CHARTE INFORMATIQUE NOBILITO

Objectif :

Ce document présente les règles relatives à l'informatique et à l'internet devant être respectées par l'utilisateur du Système d'Information.

Évolutions du document :

Version	Date	Nature des modifications
1.0	06/07/2021	Création du document

PREAMBULE

Dans un but de transparence à l'égard des Utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources (ci-après la « Charte »).

I – Dispositions générales

A. Objet de la charte

La société NOBILITO, également notée entreprise dans la suite du document, met en œuvre un Système d'Information et de communication nécessaire à son activité : postes de travail, applications, bases de données, téléphones, outils de mobilité, accès Internet, etc. Cet ensemble sera noté Système d'Information dans la suite du document.

Ces ressources, qui sont mises à la disposition des salariés ou des prestataires tiers dans l'exercice de leurs missions, font partie du patrimoine de l'entreprise, elles demeurent donc sa propriété.

L'utilisation de ces ressources doit être uniquement professionnelle, sauf exception prévue dans la présente charte, et tournée vers la performance de l'entreprise et la satisfaction des clients.

La présente charte a pour vocation d'exposer :

- Les principales règles et précautions que tout utilisateur doit respecter et mettre en œuvre lors de l'utilisation des ressources du Système d'Information.
- Les mesures, moyens de contrôle et de surveillance pris, non seulement pour la bonne exécution du contrat de travail des salariés, dans le cadre de la responsabilité civile et pénale de l'employeur,
- Les mesures, moyens de contrôle et de surveillance pris pour le suivi de la bonne exécution de la prestation de tiers non-salariés (prestataires, sous-traitants, etc.) intervenant auprès de l'entreprise.

B. CHAMP D'APPLICATION DE LA CHARTE

1. Utilisateurs

Sauf mention contraire, la Charte s'applique à l'ensemble des Utilisateurs du Système d'Information de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, freelances ou sous-traitants (désignés « Utilisateur »).

A ce titre, elle doit être communiquée à tout Utilisateur, interne ou extérieur à l'entreprise.

Les contrats entre l'entreprise et tout tiers, donnant accès à des ressources du Système d'Information de l'entreprise, stipulent que les Utilisateurs s'engagent à respecter la présente Charte.

Les salariés veillent à faire accepter valablement les règles posées dans la Charte à toute personne à laquelle ils permettraient d'accéder au SI.

Les responsables des Utilisateurs extérieurs s'engagent à faire respecter la présente Charte par leurs salariés et éventuelles entreprises sous-traitantes.

2. Système d'Information

Le Système d'Information et de Communication de l'entreprise (désigné « SI ») est principalement constitué des postes de travail (stations, ordinateurs fixes et portables), de serveurs, d'applications (dont la messagerie), de bases de données, de périphériques (imprimantes, copieurs, clés USB, ...), d'outils de mobilité (tablettes, smartphones, ...), d'équipements réseaux, d'équipements téléphoniques, d'accès à Internet.

La composition du SI est indifférente à la propriété sur les éléments (matériels dont la propriété n'est pas celle de l'entreprise) qui le composent.

Pour des raisons de sécurité du réseau, le matériel personnel des salariés ne devra pas se connecter au SI de l'entreprise et ne devra contenir aucune donnée propriété de l'entreprise.

3. Autres accords sur l'utilisation du SI

La Charte est sans préjudice des accords particuliers pouvant porter sur l'utilisation du SI par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail.

4. Application de la Charte

En qualité d'Utilisateur du Système d'Information de l'entreprise, chacun s'engage à prendre connaissance et à appliquer l'ensemble des dispositions de la présente Charte.

C. PROTECTION DES RESSOURCES PAR L'ENTREPRISE

L'entreprise définit et met en œuvre les moyens appropriés, en l'état de la technique, pour protéger les Utilisateurs et pour protéger les ressources mises à leur disposition contre les risques sur le Système d'Information. L'entreprise met à disposition de chaque Utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

L'entreprise prend donc les engagements suivants :

- Se donner les moyens budgétaires, humains, techniques, afin de respecter cette Charte ;
- Prévoir un plan de continuité du service ;
- Limiter les accès aux ressources sensibles ;
- Acquérir les droits d'usage ou de propriété intellectuelle nécessaires à l'utilisation de ces ressources dans le cadre professionnel ;
- Respecter la législation quant à la protection des données personnelles lors de leur collecte, leur finalité de traitement, leur conservation, leur traitement et leur suppression. L'aspect de respect du Règlement Général sur la Protection des Données (RGPD) en est un point majeur. Pour plus d'information se rapprocher du DPO ou visiter le site wwww.cnil.fr

D'une manière générale, l'entreprise n'est pas tenue responsable du non-respect de cette Charte par l'Utilisateur et des conséquences qu'il engendre.

D. CONTROLE DE SECURITE

1. Contrôles automatisés

Le SI s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication.

Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils recensent toutes les connexions et tentatives de connexions au SI. Ils comportent notamment les données suivantes : dates, postes de travail, utilisateurs, adresse IP et objet de l'évènement. Ils permettent d'assurer le bon fonctionnement du SI et de protéger la sécurité des informations de l'entreprise en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des Utilisateurs.

Les Utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du SI. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et les suppressions de fichiers ;
- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers ;
- aux historiques d'appels.

L'attention des Utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements et veiller au respect des règles, dans le respect de la réglementation en vigueur.

Le DSI et la direction de l'entreprise sont les seuls destinataires de ces informations.

Ce traitement d'information quand il est sur des données personnelles et/ou sensibles fera partie d'une étude détaillée dans le registre de traitement.

2. Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service informatique ou par la Direction, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs Utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un Utilisateur, et sauf risque ou événement particulier, le service informatique ne peut ouvrir les fichiers expressément identifiés par le salarié comme personnels ou privés contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé au préalable et avec son consentement. Le salarié sera alors contacté par téléphone et par courrier électronique au préalable.

Le contenu des messages à caractère personnel des Utilisateurs (tels que définis dans la présente Charte point E), ne peut en aucun cas être contrôlé par le service informatique sans la présence de l'utilisateur.

3. Intervention à distance

Le service informatique peut prendre en main à distance le matériel des Utilisateurs en cas de demande d'assistance ou de nécessité de maintenance. Toute intervention à distance fait l'objet d'une autorisation préalable de l'Utilisateur du matériel concerné.

Les logiciels d'intervention à distance ne peuvent être utilisés qu'à des fins de maintenance ou d'assistance aux Utilisateurs, et ne peuvent en aucun cas être utilisés à des fins de contrôle en direct de l'Utilisateur.

4. Vidéosurveillance

L'entreprise a placé ses locaux sous vidéosurveillance afin d'assurer la sécurité de son personnel et de ses biens. Les images enregistrées dans ce dispositif ne sont pas utilisées à des fins de surveillance du personnel ni de contrôle des horaires.

La base légale du traitement est l'intérêt légitime (cf. article 6.1.f) du Règlement européen sur la protection des données.

Les employés de l'entreprise peuvent être filmés par le dispositif. Les visiteurs occasionnels des locaux de la société sont également susceptibles d'être filmés.

Les images peuvent être visionnées uniquement en cas d'incident, par le personnel habilité de l'entreprise et par les forces de l'ordre.

Les images sont conservées un mois.

En cas d'incident lié à la sécurité des personnes et des biens, les images de vidéosurveillance peuvent néanmoins être extraites du dispositif. Elles sont alors conservées sur un autre support le temps du règlement des procédures liées à cet incident et accessibles aux seules personnes habilitées dans ce cadre.

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter le Délégué à la Protection des Données à l'adresse suivante : dpo@nobilito.fr

E. DONNEES A CARACTERE PERSONNEL

Une réglementation spécifique (dont la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés et le règlement européen sur la protection des données qui entre en vigueur au 25 mai 2018) définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle prévus dans la Charte.

Ces traitements sont indiqués dans les registres des traitements disponibles à cet emplacement :

https://docs.google.com/spreadsheets/d/1MsaHCJSfR6-HI2QnxkhUDUYwsooXt2omz8OkwAmBSs8/edit?usp=sharing

Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée en 2004 et 2016 et au Règlement Général sur la Protection des Données, l'Utilisateur bénéficie d'un droit :

- d'accès aux données (limité à deux demandes d'accès par an et sous réserve de justifier de son identité),
- de rectification des données,
- à l'effacement des informations qui le concerne dans les conditions fixées à l'article 17 du Règlement Général sur la Protection des Données,
- à la limitation du traitement,
- de définir des directives générales et particulières définissant la manière dont il entend que soient exercés, après son décès, ses droits.

Tout Utilisateur bénéficie également d'un droit d'opposition au traitement de ses données à caractère personnel. L'Utilisateur dispose en outre d'un droit à la portabilité de ses données.

Conformément à l'article 20 du RGPD, l'Utilisateur concerné dispose du droit de recevoir les données à caractère personnel le concernant qu'il a fourni à l'entreprise, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable de traitement sans que l'entreprise, à laquelle les données à caractère personnel ont été communiquées, y fasse obstacle. Enfin, la personne concernée peut, le cas échéant, introduire une réclamation auprès des services de la CNIL (https://www.cnil.fr/fr/plaintes). Pour ce faire, elle peut s'adresser à la Cnil par courrier ou par téléphone (informations disponibles ici : https://www.cnil.fr/fr/vous-souhaitez-contacter-la-cnil).

L'entreprise a désigné un correspondant à la protection des données à caractère personnel : le Délégué à la Protection des Données (DPO). Ce dernier a pour mission de veiller au respect des dispositions réglementaires relatives à la Protection des Données Personnelles.

Le Délégué à la Protection des Données est obligatoirement consulté par le responsable des traitements préalablement à leur création. Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'entreprise au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

Le Délégué à la Protection des Données veille au respect des droits des personnes (droit d'accès, de rectification, d'opposition, d'effacement, de limitation du traitement et de portabilité). Un Utilisateur peut exercer ses droits en justifiant de son identité et en s'adressant au Délégué à la Protection des Données par email à l'adresse suivante : dpo@nobilito.fr

Conformément à l'article 9 du RGPD et sauf exceptions prévues audit article, l'entreprise ne procèdera à aucun traitement de données à caractère personnel d'un Utilisateur salarié ou externe qui révèlerait l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle.

En revanche, aux fins de gestion du personnel et de traitement des rémunérations, l'employeur est amené à solliciter des données personnelles concernant le salarié à l'occasion de la conclusion, l'exécution et la rupture du contrat de travail.

Outre les services internes de l'entreprise, les destinataires de ces données sont, à ce jour, les organismes de sécurité sociale, les caisses de retraite et de prévoyance, la mutuelle, Pôle Emploi, les services des Impôts et le service de médecine au travail ainsi que les Conseils de l'entreprise et le gestionnaire de paie. Ces informations sont réservées à l'usage des services concernés et ne peuvent être communiquées qu'à ces destinataires.

Par ailleurs, il est demandé à l'Utilisateur de ne pas transporter sans protection (telle qu'un chiffrement) des données sensibles, y compris les siennes, sur des supports non fiabilisés tels que des ordinateurs portables, clés USB, disques durs externes, etc.

F. INFORMATION DES UTILISATEURS

La présente Charte est affichée publiquement en annexe du règlement intérieur et est disponible à tous dans les documents « RH – Documents collectifs » de la Gestion Electronique des Documents.

Elle est par ailleurs communiquée individuellement à chaque Utilisateur. Elle est ainsi communiquée :

- Aux salariés lors de leur arrivée dans l'entreprise ;
- Aux autres Utilisateurs via courrier électronique ou en annexe des contrats de prestation ou de sous-traitance conclus.

Enfin, le service et le ou les prestataire(s) informatique sont à la disposition des Utilisateurs pour leur fournir toute information concernant l'utilisation du SI. Il informe les Utilisateurs régulièrement sur l'évolution des limites techniques du SI et sur les menaces susceptibles de peser sur sa sécurité.

Des opérations de communication internes sont organisées, de manière régulière, afin d'informer les Utilisateurs sur les pratiques d'utilisation du SI recommandées ou obligatoires. Chaque Utilisateur doit prendre connaissance et appliquer les pratiques communiquées.

G. PROCÉDURE APPLICABLE LORS DU DÉPART DE L'UTILISATEUR

Lors de son départ, l'Utilisateur doit restituer au service de l'informatique interne les matériels et données mis à sa disposition.

En outre, en cas de départ d'un Utilisateur de l'Entreprise, la personne dûment habilitée informe par écrit le Service informatique qui supprime les accès de cet Utilisateur aux Ressources.

Avant d'effectuer toute copie de documents professionnels, l'Utilisateur salarié doit obtenir l'autorisation écrite du chef de service et l'Utilisateur tiers celle de la direction de l'entreprise.

L'Utilisateur s'engage à :

- Procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations personnelles saisies.
- Restituer intégralement les supports d'informations selon les modalités prévues au contrat de la prestation ou à son contrat de travail.

H. FORMATION, SENSIBILISATION DES SALARIÉS

Les salariés seront formés pour appliquer les règles d'utilisation prévues par la Charte.

Des sessions de sensibilisation à la sécurité informatique seront organisées une fois par an au minimum. Des opérations d'hameçonnage factices pourront également être organisées à des fins didactiques.

I. SANCTIONS

Le manquement aux règles et mesures de sécurité de la Charte est susceptible d'engager la responsabilité de l'Utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du SI, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés pouvant aller jusqu'au licenciement.

Si le service informatique ou la Direction ont des doutes quant au respect des dispositions de la présente Charte par l'utilisateur, la Direction pourra suspendre temporairement l'accès de l'Utilisateur au SI le temps de réaliser des investigations.

Si le service informatique ou la Direction est convaincu que l'Utilisateur a refusé ou négligé de respecter une disposition de cette Charte, cette dernière pourra décider les mesures suivantes :

- soumettre l'affaire aux autorités judiciaires dans le cas où les activités constatées peuvent constituer des infractions de nature pénale ;
- prendre les mesures conservatoires nécessaires ;
- engager une procédure disciplinaire pouvant aller jusqu'au licenciement.

II – RÈGLES D'UTILISATION DES RESSOURCES

A. RÈGLES GÉNÉRALES

L'Utilisateur doit réserver l'usage des ressources du Système d'Information au cadre de son activité professionnelle. Un usage personnel des moyens de communication est toutefois admis à condition que cet usage reste exceptionnel et mesuré.

Il est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses missions, et de l'usage qu'il en fait. Il doit concourir à la protection des ressources, en respectant les consignes données par le service informatique ou la Direction, et en faisant preuve de prudence.

Chaque Utilisateur est également responsable du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Il doit être particulièrement vigilant sur les risques lors de l'utilisation d'outils informatiques personnels, ou appartenant à l'entreprise en dehors des lieux de cette dernière (domicile, hôtel, gare, lieux publics, …).

L'Utilisateur s'engage à :

- signaler au service informatique, ou à la Direction, toute violation ou tentative de violation de l'intégrité de ces ressources, et de façon plus générale tout incident ou anomalie ;
- signaler immédiatement toute faille de sécurité qu'il pourrait constater sur le Système d'Information ;
- signaler immédiatement la perte ou le vol d'un équipement qui lui avait été confié (portable, smartphone, disque dur externe, clé USB, …) et qui contient des données appartenant à NOBILITO, ou qui donne accès à son Système d'Information.

De manière générale, l'Utilisateur ne doit pas se livrer, en aucune circonstance, à l'une quelconque des activités suivantes :

- Utiliser des ressources de l'entreprise à des fins de harcèlement, menace ou d'injure et de manière générale violer les droits en vigueur.
- Utiliser les ressources de l'entreprise de manière à gêner l'accès des autres utilisateurs.
- Utiliser les ressources pour disposer d'un accès non autorisé à un ordinateur ou service.
- Utiliser les ressources pour se faire passer pour quelqu'un de fictif, réel ou anonyme.
- Utiliser les ressources pour charger, stocker, publier, diffuser ou distribuer des documents, informations, images, vidéos, …
    - A caractère violent, pornographique ou contraire aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs ;
    - A caractère diffamatoire et de manière générale illicite ;
    - Portant atteinte aux ressources de l'entreprise et plus particulièrement à l'intégrité et à la conservation des données de l'entreprise ;

    - Portant atteinte à l'image de marque interne et externe de l'entreprise ;
    - Et d'une manière générale, sans rapport avec l'accomplissement de la mission confiée à l'Utilisateur.

- Essayer de quelque manière que ce soit de découvrir les comptes ou les mots de passe d'autres utilisateurs, ou des services pour lesquels une autorisation d'accès appropriée n'a pas été octroyée ;
- Modifier les équipements qui lui sont confiés et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle ;
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par le service informatique ;
- Déplacer l'équipement informatique (sauf s'il s'agit d'un équipement mobile type ordinateur portable, téléphone mobile, clé USB, etc.) ;
- Nuire au fonctionnement des outils informatiques et de communications.

Les ressources mises à la disposition de tout utilisateur pourront faire l'objet de vérifications et de contrôles par l'entreprise, dans les limites prévues par la loi.

L'utilisateur doit entreposer les fichiers dont il dispose sur des emplacements précisés par l'entreprise et sauvegardés.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation applicable et notamment relative au droit de propriété intellectuelle, au secret des correspondances, aux données personnelles, aux systèmes de traitement automatisé de données, au droit à l'image des personnes et à l'exposition des mineurs aux contenus préjudiciables.

L'utilisateur ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le SI.

B. DROIT A LA DÉCONNEXION

1. Définitions

Par la présente charte, l'entreprise réaffirme l'importance d'un bon usage des outils informatiques en vue d'un nécessaire respect des temps de repos et de congé ainsi que de l'équilibre entre vie privée et familiale et vie professionnelle.

Il y a lieu d'entendre par :

- Droit à la déconnexion : le droit pour le salarié de ne pas être connecté à ses outils numériques professionnels en dehors de son temps de travail ;
- Outils numériques professionnels : outils numériques physiques (ordinateurs, tablettes, smartphones, réseaux filaires etc.) et dématérialisés (logiciels, connexions sans fil, messagerie électronique, internet / extranet, réseaux sociaux d'entreprise, etc.) qui permettent d'être joignable à distance ;
- Temps de travail : horaires de travail du salarié durant lesquelles il est à la disposition de son employeur et comprenant les heures normales de travail du salarié et les heures supplémentaires, à l'exclusion des temps de repos quotidien et hebdomadaires, des congés payés, des congés exceptionnels, des jours fériés et des jours de repos et des temps d'absences autorisées, de quelque nature que ce soit (absence pour maladie, pour maternité, etc…).

2. Sensibilisation à la déconnexion

Des actions de sensibilisation sont organisées à destination des managers et de l'ensemble des salariés en vue de les informer sur les risques, les enjeux et les bonnes pratiques liées à l'utilisation des outils numériques.

Dans ce cadre, l'entreprise s'engage notamment à :

- sensibiliser chaque salarié à l'utilisation raisonnée et équilibrée des outils numériques ;
- désigner au sein de l'entreprise des interlocuteurs chargés des questions relatives à l'évolution numérique des postes de travail.

Ces dispositifs seront régulièrement mis à jour pour être adaptés aux demandes et besoins des salariés et devront faire l'objet d'une concertation annuelle entre l'employeur et les salariés désignés.

En outre, tout salarié qui pourrait rencontrer des difficultés à exécuter sa mission en respectant ce droit à la déconnexion pourra solliciter un entretien par mail avec la Direction des Ressources Humaines et son Responsable hiérarchique afin de trouver une solution de rééquilibrage.

3. Lutte contre la surcharge informationnelle liée à l'utilisation de la messagerie électronique professionnelle

Afin d'éviter la surcharge informationnelle, il est recommandé à tous les salariés de :

- S'interroger sur la pertinence de l'utilisation de la messagerie électronique professionnelle par rapport aux autres outils de communication disponibles ;
- S'interroger sur la pertinence des destinataires du courriel ;
- Utiliser avec modération les fonctions copie (« CC ») ou copie cachée (« Cci ») ;
- S'interroger sur la pertinence des fichiers à joindre aux courriels ;
- Eviter l'envoi de fichiers trop volumineux ;

Indiquer un objet précis permettant au destinataire d'identifier immédiatement le contenu du courriel.

4. Lutte contre le stress lié à l'utilisation des outils numériques professionnels

Afin d'éviter le stress lié à l'utilisation des outils numériques professionnels, il est également recommandé à tous les salariés de :

- S'interroger sur le moment opportun pour envoyer un courriel/SMS/un message dans le réseau social d'entreprise ou appeler un collaborateur sur son téléphone professionnel (pendant les horaires de travail) ;
- Ne pas solliciter de réponse immédiate si ce n'est pas nécessaire ;
- Définir le « gestionnaire d'absence au bureau » pendant les périodes de repos, de congés et d'arrêt maladie sur la messagerie électronique et indiquer les coordonnées d'une personne à joindre en cas d'urgence ;
- Privilégier les envois différés lors de la rédaction d'un courriel en dehors des horaires de travail.

5. Droit à la déconnexion en dehors du temps de travail effectif

Les périodes de repos, congé et suspension du contrat de travail doivent être respectées par l'ensemble des acteurs de l'entreprise.

Les managers s'abstiennent, dans la mesure du possible et sauf urgence avérée, de contacter leurs subordonnés en dehors de leurs horaires de travail tels que définies au contrat de travail ou par l'horaire collectif applicable au sein de l'entreprise.

C. CONFIDENTIALITÉ DES PARAMÈTRES D'ACCÈS

L'accès aux éléments du SI (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe). Ces paramètres sont personnels à l'Utilisateur et doivent être gardés strictement confidentiels. Ils permettent en particulier de contrôler l'activité des Utilisateurs.

Sauf exceptions encadrées par l'entreprise, ces paramètres doivent être mémorisés par l'Utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers, à d'autres Utilisateurs ou aisément accessibles. Ils doivent être saisis par l'Utilisateur à chaque accès et ne pas être conservés en mémoire dans le SI. Le non-respect des règles précitées pourra entraîner des sanctions disciplinaires.

Lorsqu'ils sont choisis par l'Utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement.

D. POSTE DE TRAVAIL, MATÉRIELS, PROGRAMMES & LOGICIELS

1. Poste de travail et matériel

Le poste de travail de l'Utilisateur ne doit pas contenir de programmes, logiciels, documents, fichiers, informations ou données personnels sauf accord du responsable hiérarchique et du service informatique en concertation.

L'Utilisateur ne doit en aucun cas remplacer un élément de son poste de travail (disque dur, carte graphique, mémoire, …) par un élément lui appartenant, il doit en faire la demande au service informatique.

En cas d'absence, même temporaire, il est impératif que l'Utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

L'accès au Système d'Information est interdit avec du matériel n'appartenant pas à l'entreprise, sauf si les autorisations d'accès écrites lui ont été fournies par la Direction et/ou le service informatique en concertation.

Quand cela est techniquement possible, les équipements mobiles doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement. L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

L'Utilisateur doit renseigner et signer un registre, tenu par le service informatique ou RH de Nobilito, actant la remise de l'équipement mobile ou la mise à disposition de tout matériel spécifique (ex : vidéoprojecteur pour la tenue d'une réunion).

L'Utilisateur en assure la garde et la responsabilité et doit informer le service informatique en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

2. Logiciels et programmes

L'Utilisateur ne doit pas :

- installer de logiciels, copier, installer, modifier ou détruire des fichiers susceptibles de créer des risques de sécurité au sein de NOBILITO ;
- installer, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, etc. en violation des droits de propriété intellectuelle de tiers, autres que ceux qui sont expressément autorisés par l'entreprise ;
- Utiliser les matériels, programmes, logiciels ou progiciels mis à sa disposition par l'entreprise, en violation des règles techniques applicables et des prescriptions définies par l'entreprise.

En particulier, l'Utilisateur doit obtenir l'accord du service informatique avant toute installation de logiciels supplémentaires.

Il doit également et obligatoirement alerter le service informatique de toute violation ou tentative de violation suspectée de son compte réseau et de manière de tout dysfonctionnement.

E. VIRUS INFORMATIQUES

Le poste de travail (station, micros, portables, ...) de chaque Utilisateur est en règle générale équipé d'un logiciel antivirus.

Cependant, l'utilisation des applications communicantes (Internet, messagerie, ...) et des supports de stockage (CD-ROM, clé USB, disque dur externe, ...) peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'Utilisateur, à l'insu de ce dernier, de programmes ou fichiers qui altèrent ou pillent les données et logiciels qu'il contient.

Il est interdit à tout Utilisateur de charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées.

F. ACCÈS À INTERNET

Dans le cadre de leur activité, les Utilisateurs peuvent avoir accès à Internet. Chacun doit donc en faire un usage approprié, quel que soit le moyen de connexion utilisé (téléphones portables, ordinateurs, tablettes, smartphones, etc. …).

Chaque site internet pouvant être régi par des règles juridiques autres que le droit français, toutes précautions doivent être prises à cet égard par l'Utilisateur.

Les Utilisateurs ne doivent en aucun cas se livrer sur Internet à des activités illicites, ou portant atteinte aux intérêts de l'entreprise.

Pour des raisons de sécurité, l'accès à certains sites et fichiers peut être limité ou prohibé par le service informatique. Celui-ci est habilité à imposer un filtrage internet et à restreindre le téléchargement de certains fichiers.

La contribution des Utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est autorisée. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée et un devoir de loyauté des Utilisateurs est donc indispensable.

Il est interdit de provoquer un encombrement du réseau à la suite de téléchargements longs (logiciels de partage de fichiers), ou en se livrant à des activités oisives.

L'utilisation d'Internet à des fins commerciales personnelles est strictement interdite.

Les périphériques personnels des Utilisateurs (téléphones portables, ordinateurs, tablettes, …) n'ont pas lieu de se connecter sur le réseau de l'entreprise, un réseau invité indépendant du réseau d'entreprise est mis à leur disposition.

A des fins de statistiques, de qualité de service et de sécurité, le trafic Internet est sujet à une supervision et à des vérifications et audits réguliers par l'entreprise, dans les limites prévues par la loi. A ce titre, l'entreprise possède les moyens techniques de traçabilité des échanges et des contenus.

G. MESSAGERIE ÉLECTRONIQUE - RÉSEAU SOCIAL D'ENTREPRISE – RÉSEAUX SOCIAUX

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le service informatique. De façon exceptionnelle, le service informatique peut mettre une adresse de messagerie électronique à la disposition d'Utilisateurs non-salariés pour exercer leur activité pour l'entreprise.

Le réseau social d'entreprise est également un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié peut accéder à ce réseau mis à disposition afin d'échanger avec les autres salariés ou dirigeants de l'entreprise.

Chacun doit faire un usage approprié de sa messagerie ou du réseau social d'entreprise. L'utilisation de la messagerie ou du réseau social d'entreprise à un usage personnel est tolérée à condition qu'elle reste dans les limites du raisonnable en termes de temps passé et de nombre de messages, lesquels doivent avoir pour objet « privé » ou « personnel », et être stockés dans un dossier intitulé « privé » ou « personnel » ou dans une conversation ou un forum indiqués « privé » ou « personnel ».

En tout état de cause, les Utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Il est formellement interdit de diffuser des photos ou informations sur les activités du groupe sans autorisation préalable écrite de la Direction ou de la Responsable communication.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles ou sur le réseau social d'entreprise est soumis aux mêmes règles que les copies de données sur supports externes, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à l'autorité hiérarchique.

Les messages électroniques reçus sur la messagerie professionnelle ou via le réseau social d'entreprise font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Il est donc impératif que les Utilisateurs n'ouvrent les pièces jointes, ou cliquent sur des liens, qu'en ayant vérifié au préalable la vraisemblance du message reçu (identité de l'expéditeur, nom de domaine, nom du site vers lequel le lien pointe, …).

Les Utilisateurs sont invités à informer le service informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage et de sécurité.

Avant tout envoi, l'Utilisateur est tenu de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

L'entreprise s'interdit d'accéder aux dossiers et aux messages comportant la mention expresse ou manifeste de son caractère personnel. En cas de manquement à ces règles d'identification des dossiers et messages, les messages sont présumés être à caractère professionnel.

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

Enfin, il est formellement interdit aux utilisateurs d'enregistrer une messagerie électronique personnelle ou un compte personnel émanant d'un réseau social sur le SI, ce sans l'autorisation préalable écrite de la Direction ou de l'Administrateur.

H. TÉLÉPHONE

L'entreprise met à disposition des Utilisateurs salariés, pour l'exercice de leur activité professionnelle, des téléphones fixes ou mobiles, à l'exception des salariés dont la nature de leur fonction ne nécessite pas d'un tel équipement.

Il est interdit à tout Utilisateur de charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées.

L'utilisation de ces moyens à usage personnel est tolérée à condition qu'elle reste dans les limites du raisonnable en termes de temps passé, de quantité d'appels et de volume de données transférées.

Les surcoûts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les Utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

L'entreprise se réserve le droit d'appliquer certaines restrictions dans l'utilisation des téléphones. A titre d'exemple, certains téléphones peuvent ne pas permettre d'appeler à l'international. Des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. L'entreprise se réserve le droit d'accéder aux numéros complets des relevés individuels en cas d'utilisation manifestement anormale, sur demande du Directeur des Ressources Humaines ou du Directeur Général ou Président.

I. TÉLÉTRAVAIL

1. Règles générales

L'utilisateur ne doit pas faire en télétravail ce qu'il ne ferait pas au bureau. Il doit avoir une utilisation responsable et vigilante de ses équipements et accès professionnels, notamment sur sa navigation web, en veillant à bien séparer les usages professionnels et les usages personnels. L'utilisateur peut par exemple créer des comptes distincts s'il utilise une même application pour ces deux sphères.

2. Connexion internet sécurisée

L'utilisateur s'assure du bon paramétrage de sa box Internet. Il vérifie son mot de passe d'accès administrateur, le change s'il est faible et met à jour son logiciel interne.

S' il utilise le Wi-Fi, l'utilisateur active l'option de chiffrement WPA2 ou WPA3 avec un mot de passe long et complexe. Il désactive la fonction WPS et supprime le Wi-Fi invité. L'utilisateur ne doit se connecter qu'à des réseaux de confiance et éviter les accès partagés avec des tiers.

3. Favoriser l'usage d'équipements fournis et contrôlés par l'entreprise

S'il en a la possibilité, il utilise autant que possible le VPN (Virtual Private Network ou réseau privé virtuel) mis à disposition par l'entreprise :

- Il privilégie l'échange de données à travers les stockages disponibles depuis le VPN plutôt que par la messagerie électronique ;
- il se connecter au moins une fois par jour au VPN pour appliquer les mises à jour;
- il désactive le VPN seulement lorsque vous utilisez des services consommateurs de bande passante, comme le streaming vidéo, qui ne nécessitent pas de passer par le réseau de l'entreprise.

4. Utilisation d'un ordinateur personnel suffisamment sécurisé

Cela doit passer par:

- l'installation d'un antivirus et d'un pare-feu. Sur le système d'exploitation Windows 10, il est possible de vérifier l'état des systèmes de protection au moyen du centre de sécurité ;
- l'utilisation d'un compte personnel avec des droits limités, protégé par un mot de passe fort et non partagé avec d'autres personnes (par exemple avec d'autres membres de la famille) et sur lequel les applications installées se limitent au strict nécessaire ;
- la mise à jour régulière du système d'exploitation et des logiciels utilisés, notamment le navigateur web et ses extensions ;
- des sauvegardes régulières du travail de l'utilisateur, de préférence sur les infrastructures de l' entreprise, si possible en activant une solution de sauvegarde automatique ;
- l'utilisation de mots de passe forts sur l'ensemble des services et l'activation de l'authentification à deux facteurs (clef d'authentification, jeton, SMS) dès que cela est proposé par le service. Les gestionnaires de mots de passe permettront de sécuriser leur stockage et leur gestion.

5. Utilisation d'un téléphone personnel

Les téléphones portables sont particulièrement exposées à la perte et aux vols:

- L'utilisateur évite d'y enregistrer des informations confidentielles : codes secrets, codes d'accès, coordonnées bancaires, etc ;
- Il active le code PIN et met en place un délai de verrouillage automatique du téléphone. Eviter les codes trop faciles (date de naissance, 0123, etc.) ;
- Il active le chiffrement des informations sur son téléphone lorsque c'est possible ;
- Il note le numéro « IMEI » du téléphone pour le bloquer en cas de perte ou de vol ;
- Il n'installe des logiciels que depuis les plateformes officielles et évite à tout prix les applications de sources inconnues ;
- Lorsqu'il installe de nouvelles applications sur votre appareil, il lit les conditions d'utilisation et la politique de confidentialité et limite les données auxquelles elles peuvent avoir accès au strict nécessaire ;
- Il règle les paramètres de géolocalisation afin de toujours contrôler quand et par qui être géolocalisé.

6. Communication sécurisée et gestion des mots de passe

L'utilisateur évite de transmettre des données confidentielles via des services grand public de stockage, de partage de fichiers en ligne, d'édition collaborative ou via des messageries. À défaut, il chiffre les données avant de les transmettre et transmet les clés de chiffrement via un canal de communication distinct (par exemple, communication du mot de passe par téléphone ou SMS).

Il installe uniquement des applications autorisées par l'entreprise. Si l'application n'est pas déjà déployée par l'entreprise, il faut la télécharger depuis les sites ou les magasins officiels des éditeurs.

Il privilégie des outils de communication chiffrés de bout en bout, si l'entreprise ne fournit pas d'outils de communication sécurisé. Il évite les applications gratuites qui n'offrent pas de garanties fortes de sécurité.

Il privilégie les systèmes de visioconférence qui protègent la vie privée. Les conditions d'utilisation du logiciel doivent garantir la confidentialité des données et ne les réutilisent pas pour d'autres finalités.

7. La politique des mots de passe

L'utilisateur prendra acte de la règle ci-dessous pour la définition de son, ses mot(s) de passe en termes de robustesse et renouvellement dans le cadre de la lutte contre les cyberattaques.

Le mot de passe devra comporter au moins 12 caractères et être constitué au moins d'une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Il sera à renouveler tous les ans