# Ligne directrice sécurité de l'information & vie privée :

# Utilisation de l'e-mail et de la communication en ligne

**(BLD ONLINE)**

# TABLE DES MATIERES

# 1. Introduction

Le présent document fait intégralement partie de la politique relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution de sécurité sociale. Le maintien, le suivi et la révision du présent document relèvent de la responsabilité du service Sécurité de l'information de l'institution de sécurité sociale.

Le présent document contient plusieurs règles de bonne conduite relatives à l'utilisation de l'e-mail et des moyens de communication en ligne mis à la disposition du collaborateur[1]. Pour rappel, le collaborateur joue un rôle essentiel dans la sécurité en général de l'institution; il est donc le premier bastion de défense contre les risques liés au traitement d'informations sensibles. Dès lors, il est important que chaque collaborateur comprenne ses droits et devoirs en la matière, ainsi que les bonnes pratiques en vigueur au sein des institutions de sécurité sociale.

# 2. Utilisation de l'e-mail et des moyens de communication en ligne

Toute organisation souscrit les directives 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:

a. Chaque organisation doit intégrer les règles dans leur lignes directrices sécurité de l'information et vie privée comme spécifié dans annexe C de cette ligne directrice. Ces règles sont décrits dans les paragraphes :
   1. Utilisation de l'e-mail et des moyens de communication en ligne
   2. Contrôles

b. Chaque organisation doit exercer un contrôle permanente sur l'utilisation de l'e-mail et la communication en ligne dans le cadres des objectives suivants:
   1. La protection de la réputation et les intérêts de l'organisation;
   2. la prévention de faits illicites, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui;
   3. la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'institution, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'institution;
   4. le respect des principes clés.

[1] Référence : Conforme à la norme 8.1 des normes minimales de la Banque Carrefour de la sécurité sociale.

# Annexe A: Gestion documentaire

Gestion des versions

| Date | Auteur | Version | Description du changement | Date approbation | Date entrée en vigueur |
|---|---|---|---|---|---|
| 2013 | | V2013 | Première version | 17/07/2013 | 01/08/2013 |
| 2017 | | V2017 | Intégration UE 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 de politique, 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 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", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- ISACA, "COBIT 5 for Information Security", Mai 2012, 220 p.


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

# Annexe C: Utilisation de l'e-mail et des moyens de communication en ligne

Ci-après figurent les directives pour la protection des informations sur le lieu du travail qui doivent être implémentées au sein d'une institution.

### 2.1. Généralités

Comme tous les instruments de travail, l'utilisation des moyens de communication de l'institution est en principe réservée à des fins professionnelles. Toutefois, l'usage limité à des fins privées du système de messagerie et d'internet est accepté, à condition que cet usage soit occasionnel, ne porte pas atteinte au bon fonctionnement du réseau, du travail ou de la productivité et qu'il ne constitue pas une infraction à la législation en vigueur[2].

Dans le cadre professionnel, les seuls moyens de communication admis par l'institution sont l'e-mail et les services de communication en ligne propres à l'institution. Les autres moyens de communication tels que blogs, vlogs, chat, Skype, whatsapp, telegram, wechat, bbm, viber et les autres services de communication en ligne ne peuvent donc être utilisés que si les directives internes relatives à l'utilisation de ces moyens de communication le permettent. L'utilisateur respectera strictement les règles d'utilisation de ces moyens de communication.

Le collaborateur s'engage à signaler immédiatement tout dysfonctionnement ou tout abus (et plus particulièrement la constatation de virus, tentative d'intrusion ou hacking...) des fonctionnalités de l'e-mail et de la communication en ligne, que ce soit au niveau des ordinateurs centraux, du réseau, des ordinateurs locaux, des logiciels, etc. Le phishing en particulier constitue un réel danger de tromperie et d'escroquerie des collaborateurs.

La direction de l'institution se réserve le droit de contrôler l'usage de l'e-mail et des moyens de communication en ligne suivant les règles exposées au point 5.3.

### 2.2. Utilisation de l'e-mail et des moyens de communication en ligne

Vu les risques inhérents liés à l'usage de l'e-mail au sein de l'institution, il est indispensable de rappeler certaines bonnes pratiques en la matière :

- L'expéditeur d'un e-mail est responsable du contenu de celui-ci. Il est dès lors formellement interdit aux collaborateurs d'envoyer des mails dont le contenu aurait un caractère illégitime et/ou contraire aux convenances et aux bonnes mœurs (notamment e-mails avec contenu obscène, politique, raciste, xénophobe, discriminatoire,…).
- En aucun cas, l'e-mail et les autres moyens de communication en ligne ne peuvent se substituer aux moyens de transfert imposés par la Banque Carrefour de la sécurité sociale pour l'échange de données à caractère personnel. A ce propos, l'usage de la messagerie électronique et des moyens de communication en ligne doit être en conformité avec les recommandations en matière de protection de la vie privée. Dès lors, aucune donnée à caractère personnel ne peut être transmise par e-mail et des moyens de communication en ligne. Préalablement à l'envoi de fichiers sensibles via e-mail et par des moyens de communication en ligne, le collaborateur doit veiller à ce que ceux-ci soient cryptés.
- L'utilisation de l'e-mail et des moyens de communication en ligne à des fins personnelles est autorisée. Cet usage à des fins privées ne peut cependant en aucun cas constituer une infraction aux présentes directives, ni à aucune autre disposition légale ou réglementaire. Si le collaborateur utilise l'e-mail et les moyens de communication en ligne à des fins personnelles, il est tenu, dans toute la mesure du possible, de supprimer de ses messages toute mention relative à l'employeur, pour éviter tout risque de confusion avec le volet professionnel (il doit insérer à cet effet la mention « Privé » ou « personnel » dans la partie « sujet »).

[2] Politiques communes aux institutions de la sécurité sociale relatives à l'usage d'internet et de l'e-mail

- En cas d'absence prolongée (plusieurs jours), le collaborateur doit, dans toute la mesure du possible, prévoir l'envoi d'une réponse automatique informant ses correspondants qu'il est absent (« out of office »). Idéalement, cette mesure s'applique uniquement aux destinataires de la sécurité sociale.
- Le collaborateur s'engage à ne pas envoyer inutilement des e-mails à de grands groupes d'utilisateurs (ex: "to all users"), ni à ajouter des fichiers de taille importante pouvant nuire au fonctionnement du système. Les fichiers de taille importante sont placés de préférence sur le système interne de gestion de document de l'institution. Les e-mails correspondants contiennent les liens vers ces fichiers.
- Le transfert systématique (Auto-Forward) de tous les messages électroniques arrivant dans une boîte aux lettres vers une adresse mail et/ou des moyens de communication en ligne externes à l'institution est totalement interdit puisque les informations sensibles professionnelles contenues dans ces messages sont aussi automatiquement transmis.

### 2.3. Naviguer en toute sécurité sur internet

Internet est avant tout mis à la disposition à des fins professionnelles. Une exploration modérée à titre personnel dans une optique d'apprentissage et de développement personnel est toutefois acceptée. Dans cette optique, le collaborateur doit être conscient des lignes directrices suivantes:

- l'institution se réserve le droit de limiter l'accès à internet;
- la navigation sur internet n'est pas sans danger et il n'est pas rare de se trouver confronté à des attaques par l'intermédiaire de certains sites. Dès lors il est rappelé au collaborateur :
    - qu'il représente toujours l'institution lorsqu'il navigue sur internet. En effet, de nombreux sites internet visités gardent une trace du passage et, dans certains cas, identifient la provenance du visiteur et son identité électronique, et par conséquent celle de l'institution ;
    - qu'il ne peut pas modifier la configuration de son navigateur, ni désactiver les logiciels de protection (anti-virus, anti-spam, firewall, …);
    - de quitter les sites non professionnels s'il suspecte que ceux-ci ne correspondent pas à ceux recherchés.
- Il est également interdit de consulter des sites contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que des sites racistes, des sites prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion ou des convictions politiques d'une personne ou d'un groupe de personnes. De même, Il est aussi interdit d'utiliser internet dans le cadre d'une activité illégale, quelle qu'elle soit.
- Pour tout ce qui est relatif au téléchargement de fichiers au travers d'internet, l'utilisateur se limitera spécifiquement à ce qui est strictement nécessaire, et ce uniquement dans le cadre professionnel et pour autant que le téléchargement soit autorisé par l'institution.
- Le collaborateur n'utilisera pas des services de partage de fichiers en ligne (généralement gratuits) non sécurisés qui permettent de partager et/ou de charger de nombreux fichiers et/ou de gros fichiers au moyen de services de partage de fichiers en ligne (gratuits) tels que dropbox, onedrive, icloud, google drive, box, wetransfer, sharefile, nomadesk. A cet effet, le collaborateur vérifiera, au préalable, auprès du conseiller en sécurité de l'information quels services de partage de fichiers en ligne sont sûrs et autorisés (tels que SFTP, spideroak, owncloud) ou quels outils il doit utiliser pour partager des fichiers en toute sécurité au moyen de services de partage de fichiers en ligne (tels que boxcryptor, viivo, cloudfogger, sookasa).
- Selon la politique interne de l'institution relative aux droits ou non d'installation de programme par l'utilisateur final, le collaborateur doit s'assurer avant toute installation de fichier ou de programme, que celui-ci provient d'une source fiable, qu'il n'y a aucun conflit avec la politique de licence appliquée au sein de l'institution et qu'il n'y a aucun risque de dommage au niveau de la protection des systèmes.

### 2.4. Contrôle

L'institution devrait exercer un contrôle global et permanent dans le cadre des objectifs suivants:

1. la prévention de faits illicites, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
2. la protection des intérêts de l'institution;
3. la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'institution, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'institution ;
4. le respect des principes et règles d'utilisation de l'e-mail et des moyens de communication en ligne décrits aux points 5.1 et 5.2.

Cependant, l'institution doit respecter les principes de base émis par la Convention collective de travail n°81[3] du 26/04/2002 lors du contrôle de l'usage de l'e-mail et des moyens de communication en ligne. Il s'agit des principes de base suivants :

1. principe de finalité,
2. principe de proportionnalité,
3. principe de transparence,
4. modalités d'individualisation des données de communication électroniques en réseau.

Pour rappel, l'objectif de la convention collective de travail est de garantir le respect de la vie privée sur le lieu de travail lorsqu'une collecte de données de communication électronique est organisée dans le but d'opérer un contrôle de celle-ci.

[3] la convention collective de travail n°81 est de fait une recommandation de la Commission de la protection de la vie privée.

# Annexe D: 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** | |
| **Sécurité des ressources humaines** | **Oui** |
| **Gestion des actifs** | |
| **Protection de l'accès** | **Oui** |
| **Cryptographie** | |
| **Sécurité physique et environnementale** | |
| **Protection des processus** | |
| **Sécurité de la communication** | **Oui** |
| **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** | |
| **Naleving** | |

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