

**Nom du client**

**Charte de la sécurité de l'information**

Informations générales

Version : 1.5

État : Draft

Projet : Charte de la sécurité de l’information

Mise en vigueur : 11/12/2019

Représentant : Nom du représentant

# Mot de la direction

Dans le cadre de sa mission, notre organisme traite des informations sensibles qu’il faut protéger. Pour assurer la sécurité de ces informations, j’ai décidé de mettre en place une charte de sécurité.

Tous les collaborateurs sont invités à lire ce document et à appliquer les bonnes pratiques qui y sont décrites.

…………..

…………..

<la\_direction>

# Usage privé au travail

Il est reconnu un droit d'usage privé des moyens mis à disposition par la société, seulement s’il est utilisé dans des limites du raisonnable et d’une façon responsable. Cet usage ne doit occasionner aucun trouble ou dysfonctionnement du système d’information et ne doit ni perturber le travail de l’employé lui-même, ni celui de ses collègues.

# Usage du système d’information

Les règles suivantes doivent être respectées :

* il est interdit d'utiliser les ressources de la société à des fins qui pourraient nuire à l’intégrité de personnes physiques ou morales ou à l’image de la société ;
* la législation en vigueur est connue de tous et appliquée ;
* les employés ne peuvent sans autorisation préalable, outrepasser les droits et autorisations qui leur ont été attribués, c'est-à-dire modifier, reproduire, détruire ou lire des informations qui ne leur sont pas destinées ;
* collaborer avec les personnes responsable de la maintenance, afin de faciliter l'identification et la correction de problèmes ou d'anomalies pouvant survenir ;
* le matériel mis à disposition du personnel sera utilisé, manipulé ou stocké avec les soins nécessaires pour éviter toute détérioration ;
* les employés ne peuvent sans autorisation préalable, sortir du matériel ou de l’information de l’enceinte de la société.

# Gestion des mots de passe

Le mot de passe doit être :

* changer de façon régulière (au moins 1 fois par an) ;
* avoir une longueur minimale de 10 caractères ;
* être composé au minimum de lettres majuscules, minuscules et de chiffres ainsi que des signes de ponctuation.

L’employé est personnellement responsable de la protection de son mot de passe. Il lui est strictement interdit :

* de garder au-delà de la première utilisation, les mots de passe attribués par défaut ;
* d’utiliser des mots de passe facile à deviner (nom de l’utilisateur, le nom d’un animal domestique, une date de naissance, un numéro de téléphone, mot du dictionnaire, etc.) ;
* d’utiliser le même mot de passe pour plusieurs systèmes ;
* de donner son mot de passe à qui que ce soit ;
* d’envoyer ou de divulguer un mot de passe par email, téléphone, Internet, etc. ;
* de noter le mot de passe sans pour autant le protéger de la façon convenable.

Les comptes génériques connus par plus d’une personne sont également proscrits.

Une dérogation existe toutefois, pour les systèmes n’acceptant pas ces contraintes (code PIN d’un smartphone, par exemple).

# Usage du matériel électronique

Les employés qui ont à leur disposition un ordinateur s'engagent à :

* protéger l'accès à l'ordinateur par un mot de passe (ou code PIN pour les smartphones) ;
* bloquer l'accès à l'ordinateur avant de quitter le poste de travail, même pour un très court laps de temps ;
* ne pas laisser l’ordinateur à des personnes tierces, excepté aux personnes qui ont en charge sa maintenance ;
* ne pas installer de logiciel sans autorisation ;
* prendre les dispositions nécessaires, pour sauvegarder les informations stockées éventuellement sur leur poste local (pas de backups).

Les utilisateurs sont conscients que les informations personnelles éventuellement stockées sur le réseau ou dans les emails sont sauvegardées et conservées selon la politique de backup en vigueur.

# Usage des services internet (web)

L’usage d’internet doit se faire en respectant les règles suivantes :

* Lorsque l’utilisateur saisit des informations sensibles, il doit vérifier qu’il est bien sur le bon site en contrôlant sa barre d’adresse. De plus, pour éviter l’interception de données, il s’assurera que la connexion est sécurisée, notamment par la présence d’un cadenas sur son navigateur et que le l’URL de la page commence par « http**s** »;
* Il est interdit à tout utilisateur de surfer sur des sites à caractères insultants, racistes, pédophiles, diffamatoires, violents, ou qui nuiraient à autrui ou ne respectant pas la loi ;
* Le téléchargement qui pourrait nuire au système d’information, ou ne respectant pas la législation sur les droits d’auteurs est interdit. En cas de doute, il faut s’abstenir.

# Usage du courrier électronique

Les courriers électroniques, tout comme les courriers traditionnels, sont soumis à des règles :

* ne pas envoyer des pièces jointes volumineuses pour éviter l’engorgement des boîtes mails ;
* au cas où un utilisateur recevrait un email qui ressemble à du spam ou à un hoax (c'est-à-dire de l'information non vérifiée), il réfléchit et valide lui-même ces informations avant de les accepter et de les transmettre. Dans le doute, il ne faut pas transmettre ce genre de contenu ;
* l’utilisateur ne doit pas cliquer sur des liens contenus dans les mails sans avoir au préalable vérifié que la source est de confiance ;
* Le courrier électronique est un moyen de communication non sûr. Seules les données du type publiques peuvent être envoyées en clair, les autres données doivent être chiffrées avant d’être envoyées hors de l’organisme.

Les agissements suivants sont interdits :

* le spam ou l'envoi, à l’extérieur comme à l’intérieur de la société, de lettres à chaînes ou d’email de plaisanteries ;
* l’envoi de courriers électroniques qui ont des contenus répressibles par la loi luxembourgeoise ;
* Toute utilisation inappropriée qui peut mettre en péril la sécurité du système de courriers électroniques ou qui peut engendrer des préjudices pour la société est défendue.

# Bureau propre

Les papiers et supports informatiques amovibles contenant des informations sensibles ne doivent pas être laissés sans surveillance sur les bureaux. Spécifiquement, les papiers doivent être retirés rapidement des imprimantes, télécopieurs ou photocopieurs, et ne doivent pas être jetés dans les poubelles.

Les documents sensibles sont déchiquetés ou déposés dans un conteneur sécurisé.

# Mise au rebut

Tout équipement qui est mis au rebut ou réutilisé dans un autre contexte doit être vidé de toutes ses données de façon adaptée à la sensibilité des informations qui s’y trouvent.

# Sanctions

Le non-respect intentionnel, unique ou répété, de règles de la présente charte, des infractions flagrantes aux articles du code pénal, aux lois sur la protection de la vie privée, ainsi que tout non-respect du droit de la propriété intellectuelle peuvent entraîner des sanctions disciplinaires ou juridiques.