|  |
| --- |
| **Versioning** |
| **Version** | **Date** | **Mise à jour proposé par** | **Approbation faite par** |
| PRD-GSI-01/V01/20180802/MCM | 2018-08-02 | Moez Ghezal – Responsable formation | Mohamed chedly mhiri – SMQ |
| PRD-GSI-01/V02/20190116/YBK | 2019-01-16 | Moez Ghezal – Responsable formation | Yassine ben khaled – RSI |
| PRD-GSI-01/V03/20200108/YBK | 2020-01-08 | Sabrine Madhi – Technicienne informatique | Yassine ben khaled – RSI |

**Politique d’usage et de la sécurité du système d’information**

**Définition et Objectif :**

Le système d’information est constitué de l’ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à la disposition de l’utilisateur.

 L’informatique nomade, constituée par les assistants personnels, les ordinateurs portables, les téléphones portables, …, est également un des éléments constitutifs du système d’information.

 Le bon fonctionnement du système d’information suppose le respect des dispositions législatives et réglementaires qui s’imposent et notamment, la sécurité, la performance des traitements et la conservation des données personnelles.

 La présente charte définit les règles d’usage et de sécurité que l’entreprise et l’utilisateur s’engagent à respecter : **elle précise les droits et devoirs de chacun.**

L’entreprise porte à la connaissance de l’utilisateur la présente charte\*.

**Engagement de L’entreprise :**

L’entreprise s’engage à mettre en œuvre les moyens nécessaires destinés à assurer la sécurité du système d’information et la protection des utilisateurs et à former tous les intégrants et les sensibiliser des nouveaux enjeux en terme de la sécurité informatique :

* Formation à l’intégration.
* Une sensibilisation annuelle.
* Les ressources mises à disposition sont prioritairement à usage professionnel.

**Engagement de l’utilisateur**

L’utilisateur est responsable, en tout lieu, de l’usage qu’il fait du système d’information auquel il a accès. Il a une obligation de réserve et de confidentialité à l’égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d’éthique et de déontologie.

Les utilisateurs ont une responsabilité particulière dans l’utilisation qu’ils font des ressources mises à leur disposition par l’entreprise.

En tout état de cause, l’utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

**Article I. Champ d’application**

Un utilisateur est une personne physique (téléopérateur, technicien, administratif, personnel de service, personnel temporaire, stagiaire, visiteur autorisé...) autorisée à accéder à l'une des ressources du système d’information de l’entreprise.

 Les règles d’usage et de sécurité figurant dans la présente charte s’appliquent à l’entreprise ainsi qu’à l’ensemble des utilisateurs.

**Article II. Conditions d’utilisation des systèmes d’information**

Continuité de service : gestion des absences et des départs

 L’utilisateur est responsable de son espace de données à caractère privé dont le responsable SI doit détruire lors de son départ définitif. Les mesures de conservation professionnelles sont définies avec le responsable désigné au sein de l’entreprise.

**Article III. Principes de sécurité**

Règles de sécurité applicables :

L’entreprise met en œuvre les mécanismes de protection appropriés sur les systèmes d’information mis à la disposition des utilisateurs.

Les utilisateurs sont informés que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas un caractère personnel aux outils informatiques protégés.

Les niveaux d’accès ouverts à l’utilisateur sont définis en fonction du poste qui lui est conféré. La sécurité des systèmes d’information mis à sa disposition lui impose :

* De respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe (elle doit être sous forme de 8 caractères au minimum alphanumériques) ;
* De garder strictement confidentiels son (ou ses) mot(s) de passe et de ne pas le(s) dévoiler à un tiers ; Ne pas réutiliser les mots de passes des applications, sites ou logiciels publiques ou personnels.
* De respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe à caractère privé (en dehors de la société) ou d’un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition des utilisateurs nécessite plusieurs précautions :

***De la part de l’entreprise :***

***Règle 1 :***

Les ressources sensibles ne sont en aucun cas accessibles en cas d’absence (en dehors des mesures de continuité mises en place par la hiérarchie) ; l’accès est limité aux seules ressources pour lesquelles l’utilisateur est expressément habilité.

***Règle 2 :***

Des protocoles sécurisés sont déployés systématiquement pour tous les accès ainsi que celui réservé à la messagerie électronique.

***Règle 3 :***

Des mécanismes de surveillance sont mis en place et génèrent une alerte immédiate sur les
évènements de sécurité associés aux comptes utilisateurs disposant de privilèges
d’administration sur le domaine (ajout, modification…)

***Règle 4 :***

Une solution antivirale est mise en place disposant de fonctions d’administration/supervision centralisées, permettant notamment le suivi et contrôle du déploiement des mises-à-jour et la configuration d’une alerte (envoi d’un message électronique) pour traitement immédiat du virus détecté.

***Règle 5 :***

Les correctifs de sécurité sur les équipements réseaux & sécurité sont déployés au plus tard un mois après leurs publications par l'éditeur.

***Règle 6 :***

Les enregistrements et les données relatives aux clients (données stockées dans les messageries, archives des messageries stockées sur le serveur de fichiers …) sont supprimés périodiquement chaque 12 mois.

***De la part de l’utilisateur :***

***Règle 1 :***

Si l’utilisateur ne bénéficie pas d’une habilitation explicite, il doit s’interdire d’accéder ou tenter d’accéder à des ressources du système d’information, même si cet accès est techniquement possible

***Règle 2 :***

Ne pas connecter directement aux réseaux locaux des matériels non confiés ou non autorisés par le responsable SI.

***Règle 3 :***

Il est strictement interdit d’installer, télécharger ou utiliser des logiciels ou progiciels sans autorisation explicite du responsable SI.

***Règle 4 :***

L’utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d’information, etc. Il signale également à la personne responsable du site toute possibilité d’accès à une ressource qui ne correspond pas à son habilitation.

\* Voir l’annexe feuille d’émargement et l’affichage sur les tableaux d’affichage Production.