Charte Informatique

Exemple Label Cyber-Safe

Avertissement : le présent document est fourni dans le cadre de la labellisation Cyber-Safe et nécessite d'être adapté à votre situation. Son usage ne garantit pas la conformité aux exigences du Label.

1 Objectif

Ce document a pour but d'énoncer les règles concernant l'accès aux ressources informatiques ainsi que l'utilisation de ces dernières.

L'utilisation du système d'information et de communication doit se faire exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte. Dans un but de transparence à l'égard des utilisateurs·trices, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des salarié·es, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Elle ne saurait se substituer à l'application du cadre légal en vigueur.

2 Champ d'application

La charte informatique s'applique à tous les collaborateurs·trices, stagiaires, etc. (ci-après utilisateurs·trices) autorisé·es à se servir des équipements informatiques du Label Cyber-Safe.

Chaque utilisateur·trice s'engage formellement à respecter les dispositions de ce document.

3 Devoirs de l'employeur

Dans le cadre des mesures prises pour préserver ses intérêts et certains équipements informatiques, l'employeur s'engage à respecter et à protéger la personnalité de l'utilisateur. Il ne consultera pas les données privées des utilisateurs, pour autant qu'elles puissent être identifiées comme telles (en-tête de message, nom de dossier ou de fichier).

En cybersécurité, la vigilance des collaborateurs est une des meilleures barrières aux intrusions ! Il est donc indispensable que les utilisateurs soient attentifs et signalent immédiatement au support technique ou à la direction tout élément suspect ou soupçon de compromission de données ou d'appareil : e-courriel « douteux », message inhabituel, ressource inaccessible, fichier au contenu bizarre, fenêtre indiquant que quelqu'un est connecté à distance sans que cela soit prévu, message de l'antivirus, etc. L'employeur s'engage à traiter les informations remontées en toute confidentialité.

4 Devoirs des utilisateurs trices

4.1 Règles de sécurité : droits d'accès

Le droit d'accès aux ressources et aux fichiers informatiques est accordé par un compte qui est **personnel et incessible**. Il doit être protégé par un mot de passe dont la construction est sûre, d'au moins 10 caractères, comprenant des lettres minuscules, majuscules, des chiffres et des caractères spéciaux, dont au moins un caractère de chacune de ces catégories. En outre, il ne doit contenir ni le nom, ni le prénom, ni aucune information facilement déductible sur l'utilisateur·trice ; **il ne doit pas non plus reprendre un mot de passe (tout ou partie) utilisé à titre privé**.

L'authentification à deux facteurs[1] est exigée. Les moyens d'authentification proposés doivent être strictement personnels (téléphone, courriel privé, …) et eux-mêmes protégés par mot de passe.

Aucune divulgation du mot de passe n'est autorisée. L'utilisateur·trice ne se sert que des comptes pour lesquels il a reçu une autorisation.

L'utilisateur·trice s'engage à ne pas se connecter sur un wifi public – même sécurisé – sans utiliser de VPN. A défaut, il utilise le partage de la connexion avec son téléphone mobile.

4.2 Obligation de confidentialité

L'accès par les utilisateurs·trices aux informations et documents conservés sur les systèmes et réseaux informatiques (internet compris) est limité à ceux qui leur sont propres ainsi qu'à ceux qui sont publics ou partagés. Il est interdit en particulier de prendre connaissance intentionnellement d'informations transitant sur les réseaux ou détenues par d'autres utilisateurs·trices, quand bien même ces derniers ne les auraient pas protégées.

[1] Un deuxième moyen d'authentification prédéfini est exigé pour toute connexion à partir d'un nouvel emplacement (appareil, application, …)

4.3 Logiciels : installation et copie

Les logiciels ne sont installés sur les postes qu'avec l'accord préalable du·de la webmaster.

L'utilisateur·trice s'engage à ne pas installer sur le poste de travail, ou tout autre ordinateur du réseau, d'environnements de stockage Cloud (par exemple : Dropbox, Google Drive….) ;

Les copies personnelles ou les installations privées des logiciels sous licence du Label Cyber-Safe ne sont pas autorisées.

4.4 Postes de travail et équipements associés

Modifications du réseau et des câbles de connexion : les modifications sont exécutées exclusivement par le·la webmaster ou une personne autorisée par ce·tte dernier·ère.

Modifications des configurations : les modifications sont effectuées exclusivement par le·la webmaster ou par une personne autorisée par ce·tte dernier·ère.

4.5 Équipements privés

L'utilisateur·trice utilise exclusivement le matériel professionnel qui lui est mis à disposition pour effectuer son activité professionnelle.

Il·elle s'engage à ne pas connecter au poste de travail, ou à tout ordinateur du réseau, d'appareils électroniques privés tels que notamment smartphones, clés USB, systèmes externes et tablettes.

L'utilisateur·trice qui souhaite, à titre exceptionnel, connecter un équipement privé (laptop, etc.) sur le réseau informatique doit en demander l'autorisation motivée à la Direction ou au·à la webmaster.

Il·elle s'engage à ne pas installer la suite Office à partir de son compte professionnel sur un appareil privé, ni à y synchroniser les fichiers du Label Cyber-Safe. Il·elle est toutefois autorisé·e à configurer la messagerie électronique sur ses appareils.

Si pour une raison exceptionnelle, l'utilisateur·trice doit impérativement se connecter sur un appareil non professionnel, il·elle utilise exclusivement Office online (dans un navigateur).

4.6 Signalement des incidents

Afin d'assurer un fonctionnement optimal des infrastructures et de bonnes conditions de travail pour tout le monde, les collaborateurs sont priés de signaler immédiatement tout problème technique, panne ou casse (par ex. perte de connexion réseau, matériel défectueux ou abîmé, bruit, fumée ou autre élément suspect avec un PC ou accessoire). Cela afin que le support technique ou la personne responsable puisse réagir rapidement et, le cas échéant, contacter le dépanneur ou commander la pièce de rechange.

La perte, l'oubli ou le vol, en particulier d'un PC portable, d'une tablette, d'un smartphone ou d'un dispositif de stockage (disque dur, clé USB, carte mémoire…), dans un lieu connu ou non, doit impérativement être signalé immédiatement au support technique.

En cybersécurité, la vigilance des collaborateurs est une des meilleures barrières aux intrusions ! Il est donc indispensable que les utilisateurs soient attentifs et signalent immédiatement au support technique ou à la direction tout élément suspect ou soupçon de compromission de données ou d'appareil : email « douteux », message inhabituel, ressource inaccessible, fichier au contenu bizarre, fenêtre indiquant que quelqu'un est connecté à distance sans que cela soit prévu, message de l'antivirus, etc.

Si quelqu'un pense avoir cliqué où il ne fallait pas dans e-mail, il est primordial de ne pas paniquer ou minimiser/dissimuler le problème, mais de faire remonter l'information immédiatement pour que des contrôles puissent être menés et, le cas échéant, les « portes » fermées à temps !

5 Internet

5.1 Principes généraux

L'internet doit être consulté par l'utilisateur·trice uniquement à des fins professionnelles et dans le cadre des fonctions qui lui sont attribuées.

L'utilisation de l'internet à des fins personnelles est autorisée à condition que les ressources consommées soient infimes et que ni le temps de travail ni la capacité du réseau ne s'en trouvent affectés. La consultation à des fins personnelles doit par définition demeurer occasionnelle et accessoire.

La diffusion d'informations personnelles ou publicitaires n'ayant pas trait à l'activité professionnelle est strictement interdite.

L'utilisateur·trice n'est pas autorisé·e à s'abonner à des services d'informations payants, sauf autorisation préalable.

5.2 Utilisation abusive

Tout·e utilisateur·trice doit veiller à utiliser l'internet sans faire courir au Label Cyber-Safe des risques d'ordre légal, réglementaire ou opérationnel et sans compromettre la réputation de l'association. Toute utilisation abusive ou illégale est strictement interdite. L'accès, le chargement ou téléchargement, et la transmission de données dont le contenu est contraire à la loi, à l'éthique, à la morale ou bien d'un caractère injurieux, offensant, humiliant ou dénigrant sont expressément défendus.

L'employeur se réserve le droit de bloquer, sans préavis, l'accès à certaines catégories de sites Internet, notamment :

- Sites de messagerie non professionnelle, y compris site de messagerie instantanée ("chat") ;
- Sites de transactions financières (notamment les sites boursiers) ou ceux payants ;
- Sites de jeux et de paris ;
- Sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit ;
- Sites qui sollicitent trop fortement les systèmes d'information (par ex. connexion à des sites radiophoniques).

5.3 Téléchargement des informations

Les logiciels, données et fichiers (y compris les fichiers comprenant un contenu audio ou vidéo, voire les deux) ne peuvent être téléchargés à partir de l'internet vers les réseaux qu'à la seule condition qu'ils soient en rapport avec l'activité professionnelle. Ces opérations sont autorisées, étant entendu que les utilisateurs·trices veilleront à respecter le droit des parties tierces et à ne pas introduire de virus dans le réseau.

L'utilisateur·trice s'engage à ne pas copier illégalement des logiciels ou des fichiers protégés par un "copyright" (musique, film, etc.), à ne pas diffuser des informations appartenant à des tiers sans leur autorisation. Il·elle s'engage à mentionner ses sources lors de l'utilisation d'informations.

5.4 Communication électronique

L'utilisateur·trice se servira de son adresse répertoriée sur la messagerie électronique du Label Cyber-Safe pour toutes ses communications d'ordre professionnel. Il·elle veillera à rédiger ses messages avec la plus grande correction car le nom du Label Cyber-Safe apparaît dans son adresse.

Les envois en masse (chaîne) ou la rediffusion d'annuaires (spam) sont interdits.

La transmission de contenu confidentiel (dans le corps du message ou en pièce jointe) devra être crypté.

L'utilisateur·trice s'engage dans la mesure du possible à ne pas utiliser son compte de messagerie professionnel à des fins privées. Le cas échéant, il·elle veillera à préfixer les courriels de la mention « privé » ou les classera dans un dossier portant la mention « privé ». A défaut, ces courriels seront considérés comme professionnels.

5.5 Droits d'accès / Password

Le droit d'accès aux ressources et aux fichiers informatiques est accordé par un compte qui est **personnel et incessible**.

Mise à disposition de Bitwarden :

Afin de renforcer la sécurité de nos informations, le Label Cyber-Safe met à disposition de tous les employés l'outil de gestion de mots de passe Bitwarden.

- Tous les mots de passe utilisés dans le cadre de vos activités professionnelles doivent impérativement être conservés dans Bitwarden.

- Lors de la création d'un nouveau mot de passe, veuillez utiliser la fonction de proposition de mot de passe intégrée à Bitwarden pour garantir un niveau de sécurité optimal.

- Les mots de passe ne doivent pas être enregistrés dans le navigateur internet (Chrome, Edge, Safari,...)

En cas de doute ou pour toute question relative à l'utilisation de Bitwarden, veuillez contacter le service informatique.

Tous vos accès, mais surtout le mot passe de Bitwarden, doivent être protégés par un mot de passe dont la construction est sûre, d'au moins 12 caractères, comprenant des lettres minuscules, majuscules, des chiffres et des caractères spéciaux, dont au moins un caractère de chacune de ces catégories. En outre, il ne doit contenir ni le nom, ni le prénom, ni aucune information facilement déductible sur l'utilisateur ; **il ne doit pas non plus reprendre un mot de passe (tout ou partie) utilisé à titre privé**.

Proposition de méthodologie pour construire un mot de passe robuste :

Prendre les premières lettres d'une phrase simple :

- Sans lien avec votre vie/famille
- Avec un caractère pour marquer les espaces
- En changeant certaines lettres par un chiffre ressemblant
- La bonne longueur est entre 12 et 16 caractères

Exemple : **Eu**ropa **Pa**rk! **Ic**h **Li**ebe devient le mot de passe robuste : **3u.Pa! Ic.Li.**

Aucune divulgation du mot de passe n'est autorisée. L'utilisateur ne se sert que des comptes pour lesquels il a reçu une autorisation. Il ne peut en aucun cas transmettre un compte, interne ou client, qui lui est personnellement attribué.

Ces mêmes règles s'appliquent pour déterminer les mots de passe d'accès sur les sites internet utilisés à titre professionnel. La double identification doit être privilégiée. **En aucun cas le mot de passe de connexion à la session utilisateur ne doit être réutilisé.**

5.6 Logiciel utilisant l'intelligence artificielle

L'IA générative, telle que ChatGPT ou Bart, peut être un outil puissant pour vos activités professionnelles. Cependant, son utilisation doit être maitrisée afin d'éviter des conséquences non intentionnelles telles que la divulgation involontaire de données personnelles, sensibles ou confidentielles. Ce document fournit des lignes directrices pour une utilisation responsable et éthique de cette technologie.

Risques et utilisation acceptable:

- **Licences** : le Label Cyber-Safe dispose de licences pour l'utilisation de ChatGPT, son utilisation n'est autorisée que via ces comptes du Label Cyber-Safe.

- **Contenu généré** : La technologie d'IA générative peut produire du texte semblable à celui rédigé par des humains. Cependant, il est essentiel de se rappeler que ces systèmes peuvent générer du contenu biaisé ou inapproprié. Par conséquent, les employés du Label Cyber-Safe doivent utiliser ces technologies avec prudence, discrétion et maitriser le sujet du contenu.

- **Données sensibles** : Vous devez supposer que TOUTES les informations que vous téléchargez sur les systèmes d'IA générative feront partie de son ensemble de données d'apprentissage automatique et pourront être produites en réponse aux requêtes d'autres personnes.
  Par conséquent, les informations personnelles, sensibles, confidentielles ou d'autres informations couvertes par les lois sur la confidentialité des données ne doivent être entrées dans aucun système d'IA générative, quelles que soient les paramètres de contrôle des données activés dans le système.

- **Contenu Inapproprié** : Vous ne devez pas utiliser l'IA générative pour générer du contenu diffamatoire, discriminatoire ou illégal.

- **Usurpation d'Identité** : Vous ne devez pas utiliser l'IA générative pour usurper l'identité d'individus ou d'organisations.

- **Respect des Lois** : Vous ne devez pas utiliser l'IA générative pour générer du contenu qui viole les lois ou règlements relatifs à la vie privée.

- **Réputation du Label Cyber-Safe** : Vous ne devez pas utiliser l'IA générative pour participer à des activités pouvant nuire à la réputation du Label Cyber-Safe.

  Pour toute question ou préoccupation, veuillez contacter service informatique.

5.7 Utilisation de messageries instantanées

L'utilisation de messageries instantanées (WhatsApp, Slack,…) chez le Label Cyber-Safe est tolérée dans le cadre d'événements ou de projets, à condition de respecter les consignes suivantes :

- **Usage Exclusif pour l'organisation opérationnelle** : Les groupes WhatsApp doivent être utilisés uniquement pour la coordination et l'organisation opérationnelle d'évènements liés au Label Cyber-Safe. Toute autre utilisation est strictement interdite.

- **Aucune Information liée au client** : Il est interdit de partager des informations professionnelles dans un système de messagerie instantanée (Groupes WhatsApp, Apple Messenger, Slack, …). Cela inclut, mais sans s'y limiter, les informations confidentielles, les données sensibles, les discussions de projets ou toute autre information liée aux activités professionnelles du Label Cyber-Safe.

- **Respect de la Vie Privée** : Les membres des groupes doivent respecter la vie privée des autres participants. Aucune information personnelle ne doit être partagée sans le consentement explicite de la personne concernée.

- **Comportement Approprié :** Tous les membres des groupes WhatsApp doivent maintenir un comportement respectueux et approprié. Toute forme de harcèlement, de discrimination ou de langage inapproprié est strictement interdite.

- **Modération et Surveillance** : Les administrateurs des groupes sont responsables de la modération du contenu et doivent s'assurer que les règles d'utilisation sont respectées. En cas de non-respect des règles, les administrateurs doivent prendre des mesures correctives immédiates.

- **Suppression des Groupes** : Une fois l'événement terminé, les administrateurs doivent supprimer les groupes afin de garantir la suppression des discussions et qu'aucune discussion subsidiaire n'ait lieu.

Pour toute question ou préoccupation veuillez contacter le service informatique.

6 Contrôle

Il est d'une importance capitale pour la réputation du Label Cyber-Safe et le bon fonctionnement du Secrétariat que les utilisateurs·trices observent les instructions exposées dans cette charte.

Afin de vérifier le respect des règles visant à garantir la sécurité et la réputation du Label Cyber-Safe et à ne pas exposer celle-ci à des risques d'ordre légal, réglementaire et opérationnel, il sera procédé à des contrôles ponctuels et anonymes.

Pour effectuer ces contrôles, la Direction assistée du·de la webmaster observe les principes concernant le respect de la vie privée et la protection des données prescrits par les dispositions légales en vigueur. Ils n'analyseront les agissements d'un·e utilisateur·trice déterminé·e que lorsqu'une irrégularité a été constatée.

Lorsque l'analyse des journaux permet de mettre en évidence une utilisation abusive voire illégale des systèmes et réseaux informatiques, la Direction notifie un avis à tous les utilisateurs·trices faisant état :

- Des présomptions d'actes illicites
- Des mesures prises, en l'occurrence la collecte d'informations pendant une période déterminée.

Si les abus persistent, les données recueillies seront exploitées de façon nominative.

7 Sanctions

Toute utilisation abusive de l'internet et tout comportement contrevenant aux dispositions de cette charte sont expressément interdits. Les contrevenant·es sont passibles de sanctions pouvant aller de mesures disciplinaires, jusqu'au renvoi ou même des poursuites judiciaires.

Nom et Prénom :

Lieu et date :

Signature :

À considérer en complément du point 4.5 de la Charte ci-dessus, selon pertinence:

Gestion des équipements privés :

L'utilisateur-trice qui se connecte aux ressources informatiques de l'organisation avec des équipements privés garantit :

- Leur innocuité, soit :
  - L'installation des correctifs de sécurité du fournisseur du logiciel de base (OS)
  - La mise à jour des suites installées
  - La mise à jour des anti-virus
  - La relève des alertes
- Le respect par ses logiciels et fichiers de tous les droits de propriété intellectuelle.
- L'accès à l'appareil doit être protégé par un mécanisme d'authentification tel qu'un mot de passe ou un code de verrouillage.

L'utilisateur-trice qui stocke des données ou des accès à des données sensibles de l'organisation sur des équipements privés garantit le chiffrement de son disque.