau des systèmes de gestion sécurisée des accès Internet. Ces traces peuvent être enregistrées et conservées dans le but exclusif d'une exploitation en cas d'incident de sécurité majeur, ceci en conformité avec la législation en vigueur.

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

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

- le contournement des dispositifs de sécurité est interdit ;
- toute transmission interne ou externe d'informations à caractère indécent, obscène, profanateur, menaçant, frauduleux ou illégal est interdite ;
- le téléchargement 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 concernant l'État 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.

3.4 Ordinateurs portables

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

- l'ordinateur portable est un équipement personnel et seul l'utilisateur auquel il est affecté est autorisé à l'utiliser. (Cette règle ne s'applique pas aux ordinateurs portables spécifiquement désignés pour être partagés) ;
- 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 une voiture ;
- 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 zones où des personnes mal intentionnées pourraient avoir une vue directe de l'écran. L'utilisation de filtres de confidentialité est fortement recommandée.

3.5 Supports de stockage amovibles (clés USB, disques amovibles, CD/DVD)

Les supports de stockage amovibles contenant des informations non publiques doivent être protégés lorsqu'ils sont laissés sans surveillance.

Les informations confidentielles 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.

3.6 Appareils mobiles (smartphones, tablettes)

Les règles de sécurité suivantes sont applicables :

- l'utilisateur charge uniquement les données essentielles à son besoin métier sur son appareil mobile ;
- 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 incidents de sécurité[1] ;
- le "jailbreak" ou l'installation de logiciels / firmware conçus pour avoir accès à des fonctionnalités non conformes sont interdits ;
- l'installation de logiciels piratés ou de contenus illégaux est interdite ;
- la connexion filaire ou sans fil des appareils mobiles non gérés par l'État (i.e. tout appareil privé) aux postes de travail et ordinateurs portables de l'État n'est pas autorisée ;
- les utilisateurs ne devraient pas utiliser les postes de travail ou 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 ;
- le transfert de données entre les appareils mobiles et les postes de travail ou ordinateurs portables de l'État est autorisé sous réserve qu'il s'agit de données professionnelles transmises moyennant l'utilisation d'outils autorisés, gérés et mis à disposition par l'État ;
- 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.

3.7 Réseaux sans-fil (WiFi)

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 :

- de s'assurer que le pare-feu et l'antivirus soient activés ;
- de choisir une authentification forte lors d'une connexion à une application ;
- de désactiver le réseau sans-fil à la fin d'utilisation.

De manière générale, les utilisateurs évitent au maximum l'utilisation de réseaux WiFi qui ne sont pas gérés par l'État (WiFi publics).

[1] Soit le Helpdesk de l'entité si cette fonction existe, sinon le responsable informatique. Si aucune de ces fonctions n'est définie, alors la notification doit être faite au GovCERT. Il revient au Helpdesk respectivement au responsable informatique d'évaluer l'impact de l'incident. En cas d'incident d'envergure, notamment s'il y a un risque d'impact sur des tiers, l'incident est à notifier sans délai au GovCERT.

3.8 Imprimantes

L'utilisation des imprimantes est réservée aux besoins professionnels. L'utilisateur veille à protéger la confidentialité des informations qu'il imprime et récupère les documents imprimés dès que possible.

4 Réagir en cas d'incidents de sécurité

Les utilisateurs sont tenus de signaler tout incident de sécurité dans les plus brefs délais à l'instance gestionnaire des incidents de sécurité[1].

En cas d'attaque sur une station de travail ou un ordinateur portable connecté au réseau, il est demandé à l'utilisateur de déconnecter la machine du réseau sans toutefois l'arrêter ou la redémarrer afin que les spécialistes puissent faire les analyses nécessaires.

Voici quelques exemples d'incidents de sécurité qui doivent faire l'objet d'un signalement par l'utilisateur concerné :

- vol de matériel ;
- erreur humaine mettant en danger les informations ;
- une violation de l'intégrité, de la confidentialité et de la disponibilité de l'information ;
- un changement non autorisé apporté au système ;
- accès non autorisé ou tentative d'accès ;
- découverte d'une vulnérabilité ou d'une faille de sécurité ;
- perception d'une menace.

5 Sensibilisation

En complément de cette charte de bonne conduite, plusieurs autres sites internet de sensibilisation et de formation à la sécurité des systèmes d'information sont disponibles et consultables par les utilisateurs :

- > http://www.govcert.lu
- > http://www.cert.lu
- > http://www.bee-secure.lu
- > http://www.cases.lu
- > http://www.cybersecurity.lu

L'ensemble du personnel de l'État est invité à suivre des formations (par exemple cours INAP ou formations organisées par l'entité) dans le cadre de la sensibilisation.

[1] Soit le Helpdesk de l'entité si cette fonction existe, sinon le responsable informatique. Si aucune de ces fonctions n'est définie, alors la notification doit être faite au GovCERT. Il revient au Helpdesk respectivement au responsable informatique d'évaluer l'impact de l'incident. En cas d'incident d'envergure, notamment s'il y a un risque d'impact sur des tiers, l'incident est à notifier sans délai au GovCERT.