CHARTE INFORMATIQUE
DU
GROUPE NOVARC



www.novarc.com

NOVEMBRE 2026

SOMMAIRE

PREAMBULE 3
Article 1 – GENERALITES 3
1.1. Définitions 3
1.2. Champ d'application 5
1.3. Conditions d'accès au Système d'information 6
1.3.1. Identifiants 6
1.3.2. Droits et configurations 7
1.3.3. Usage professionnel 7
1.3.4. Droit à la déconnexion 8
1.4. Entrée en vigueur – Opposabilité 8
Article 2 – OBJET DE LA CHARTE 9
Article 3 – CONDITIONS D'UTILISATION DES RESSOURCES MATERIELLES 9
3.1. Le Poste de travail 9
3.1.1. Utilisation générale 9
3.1.2. Utilisation en déplacement 10
3.1.3. Télétravail 11
3.2. Dispositifs portables 11
3.2.1. Clés USB, disques durs et autres espaces de stockage portatifs 11
3.2.2. Téléphones portables – Smartphones - Tablettes 12
3.2.3. Autres systèmes embarqués 13
3.3. Réseau de l'Entreprise 13
3.4. Responsabilité sociétale des entreprises – Protection de l'environnement 14
Article 4 – CONDITIONS D'UTILISATION DES RESSOURCES LOGICIELLES 14
4.1. ERP et applicatifs métiers 14
4.2. Intranet 14
4.3. Messageries électroniques 15
4.3.1. Mails 15
4.3.2. Messageries instantanées 19
4.4. Logiciels SaaS 19
4.5. Utilisation de l'Intelligence Artificielle 20
Article 5 – INTERNET & RESEAUX SOCIAUX 22
5.1. Internet 22

5.2. Réseaux sociaux 23
5.3. Monitoring et traçage 23
5.3.1. Monitoring et contrôle interne 23
5.3.2. Traçage externe 24
Article 6 – GESTION DES DONNEES DE L'ENTREPRISE 24
6.1. Confidentialité 24
6.2. Données personnelles 25
6.3. Propriété intellectuelle 26
Article 7 – SECURITE 27
7.1. Moyens techniques 27
7.1.1. Dispositifs de protection contre les attaques informatiques 27
7.1.2. Backups 27
7.2. Moyens organisationnels 28
Article 8 – ENGAGEMENT DE L'UTILISATEUR 29
Article 9 – AUDIT 29
Article 10 - SANCTIONS 29
Article 11 - FORMATION / SENSIBILISATION 29
Article 12 – VIGILANCE 30

Type de document

Charte Utilisateur

Confidentialité

Public

Périmètre

Groupe NOVARC et ses filiales

Version et historique

Version	Date	Auteur	Approbation
2.0	20/10/2026	Christophe SAMARD	DSI

PREAMBULE

L'Entreprise met à la disposition de tout Utilisateur des équipements informatiques (PC, stations, logiciels, etc…), des moyens de communication (messageries, accès internet, téléphonie, visio-conférence, portails collaboratifs etc…) ainsi que des informations et données (base de données, images, vidéos etc…) qui sont nécessaires à l'accomplissement de sa mission.

La présente Charte s'inscrit dans le cadre général des grands principes de la vie sociale et professionnelle. Elle vise à réaliser un équilibre entre les besoins de sécurité de l'Entreprise et le respect des libertés individuelles et collectives conformément aux lois et règlements en vigueur.

Cette Charte est destinée à informer les Utilisateurs sur leurs droits et leurs obligations dans le cadre de l'utilisation du Système d'information et de communication de l'Entreprise, à instaurer la confiance dans l'utilisation de ce système, et à en préserver l'intégrité et le bon fonctionnement, dans le respect des droits et des libertés de chacun, tout en respectant les principes de loyauté et de proportionnalité.

La Charte ne fait pas obstacle à la mise en place d'une Charte spécifique destinée à régir les conditions d'utilisation du Système d'information et de communication par les représentants du personnel de l'Entreprise. De même, la Charte ne saurait faire obstacle aux dispositions légales, réglementaires et conventionnelles relatives aux représentants du personnel ou au droit syndical.

Article 1 – GENERALITES

1.1. Définitions

Administrateur du Système d'information : Désigne le Directeur du Système d'information du Groupe NOVARC et les membres de son service agissant directement sous son autorité. Il veille à la protection, à la maintenance, et au bon fonctionnement du Système d'information de l'Entreprise.

Dans le cadre de ses missions, l'Administrateur du Système d'information agit sous l'autorité de la Direction de l'Entreprise et dans le respect des dispositions légales et réglementaires applicables. Il peut déléguer certaines opérations techniques aux personnes habilitées à cet effet, sous sa responsabilité.

L'Administrateur du Système d'information respecte la présente Charte et veille à son application par les personnes placées sous son autorité.
Il agit en concertation avec les services compétents du Groupe NOVARC afin d'assurer la conformité du Système d'information aux dispositions légales et réglementaires applicables, notamment celles relatives à la protection des données personnelles, à la cybersécurité, au secret des correspondances et aux recommandations ou référentiels émis par les autorités compétentes, notamment la CNIL.

Lorsque des outils intégrant des fonctionnalités d'intelligence artificielle sont utilisés au sein de l'Entreprise, leur utilisation doit également respecter la réglementation applicable, notamment le règlement européen sur l'intelligence artificielle (AI Act – règlement UE 2024/1689).

L'Administrateur du Système d'information a notamment accès aux serveurs de fichiers, aux serveurs web et aux serveurs de messagerie de l'Entreprise. Il est donc susceptible de prendre connaissance de l'ensemble des données reçues émises ou élaborées par les Utilisateurs. Cependant, l'Administrateur

du Système d'information ne peut divulguer les informations dont il aurait eu connaissance dans le cadre de ses fonctions, en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des Utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni la sécurité du Système d'information, ni ne causent de troubles objectifs au sein de l'Entreprise.

Charte : Désigne la présente charte d'utilisation de son Système d'information et de Communication.

Donnée(s) Personnelle(s) : Désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, conformément au Règlement (UE) 2016/679 (RGPD).

DPO : Data Protection Officer (délégué à la protection des données): Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Entreprise : Désigne la société NOVARC (GROUPE NOVARC), société anonyme à directoire, au capital de 3 900 446,75 euros, sise 815 C Chemin du Razas – 26780 MALATAVERNE et immatriculée au Registre du Commerce et des Sociétés de ROMANS sous le numéro 380 765 131 ; ainsi que toutes ses Filiales détenues directement ou indirectement et sur lesquelles elle exerce un pouvoir de contrôle au sens de l'article L233-3 du Code de commerce.

ERP Enterprise Resource Planning ou logiciel métier : Solution logicielle permettant de supporter les processus métier de l'Entreprise.

Filiale(s) du Groupe : Désigne toute société contrôlée directement ou indirectement par NOVARC au sens de l'article L.233-3 du Code de commerce, y compris les sociétés établies hors du territoire français, dès lors qu'elles utilisent tout ou partie du Système d'information du Groupe NOVARC.

Information(s) Confidentielle(s) : désigne les informations, de toutes natures, présentes sur tous supports et ayant un intérêt stratégique, économique ou financier pour l'Entreprise, son personnel, la concurrence, l'administration et les autorités ou les tiers de façon générale et qui ne sont pas connues du public ou librement consultables par ce dernier. Ces informations peuvent être présentes sur des fichiers ayant l'avertissement « Confidentiel » ou non.

Intranet : Désigne le réseau de télécommunications et de téléinformatique destiné à l'usage exclusif de l'Entreprise et utilisant les mêmes protocoles techniques qu'internet.

Mobile Device Management (MDM) : désigne la solution de gestion centralisée des équipements mobiles professionnels permettant à l'Entreprise d'assurer leur configuration, leur sécurisation, leur administration et, le cas échéant, la protection des données professionnelles qui y sont stockées.

Outil d'intelligence artificielle (Outil d'IA) : désigne tout logiciel, service ou fonctionnalité intégrant un Système d'IA et utilisé par un Utilisateur dans le cadre de ses activités professionnelles.

Poste de travail : désigne l'ensemble des équipements nécessaires à l'accomplissement du travail de l'Utilisateur et qui lui ont été attribués à son arrivée par l'Entreprise (notamment l'écran, le clavier, l'imprimante, l'ordinateur et par extension son système d'exploitation).

Prompt : désigne toute instruction, requête, donnée, document ou autre contenu transmis à un Outil d'IA afin d'obtenir un résultat généré ou assisté par celui-ci.

RSSI : Responsable de la sécurité du système d'information : Il a pour mission de mettre en œuvre le cadre et les politiques de sécurité de l'information pour le Groupe.

SaaS : Software as a Service : Type de solution logicielle hébergée chez un prestataire externe à l'Entreprise qui lui en délivre le service.

Système (s) d'information : Désigne l'ensemble des ressources matérielles, logicielles, réseaux, services et données mis en œuvre par l'Entreprise pour collecter, traiter, stocker, transmettre, partager, sécuriser et exploiter l'information.
Cette notion comprend notamment :

- Les équipements informatiques et numériques, fixes ou mobiles, tels que les Postes de travail, ordinateurs portables, smartphones, tablettes, serveurs, équipements réseau, périphériques de stockage, imprimantes, photocopieurs et téléphones ;
- Les infrastructures de communication et de connectivité, incluant les réseaux locaux, étendus, sans fil, les accès Internet et les solutions de télécommunication ;
- L'ensemble des logiciels, applications, systèmes d'exploitation, outils de sécurité, plateformes collaboratives et services numériques utilisés par l'Entreprise ;
- Les services hébergés ou fournis par des tiers, notamment les solutions en mode SaaS (Software as a Service), les services cloud, les plateformes externes et les applications accessibles via Internet ;
- L'ensemble des données, bases de données, fichiers, documents électroniques, contenus multimédias, espaces collaboratifs, Intranets, extranets et plus généralement tout flux d'information traité ou échangé dans le cadre des activités de l'Entreprise.

Système d'intelligence artificielle (Système d'IA) : désigne un système d'intelligence artificielle au sens du règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (« AI Act »).

Utilisateur(s) : désigne toute personne physique autorisée à accéder, à quelque titre que ce soit, à tout ou partie du Système d'information de l'Entreprise, notamment les salariés, alternants, stagiaires, intérimaires, mandataires sociaux, prestataires, sous-traitants, consultants, agents commerciaux, partenaires, conseils externes ou tout autre tiers habilité.

Les droits d'accès accordés aux Utilisateurs sont limités aux seules ressources nécessaires à l'accomplissement de leurs fonctions ou de leur mission et sont accordés pour la durée strictement nécessaire.

1.2. Champ d'application

La présente Charte s'applique aux Utilisateurs de l'Entreprise.

La Charte est mise à la disposition de l'ensemble du personnel de l'Entreprise et, faisant partie intégrante du Règlement intérieur, lui est remise personnellement lors de l'embauche.

La présente Charte est portée à la connaissance de l'ensemble des Utilisateurs préalablement ou concomitamment à l'octroi de leur accès au Système d'information.

Pour les salariés des sociétés françaises auxquelles la présente Charte est applicable, celle-ci est intégrée ou annexée au règlement intérieur dans les conditions prévues par la législation applicable.

Pour les Utilisateurs ne relevant pas d'un règlement intérieur français, notamment les collaborateurs de Filiales étrangères, prestataires, consultants, sous-traitants ou autres tiers autorisés, la Charte est rendue opposable selon des modalités adaptées à leur situation, notamment par incorporation ou référence dans un contrat, une convention, une politique interne applicable ou par acceptation expresse par voie électronique ou documentaire.

L'accès au Système d'information est subordonné à l'acceptation préalable de la présente Charte.

Pour les sociétés ou Utilisateurs établis hors de France, la présente Charte s'applique sous réserve des dispositions impératives du droit local. Chaque société du Groupe concernée prend les mesures nécessaires afin d'en assurer l'opposabilité conformément au droit qui lui est applicable.

La présente Charte s'applique à l'ensemble des Utilisateurs accédant au Système d'information du Groupe NOVARC, y compris depuis l'étranger, sous réserve des dispositions impératives de droit local applicables.

1.3. Conditions d'accès au Système d'information

1.3.1. Identifiants

L'accès au Système d'information de l'Entreprise est, sauf dérogations accordées par l'Administrateur du Système d'information, réservé aux seuls Utilisateurs de l'Entreprise.

Le contrôle de l'accès au Système d'information permet d'identifier toute personne utilisant un ordinateur. Cette identification permet, à chaque connexion, l'attribution de droits et de privilèges propres à chaque Utilisateur sur les ressources du Système dont il a besoin pour son activité professionnelle.

Les identifiants et mots de passe attribués à chaque Utilisateur sont strictement personnels et confidentiels. Ils ne doivent être communiqués à aucun tiers, y compris à un autre Utilisateur ou à un responsable hiérarchique.

L'Administrateur du Système d'information ne demande pas à un Utilisateur de lui communiquer son mot de passe personnel.

En cas d'oubli, de perte, de suspicion de compromission ou lorsque les nécessités de fonctionnement du Système d'information l'exigent, l'Administrateur du Système d'information met en œuvre une procédure de réinitialisation ou tout autre mécanisme d'administration permettant de rétablir ou d'assurer l'accès nécessaire sans exiger la communication du mot de passe personnel de l'Utilisateur.

Chaque mot de passe doit être modifié selon des critères et une fréquence déterminée par l'Administrateur du Système d'information. Le mot de passe doit être conforme aux règles définies dans la politique de mot de passe de l'Entreprise.

1.3.2. Droits et configurations

L'Utilisateur est autorisé à utiliser le Système d'information dans la limite des ressources, des droits et des privilèges octroyés en amont par l'Administrateur des Systèmes d'information en fonction des attributions et du Poste de l'Utilisateur dans l'Entreprise. Dès lors, sans accord de l'Administrateur du Système d'information, l'Utilisateur n'est pas autorisé à :

- Déplacer ou désinstaller un composant matériel ou logiciel du Système d'information ;
- Modifier ou dépareiller les configurations installées sur les équipements mis à sa disposition ou qui ont été attachées à son profil d'utilisateur ;

L'Utilisateur doit respecter les droits qui lui sont octroyés et ne doit pas chercher à les outrepasser ou à les élever de sorte à accéder à des informations pour lesquelles il n'est pas habilité. Il ne doit pas non plus contourner les restrictions d'utilisation d'un logiciel. De manière plus générale, l'Utilisateur ne doit pas contourner les mesures et moyens de sécurité mis en place dans l'Entreprise.

A ce titre, l'Utilisateur est averti que l'intrusion non autorisée dans le Système d'information de l'Entreprise peut être considérée comme une infraction pénale. À ce titre, l'Utilisateur est informé que l'accès ou le maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données constitue une infraction pénale conformément aux dispositions de l'article 323-1 du Code pénal.
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 euros d'amende.

Lorsque cette infraction a entraîné soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, les peines sont portées à cinq ans d'emprisonnement et à 150 000 euros d'amende.

Tout travail de recherche ou autre, risquant de conduire à la violation de cette dernière règle, ne pourra être accompli qu'avec l'autorisation de l'Entreprise et dans le strict respect des règles qui auront alors été définies.

Si une élévation des droits de l'Utilisateur est nécessaire pour l'accomplissement de ses missions, il en fait la demande à l'Administrateur du Système d'information qui pourra ou non, accéder à sa demande.

Les ressources, droits et privilèges accordés à l'Utilisateur peuvent être suspendus, limités ou retirés à tout moment par l'Entreprise, notamment en cas de suspension ou de cessation de la relation contractuelle, de changement de fonction, de fin de mission, de départ de l'Entreprise ou de non-respect de la présente Charte.

1.3.3. Usage professionnel

L'utilisation du Système d'information par l'Utilisateur est réservée à un usage professionnel. Une utilisation privée du Système d'information de l'Entreprise est néanmoins tolérée dans la mesure où elle :

- N'entrave pas la bonne marche du travail de l'Utilisateur,
- N'est pas contraire aux intérêts de l'Entreprise et aux lois et règlements en vigueur,
- Ne perturbe pas le bon fonctionnement du Système d'information,
- Respecte l'intégrité des données du Système d'information de l'Entreprise,
- Reste raisonnable, adaptée et non abusive dans sa durée.

Les fichiers et dossiers créés, reçus ou stockés au moyen du Système d'information sont présumés avoir un caractère professionnel, sauf lorsqu'ils sont clairement identifiés par l'Utilisateur comme étant « personnel » ou « privé ».

Les fichiers et dossiers identifiés comme personnels ou privés ne peuvent être consultés par l'Entreprise qu'en présence de l'Utilisateur ou après que celui-ci a été dûment invité à être présent.

Il peut toutefois être procédé à leur consultation en l'absence de l'Utilisateur lorsqu'un risque ou un événement particulier le justifie, dans le respect des dispositions légales et réglementaires applicables.

1.3.4. Droit à la déconnexion

Les règles édictées dans la présente Charte ont également pour objet de garantir un droit à la déconnexion des Utilisateurs et de prévenir les phénomènes de stress au travail ou d'épuisement professionnel.

Il est ainsi rappelé l'importance du bon usage du Système d'information en vue de respecter les temps de repos et de congés ainsi qu'en vue de préserver l'équilibre essentiel entre la vie privée et familiale et la vie professionnelle.

Les Utilisateurs disposant, pour l'exercice de leurs fonctions, d'outils de communication à distance (tablettes, ordinateurs, téléphones portables, …), s'engagent à déconnecter ces appareils après leur journée de travail et pendant leurs périodes de repos et congés.

Il est rappelé aux Utilisateurs qu'ils ne sont jamais tenus de prendre connaissance des courriels qui leur sont adressés ou d'y répondre en dehors de leur temps de travail.

Il est, en outre, demandé aux responsables hiérarchiques d'éviter, dans la mesure du possible et sauf urgence et/ou importance du sujet en cause avérée, de contacter leurs collaborateurs ou de leur adresser des messages pendant certaines plages horaires, à savoir : de 21 h jusqu'à 8 h en semaine, ainsi que pendant les périodes de repos et congés de leurs collaborateurs. Dans ce cadre, ils sont invités à utiliser la fonction « envoi différé ».

1.4. Entrée en vigueur – Opposabilité

La présente Charte entre en vigueur le 1er novembre 2026.

Au sein des sociétés françaises concernées, la présente Charte constitue, lorsqu'elle comporte des prescriptions générales et permanentes relatives notamment à la discipline, à la sécurité ou aux conditions d'utilisation des outils professionnels, une adjonction au règlement intérieur conformément aux dispositions du Code du travail.

Elle est soumise aux formalités légales applicables au règlement intérieur, notamment à la consultation préalable du Comité social et économique lorsqu'elle est requise, aux mesures de publicité applicables et à sa communication, accompagnée de l'avis du Comité social et économique, à l'inspection du travail.

Toute modification ou suppression de dispositions relevant du règlement intérieur est soumise aux mêmes formalités.

Pour les Utilisateurs ne relevant pas d'un règlement intérieur français, notamment les collaborateurs des Filiales étrangères et les Utilisateurs tiers, l'opposabilité de la Charte est assurée selon les modalités prévues à l'article 1.2, sous réserve des dispositions impératives du droit applicable.

Article 2 – OBJET DE LA CHARTE

L'objet de la Charte est d'encadrer l'utilisation du Système d'information et de communication de l'Entreprise.

La présente Charte tend ainsi :

- A définir les conditions d'utilisation, de mises à jour, de maintenance, de correction, de réparation des éléments matériels et logiciels du Système d'information de l'Entreprise ;
- A protéger l'intégrité des données et du fonctionnement du Système d'information de l'Entreprise ;
- A empêcher la diffusion, non autorisée des informations de nature financière, économique, commerciale, juridique, technique, administrative, artistique, industrielle, et de toute autre Information Confidentielle, sensible ou stratégique appartenant à l'Entreprise ;
- A empêcher l'intrusion dans le Système d'information de l'Entreprise, de matériels et de logiciels, de données et de fichiers de nature à porter préjudice à l'Entreprise.
- A empêcher une utilisation du Système d'information de l'Entreprise non-conforme aux lois et règlements en vigueur.

Article 3 – CONDITIONS D'UTILISATION DES RESSOURCES MATERIELLES

3.1. Le Poste de travail

3.1.1. Utilisation générale

3.1.1.1. Ordinateur et système d'exploitation

L'Utilisateur s'est vu mettre à disposition un ensemble de matériels et logiciels du Système d'information de l'Entreprise constituant ainsi son Poste de travail. L'Utilisateur en assure la sécurité, tant physique que logicielle, en effectuant l'ensemble des mises-à-jour nécessaires et recommandées de son système d'exploitation et en s'assurant qu'un tiers ne puisse pas accéder à son Poste de travail en son absence (verrouillage de sa session et du lieu dans lequel se trouve son Poste de travail). En tout état de cause, l'Utilisateur ne communique jamais son identifiant et/ou mot de passe à qui que ce soit.

Seul l'Administrateur du Système d'information est autorisé à introduire de nouveaux matériels, programmes ou logiciels dans le Système d'information de l'Entreprise. L'Utilisateur s'interdit donc de télécharger tout programme ou élément de programme, application ou encore « plugin » à partir d'un serveur internet, quand bien même serait-il incité à le faire par son éditeur.
Lorsque l'Utilisateur a besoin d'un nouveau matériel, programme ou logiciel dans l'accomplissement de son travail, il doit obtenir l'autorisation préalable de l'Administrateur du Système d'information avant son admission dans le Système d'information suivant le processus défini dans l'Entreprise.

L'Administrateur du Système d'information de l'Entreprise n'effectue pas de sauvegardes des disques durs « locaux » des Postes de travail des Utilisateurs sauf dans certains cas dérogatoires qui expressément convenus entre l'Administrateur et l'Utilisateur. Les Utilisateurs doivent donc impérativement enregistrer leurs fichiers et autres travaux sur le serveur de l'Entreprise. L'espace

maximum alloué à chaque Utilisateur sur sa machine virtuelle est celui indiqué par l'Administrateur du Système d'information. L'Utilisateur veillera à respecter cette limite.

Afin d'éviter la perte de données, l'Utilisateur doit systématiquement éteindre son Poste de travail par arrêt logiciel et non par l'interrupteur pour terminer proprement ses sessions (hors cas de blocage technique).

3.1.1.2. Téléphone fixe

Lorsque l'Utilisateur dispose d'un téléphone, il en fait une utilisation raisonnable au risque de faire l'objet de sanctions et d'être facturé, partiellement ou totalement, des appels non justifiés ou abusifs.

3.1.1.3. Imprimantes

L'utilisation des imprimantes via le Système d'information est réservée à un usage strictement professionnel.

L'Utilisateur est tenu :

- De limiter l'impression ou la copie papier au strict nécessaire et uniquement au cadre professionnel,
- De régler par défaut l'impression et la copie papier de documents en recto verso et en noir et blanc,
- De limiter l'impression et/ou la copie papier en couleur au strict minimum.

3.1.2. Utilisation en déplacement

Lorsque l'Utilisateur est amené à se déplacer avec son Poste de travail, il s'assure :

- Que tout disque dur externe utilisé ou autres supports de stockage externe soient chiffrés. A défaut, l'Utilisateur est invité à se rapprocher de l'Administrateur du Système de l'information ;
- De ne jamais laisser ses appareils sans surveillance ou dans un lieu non sécurisé (pièce fermée à clé à minima avec accès limité à l'Utilisateur seulement) ;
- D'utiliser une connexion web chiffrée (vérification de la présence du « petit cadenas fermé » à gauche de l'URL sur la page du navigateur) ;
- Sauf impératif, de ne pas se connecter sur des réseaux wifi publics ;
- D'utiliser uniquement les équipements fournis par l'Entreprise et de ne connecter ou de se connecter à aucun équipement tiers (clé USB, clavier…etc.) ;
- De ne prêter à personne un équipement de son Poste de travail ;
- De faire preuve de vigilance dans l'utilisation du Poste de travail afin que les données traitées ne soient pas visibles pour des tiers (utilisation dans le train, dans un café…). Une utilisation « publique » du Poste de travail nécessite l'utilisation d'un filtre de confidentialité délivrable sur demande de l'Utilisateur par l'Administrateur du Système de l'information.

A son retour de déplacement, l'Utilisateur remet en ordre son Poste de travail et transmet à l'Administrateur du Système d'information tout équipement qui pourrait ou qu'il suspecte d'avoir été compromis. L'Utilisateur s'assure également de n'avoir ramené au sein de l'Entreprise, aucun équipement étranger (équipements reçus en « goodies » par exemple : clé USB, batterie externe…etc.).

3.1.3. Télétravail

Lorsque l'Utilisateur recourt au télétravail, en plus d'appliquer les règles générales de protection du Poste de travail et celles relatives aux déplacements, l'Utilisateur apporte un soin particulier à :

- Séparer strictement ses usages professionnels et personnels ;
- Disposer d'une connexion filaire ou wifi sécurisée (notamment en utilisant un protocole wifi fiable et récent) ;
- Sauvegarder son travail sur le serveur de l'Entreprise au travers d'une connexion VPN dès que sa connexion à internet le lui permet ;
- Verrouiller sa session et le lieu dans lequel se trouve son Poste de travail en cas d'absence étant entendu que l'Utilisateur est garant de la bonne utilisation du Poste de travail (interdiction de prêter le Poste de travail aux membres du foyer ou à ses proches notamment) ;
- Ne pas faire suite ou télécharger les pièces jointes de courriel frauduleux ou douteux ;

Les Utilisateurs concernés par le télétravail doivent souscrire une assurance multirisque habitation couvrant le vol ou la détérioration du Poste de travail mis à leur disposition. Les primes y afférentes sont à la charge de l'Entreprise.

En tout état de cause, lorsqu'il est mis fin au télétravail de l'Utilisateur, ce dernier restitue l'intégralité des éléments de son Poste de travail à l'Entreprise.

3.2. Dispositifs portables

3.2.1. Clés USB, disques durs et autres espaces de stockage portatifs

L'Entreprise met à la disposition des Utilisateurs des équipements de stockage portatifs sur demande faite à l'Administrateur des Systèmes de l'information.

Ces derniers sont la propriété exclusive de l'Entreprise et ne peuvent en aucun cas servir à un usage personnel. En cas de cessation des fonctions de l'Utilisateur dans l'Entreprise, tous les appareils de stockage portatifs devront être restitués.

Avant chaque utilisation sur son Poste de travail, l'Utilisateur doit réaliser une analyse antivirus de l'appareil de stockage portatif. L'Administrateur des Systèmes de l'information peut avoir mis en place sur les Postes de travail des dispositifs de blocage des ports USB.

L'Utilisateur est garant de l'absence de tout fichier malveillant sur l'appareil de stockage portatif. A ce titre il doit faire preuve d'une extrême vigilance et ne pas connecter l'appareil de stockage portatif sur un appareil non sécurisé ou suspect. En cas de doute, l'Utilisateur en informe l'Administrateur des Systèmes d'information sans délai.

Le stockage d'Informations Confidentielles sur un support de stockage portatif est par principe interdit. Néanmoins, lorsque le stockage de telles informations est indispensable pour le travail de l'Utilisateur, ce dernier peut être amené à transporter des Informations Confidentielles au sein d'un appareil de stockage portatif. L'Utilisateur s'assure alors que le périphérique de stockage portatif soit chiffré, -. L'Administrateur des Systèmes d'information peut fournir un appareil chiffré sur demande de l'Utilisateur.

En cas de perte ou de vol d'un appareil de stockage portatif, l'Utilisateur en informe sans délai l'Administrateur des Systèmes d'information.

3.2.2. Téléphones portables – Smartphones- Tablettes

3.2.2.1. Utilisation de téléphones fournis par l'Entreprise

Les téléphones portables mis à la disposition des Utilisateurs par l'Entreprise, sont réservés à un usage strictement professionnel.

Tout abus ou utilisation déraisonnable du téléphone fourni par l'Entreprise pourra entraîner sa suspension définitive et la facturation partielle ou totale des appels non justifiés de l'Utilisateur.

L'Utilisateur est tenu de respecter une série de règles d'utilisation du téléphone portable mis à sa disposition. A ce titre, il s'engage à :

- Désactiver l'option « données à l'étranger » de son téléphone mobile lors de ses déplacements à l'étranger hors CEE afin d'éviter les frais dits de roaming ou d'itinérance ; Avoir recours le cas échéant à une carte SIM locale avec un forfait DATA adapté aux besoins.
- Privilégier les accès wifi locaux si ceux-ci sont sécurisés ;
- Demander l'autorisation de l'Administrateur des Systèmes de l'information préalablement à l'installation d'applications étant entendu que leur téléchargement est par principe interdit ;
- Ne pas enregistrer d'Informations Confidentielles concernant l'Entreprise sur le smartphone tels que des codes d'accès, coordonnées bancaires, etc. ;
- Verrouiller son smartphone au moyen d'un code PIN et choisir un code PIN compliqué ;
- Activer le verrouillage automatique du smartphone après un certain temps d'inutilisation, ce qui le rendra inactif en cas de perte ou vol ;
- Activer le chiffrement des données du téléphone ;
- Avertir dès que possible l'Entreprise en cas de perte ou de vol ;
- Eviter au maximum de se connecter sur des réseaux wifi public
- Ne pas connecter le smartphone à -un autre équipement tiers ;
- Désactiver les interfaces sans-fil (Bluetooth et Wifi) ou sans contact (NFC par exemple) lorsqu'elles ne sont pas utilisées ;
- Limiter l'utilisation des assistants vocaux et ne pas communiquer de données confidentielles ou sensibles.
- Mettre à jour le smartphone sans délai lorsqu'une mise à jour lui est proposée.

L'utilisation du téléphone mobile est soumise aux dispositions réglementaires en vigueur, notamment l'interdiction de l'utiliser en situation de conduite d'un véhicule. L'Entreprise ne saurait être tenue pour responsable en cas d'accident ou de poursuite résultant de l'utilisation d'un téléphone au volant.

Le numéro du téléphone portable professionnel est la propriété exclusive de l'Entreprise. A titre exceptionnel, il peut être transféré à l'Utilisateur après autorisation expresse et écrite du responsable de la division dont dépend l'Utilisateur.

3.2.2.2. Utilisation de téléphones personnels

L'utilisation de téléphones personnels dans le cadre professionnel est prohibée.

Il est interdit pour tout Utilisateur d'utiliser la carte SIM de sa ligne professionnelle dans un appareil personnel et non mis à sa disposition par l'Entreprise, notamment dans des téléphones dits « double SIM ».

3.2.2.3. Mise en place du MDM (Mobile Device Management)

Afin de renforcer la sécurité des équipements mobiles professionnels et des données qui y sont traitées, l'Entreprise met en œuvre une solution de gestion centralisée des équipements mobiles (« MDM »).

Le MDM peut notamment permettre la configuration à distance des paramètres de sécurité, la gestion des mises à jour, l'application de restrictions de sécurité et, lorsque cela est techniquement possible et nécessaire, la suppression à distance des données professionnelles en cas de perte, de vol, de compromission ou de fin d'utilisation de l'équipement.

Le dispositif MDM mis en œuvre par l'Entreprise n'a pas pour objet de permettre une surveillance permanente des Utilisateurs ni leur géolocalisation.

L'Entreprise met en œuvre le MDM dans le respect des principes de nécessité, de proportionnalité et de protection des Données Personnelles. Les Utilisateurs sont informés des caractéristiques essentielles du dispositif, de ses finalités et des données traitées conformément à la réglementation applicable.

Lorsque les dispositions du Code du travail l'exigent, les représentants du personnel sont préalablement informés ou consultés sur la mise en œuvre du dispositif.

Les Utilisateurs sont tenus de :

- Accepter l'enrôlement de leur appareil professionnel dans le système MDM ;
- Ne pas tenter de contourner ou désactiver les fonctionnalités du MDM ;
- Informer immédiatement l'Administrateur du Système d'information en cas de dysfonctionnement ou de perte de l'appareil ;
- Respecter les configurations imposées par le MDM, notamment en matière de mot de passe, de chiffrement, et de restrictions d'usage."

Ce dispositif permet notamment de configurer à distance les paramètres de sécurité, de gérer les mises à jour et, lorsque cela est techniquement possible, de supprimer à distance les données professionnelles en cas de perte, de vol ou de compromission de l'appareil.

3.2.3. Autres systèmes embarqués

Dans les cas où l'Utilisateur serait amené à utiliser d'autres systèmes embarqués de l'Entreprise (voitures connectées, montres connectées…etc.), il est astreint aux mêmes règles que celles applicables au Poste de travail et aux autres dispositifs portables.

3.3. Réseau de l'Entreprise

L'Utilisateur n'est pas autorisé à connecter d'équipement personnel (ordinateur, smartphone, objets connectés…etc.) à l'un quelconque des réseaux de l'Entreprise, qu'il soit en WIFI ou filaire.

L'Entreprise met cependant à disposition du public, un réseau « invité » permettant aux tiers de bénéficier d'un accès internet lors de leur visite dans l'un des locaux de l'Entreprise. Un sponsor interne devra valider la connexion d'un équipement sur le wifi guest : la personne qui souhaite se connecter devra saisir l'adresse mail d'un sponsor interne pour l'approuver. Les Utilisateurs sont libres de s'y connecter et devront dès lors renseigner leurs informations personnelles sur le portail de connexion et accepter les conditions générales de connexion au réseau invité.

3.4. Responsabilité sociétale des entreprises – Protection de l'environnement

L'utilisation du Système d'information par l'Utilisateur n'est pas sans conséquence sur les objectifs ambitieux que s'est fixée l'Entreprise dans le cadre de sa responsabilité sociétale (RSE).

Dès lors, il est de la responsabilité de chacun des Utilisateurs d'utiliser les outils informatiques qui sont mis à leur disposition en ayant conscience de l'impact que cela peut avoir sur l'environnement.

A titre d'exemple, le stockage de données sur les serveurs de l'Entreprise, que ce soit sur les machines virtuelles personnelles des Utilisateurs ou sur les dossiers partagés, représente un coût financier et environnemental non négligeable. L'Utilisateur est donc invité, dans la mesure du possible, à :

- Réduire au maximum l'envoi de courriels ;
- Réduire au maximum le volume de fichiers qu'il stocke sur sa machine virtuelle et sur les serveurs de l'Entreprise ;
- Trier régulièrement ses fichiers et ses courriels pour supprimer ceux qui seraient superflus ;

De la même façon, l'Utilisateur est invité à limiter le transfert de fichiers volumineux ou à éviter de consommer du contenu vidéo par « streaming » dans le cadre professionnel lorsque cela n'est pas nécessaire.

Article 4 – CONDITIONS D'UTILISATION DES RESSOURCES LOGICIELLES

4.1. ERP et applicatifs métiers

L'Entreprise peut mettre à disposition de l'Utilisateur des logiciels accessibles depuis un navigateur et une connexion internet. Ces logiciels sont des logiciels de type SaaS (Software as a Service).

Lors de l'utilisation de ces logiciels, l'Utilisateur est soumis au respect de leurs conditions générales d'utilisation. Dans le cas où ces dernières contrediraient la présente Charte ou d'autres dispositions internes de l'Entreprise et opposables à l'Utilisateur, ce dernier en informe sans délai l'Entreprise. En tout état de cause, les dispositions internes de l'Entreprise et de la présente Charte prévalent.

4.2. Intranet

L'Entreprise met à la disposition des Utilisateurs un Intranet et des portails collaboratifs destinés à un usage strictement professionnel.

L'Intranet et les portails collaboratifs fonctionnent sous la responsabilité informatique de l'Administrateur du Système d'information et sous la responsabilité éditoriale du dirigeant de l'Entreprise ou de son délégataire.

Aucun Utilisateur ne peut introduire ou tenter d'introduire des éléments ou du contenu sur l'Intranet sans autorisation de l'Administrateur du Système d'information et du directeur de la publication de l'Entreprise ou de leurs délégués.

4.3. Messageries électroniques

4.3.1. Mails

4.3.1.1. Mise à disposition

Chaque Utilisateur peut, au regard des fonctions exercées par lui au sein de l'Entreprise, disposer d'une messagerie électronique professionnelle.

L'adresse de messagerie est généralement composée du prénom et du nom de l'Utilisateur. Elle est attribuée par l'Administrateur du Système d'information qui peut en délivrer une nouvelle à l'Utilisateur, si la demande est justifiée, en cas de changement de nom de l'Utilisateur notamment.

Lors du départ définitif d'un Utilisateur ou de la fin de la relation contractuelle d'un Utilisateur tiers, l'Administrateur du Système d'information doit être informé par la Direction de l'Entreprise afin de mettre en œuvre les mesures appropriées concernant le compte de messagerie, les fichiers et les messages électroniques de l'Utilisateur, dans le respect des dispositions légales et réglementaires applicables.

4.3.1.2. Utilisation à titre professionnel

La messagerie électronique mise à la disposition de l'Utilisateur par l'Entreprise est utilisée à titre professionnel.

Les règles hiérarchiques et d'organisation des pouvoirs internes de signatures doivent être respectées. Ainsi, aucun courriel ne doit être envoyé par un Utilisateur qui n'en a pas l'autorité.

L'Utilisateur s'interdit de répondre à des courriels répétés et de les transférer lorsque ceux-ci ne présentent aucun rapport avec ses fonctions et ses attributions au sein de l'Entreprise. Il s'engage dans pareil cas à les détruire immédiatement.

Le courriel pouvant être reconnu comme preuve ou commencement de preuve par écrit, l'Utilisateur doit porter une attention toute particulière à sa rédaction et à sa diffusion.

L'Utilisateur veille, dans le cadre de ses communications électroniques professionnelles, à adopter un comportement respectueux, loyal et conforme à ses obligations professionnelles. Il s'abstient de tout propos injurieux, diffamatoire, discriminatoire, illicite ou susceptible de porter atteinte aux intérêts, à l'image ou à la réputation de l'Entreprise ou de ses collaborateurs, partenaires ou clients.

Les risques liés à la diffusion ou à l'interception des messages électroniques imposent que toute transmission d'Informations Confidentielles, qu'elle soit interne ou externe à l'Entreprise, soit limitée aux seuls destinataires habilités et fasse l'objet des mesures de protection appropriées. Si un Utilisateur est contraint d'adresser vers l'extérieur des Informations Confidentielles via sa messagerie électronique, il doit demander à l'Administrateur du Système d'information de l'assister pour le chiffrement de l'information.

L'Administrateur du Système d'information peut :

- Soit installer un outil de chiffrement sur le matériel confié à l'Utilisateur,
- Soit assurer lui-même cette transmission chiffrée.

Tout message comportant des Informations Confidentielles devra comporter la mention « CONFIDENTIEL » qu'il soit envoyé, ou non à l'extérieur du Système d'information.

Chaque message comportera l'avertissement suivant en français et en anglais :

« Ce courriel et ses pièces jointes sont strictement confidentiels et réservés à l'usage exclusif de son ou ses destinataires.
Si vous avez reçu ce courriel par erreur, nous vous vous remercions d'en informer immédiatement l'expéditeur en lui retournant ce message et le détruire de votre système informatique. Toute diffusion, distribution, copie ou autre utilisation du courriel ou de ses pièces jointes par une personne autre que son ou ses destinataires est formellement prohibée.
Nous déclinons toute responsabilité en cas de modification, altération, falsification ou omission concernant le contenu du courriel résultant de sa transmission ».

De même que partout ailleurs, la courtoisie constitue une règle de base dans tous les échanges électroniques.

Par ailleurs, l'Utilisateur doit rédiger des messages courts et clairs afin d'éviter toute surcharge informationnelle nuisant à l'efficacité de la communication.
Il doit également utiliser avec discernement les listes de diffusion personnelles ou collectives.
Il doit éviter l'envoi de copies à un nombre injustifié de destinataires.

Dans le cadre de l'utilisation de sa messagerie électronique, l'Utilisateur doit avoir conscience que son comportement reflète l'image de l'Entreprise puisqu'il est identifié par son adresse électronique comme membre de l'Entreprise. Aussi, il appartient à l'Utilisateur de faire de sa messagerie électronique un usage conforme à ce qui peut être attendu d'un utilisateur diligent (usage raisonnable). En particulier, et sans que cette liste soit limitative, l'Utilisateur :

- N'émet pas d'opinions personnelles susceptibles de porter préjudice à l'Entreprise,
- Ne diffuse pas son adresse e-mail professionnelle sur des sites Internet ou des médias sociaux sans rapport avec l'activité professionnelle, sans accord préalable de l'Administrateur du Système d'information et ce afin d'éviter l'envoi massif de spams,
- Ne dissimule pas son identité notamment par l'utilisation de pseudonymes, par la publication de contenu anonyme, ni n'usurpe l'identité ou l'identifiant d'un collègue de l'Entreprise ou de toute tierce personne,
- Ne participe pas à des jeux,
- Ne peut utiliser sa messagerie électronique à des fins syndicales, politiques ou religieuses, étant précisé que l'Entreprise peut autoriser, sur demande préalable, une utilisation syndicale professionnelle de la messagerie professionnelle.

L'Utilisateur est informé que les courriels émis et reçus depuis la messagerie électronique mise à sa disposition par l'Entreprise sont présumés, sauf si l'Utilisateur les identifie comme étant privés, avoir un caractère professionnel de sorte que l'Administrateur du Système d'information peut y avoir accès hors sa présence.

L'Utilisateur est informé qu'en cas d'absence de longue durée (par exemple, maladie ou maternité), les courriels à caractère professionnel seront redirigés vers son responsable hiérarchique. Il est ici

précisé que tout courriel de l'Utilisateur étant identifié comme ayant un caractère personnel ou privé et qui serait redirigé vers son responsable hiérarchique du fait d'une absence de longue durée ne sera pas ouvert.

4.3.1.3. Utilisation à titre privé

Les Utilisateurs sont invités, en priorité, à utiliser leur messagerie personnelle pour l'envoi de messages à caractère personnel.

Toutefois, l'utilisation de la messagerie électronique à titre privé est autorisée à titre exceptionnel, dans des proportions raisonnables, adaptées et non abusive, à la condition de ne pas affecter le fonctionnement du Système d'information de l'Entreprise du volume des messages échangés, de la taille des messages échangés et du format des pièces jointes notamment. En cas d'usage de la messagerie électronique à des fins privées, l'Utilisateur devra supprimer toute mention relative à l'Entreprise ou toute autre indication qui pourrait laisser croire que le message est rédigé et/ou envoyé dans l'exercice de ses fonctions.

L'Utilisateur souhaitant utiliser sa messagerie électronique à des fins privées doit classer ses courriels personnels (reçus et envoyés) dans un répertoire spécifique portant la mention « privé » ou « personnel » et indiquer dans l'objet même des messages électroniques envoyés la mention « privé » ou « personnel » de manière à prévenir l'Administrateur du Système d'information de la nature particulière s'attachant à cette catégorie de messages.

L'Utilisateur, soumis à une obligation de bonne foi par application des articles 1104 du Code civil et L. 1222-1 du Code du travail s'engage à ne pas qualifier de « personnel » des courriels professionnels.

Les courriels reçus ou envoyés ne comportant pas la mention « privé » ou « personnel », ou ne comportant pas d'éléments extérieurs laissant clairement apparaître dans leur intitulé, leur contenu, leur format, leurs pièces jointes, leur expéditeur ou leur destinataire, qu'ils sont de nature privée, sont considérés comme des courriels professionnels par l'Administrateur du Système d'information.

Les courriels identifiés comme étant privés ou personnels sont couverts par le secret des correspondances privées.

4.3.1.4. Contenu des messages électroniques

Aucun courriel, y compris lorsqu'il relève d'une utilisation privée de la messagerie électronique, ne doit comporter d'éléments sous forme de texte, d'image, de son, contraires aux lois et aux bonnes mœurs, à caractère dégradant, illicite, violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, homophobe, sexiste, pornographique, terroriste, ou susceptible de porter atteinte au respect et à la dignité de la personne humaine et ce, tant à l'égard des autres Utilisateurs que de tout tiers extérieur à l'Entreprise.

Aucun message électronique y compris relevant d'une utilisation privée, ne doit comporter d'éléments de nature à porter atteinte à l'image de l'Entreprise ainsi qu'à toutes les sociétés du Groupe NOVARC.

Aucun message électronique y compris relevant d'une utilisation privée, ne doit comporter d'éléments protégés par les lois en vigueur sur la propriété intellectuelle, autres que ceux expressément autorisés par l'Entreprise. Les Utilisateurs s'interdisent de solliciter auprès d'autres

Utilisateurs ou de tiers, l'envoi de messages comportant des éléments de cette nature et s'engagent à les détruire immédiatement s'ils sont amenés à en recevoir à leur insu.

4.3.1.5. Format, type et taille des messages électroniques

Afin de garantir le bon fonctionnement du Système d'information de l'Entreprise, l'Administrateur du Système d'information peut limiter le format, le type et la taille des courriels et de leurs pièces jointes envoyés et/ou reçus par l'Utilisateur. Ce dernier en est avisé par note de service, il doit suivre les recommandations et les règles techniques communiquées par l'Administrateur du Système d'information.

L'Administrateur du Système d'information met à la disposition de l'Utilisateur des outils de compression de fichiers.

4.3.1.6. Volume de la messagerie

La messagerie électronique de l'Utilisateur est conservée sur le serveur concerné de l'Entreprise. L'espace maximum alloué à chaque utilisateur est celui indiqué par l'Administrateur du Système d'information. L'utilisateur veillera à respecter cette limite.

4.3.1.7. Bonnes pratiques d'utilisation de la messagerie électronique

L'Utilisateur doit :

- S'interroger sur la pertinence de l'utilisation de la messagerie électronique professionnelle par rapport aux autres outils de communication disponibles afin de veiller à ce que l'usage de la messagerie ne puisse pas se substituer aux dialogues et échanges oraux et de prévenir l'isolement et la dépersonnalisation des échanges,
- Indiquer clairement le sujet du message dans la zone « Objet » (ou « Sujet »),
- N'envoyer le courrier électronique qu'aux personnes concernées :
    - En « A » pour les personnes dont on attend une action,
    - En « CC » pour informer les personnes strictement concernées par le message,
- Être bref et bien situer le contexte du message,
- Restreindre au strict nécessaire l'utilisation des caractères en majuscule et en couleur,
- Utiliser avec parcimonie les critères d'urgence, une utilisation fréquente leur ôtant toute efficacité, et ne pas solliciter de réponse immédiate si cela n'est pas nécessaire,
- Limiter autant que possible l'envoi de pièces jointes et de fichiers trop volumineux à destination des autres Utilisateurs,
- Eviter autant que possible l'envoi de pièces jointes vers d'autres Utilisateurs pour ne pas engorger le serveur de messagerie et favoriser les outils collaboratifs mis à disposition par l'Administrateur du Système d'information pour le partage de fichiers (Teams, SharePoint…),
- Eviter d'imprimer le courrier électronique,
- Respecter la confidentialité des messages reçus,
- Ne pas systématiquement « Répondre à tous »,
- S'interroger sur le moment opportun pour envoyer un courriel à un autre Utilisateur,
- Privilégier les envois différés lors de la rédaction d'un courriel en dehors des horaires de travail,

- Supprimer, sans les ouvrir, les emails avec pièce jointe dont on ne connait pas l'émetteur et qui présentent une forte probabilité de virus, spam, malware,
- Eviter d'envoyer des messages dépassant 10 MO. Au-delà, contacter l'Administrateur du Système d'information pour privilégier des services mis à disposition et permettant l'envoi de fichiers volumineux,
- S'abstenir de consulter ses messages lors de réunions afin de faciliter sa concentration.

4.3.2. Messageries instantanées

L'Entreprise peut mettre en place des moyens de communication comprenant des messageries instantanées ou quasi-instantanées (ex : Teams…).

L'ensemble des dispositions de l'article 4.3.1 ci-dessus, dès lors qu'elles sont transposables dans la pratique à l'utilisation d'une messagerie instantanée ou quasi-instantanée, leur sont applicables. Dès lors, il est utilement rappelé que l'Utilisateur s'interdit de publier des messages comprenant des éléments sous forme de texte, d'image, de son, contraires aux lois et aux bonnes mœurs, à caractère dégradant, illicite, violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, homophobe, sexiste, pornographique, terroriste, ou susceptible de porter atteinte au respect et à la dignité de la personne humaine et ce, tant à l'égard des autres Utilisateurs que de tout tiers extérieur à l'Entreprise.

L'accès à ces messageries doit être sécurisé par un mot de passe et suivre les règles de sécurité, de confidentialité et de respect de la législation édictées dans la présente Charte.

L'Utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans le cadre d'échanges électroniques sur ces messageries instantanées ou quasi-instantanées notamment sur les chats, forums de discussions, réseaux sociaux, etc.

En outre, le sens de la responsabilité de chacun conduit à ne pas se permettre de participer anonymement à des discussions électroniques.

4.4. Logiciels SaaS

L'Utilisateur peut vouloir utiliser des logiciels Saas non autorisés par l'Administrateur du Système d'information dans le cadre de l'accomplissement de son travail (ex : I love PDF…etc.), étant entendu que certains de ces logiciels Saas utilisent de l'intelligence artificielle (ex : chat GPT, Midjourney…). L'utilisation de tels outils est par principe interdite.

Les Utilisateurs souhaitant recourir à un service Saas non proposé par l'Entreprise doivent en informer l'Administrateur du Système d'information avant toute souscription et utilisation du service. Les Utilisateurs se verront alors autorisés ou non à utiliser le logiciel Saas demandé. En cas de refus, l'Administrateur du Système d'information pourra proposer à l'Utilisateur un service similaire, autorisé par l'Entreprise, en substitution du service demandé.

Toute demande doit faire l'objet d'une étude métier (Projet) et être accompagnée du nom du service, du lien d'accès au site internet de l'éditeur et l'objet/ but de l'utilisation du service pour être complète. A défaut, l'Administrateur du Système d'information ne traitera pas la demande.

En tout état de cause, les Utilisateurs ne doivent pas transmettre d'Informations Confidentielles et de Données Personnelles appartenant à l'Entreprise lors de l'utilisation du service.

En cas de fuite de données (avérée ou seulement soupçonnée) dans le cadre de l'utilisation d'un logiciel Saas, l'Utilisateur en informe sans délai l'Administrateur du Système d'information.

4.5. Utilisation de l'Intelligence Artificielle

4.5.1. Principe d'autorisation

L'utilisation professionnelle d'un Outil d'IA est subordonnée à son autorisation préalable par l'Entreprise selon la procédure interne applicable.

Les Utilisateurs ne doivent pas souscrire, installer ou utiliser, pour les besoins de leur activité professionnelle, un Outil d'IA non autorisé par l'Entreprise.

L'évaluation préalable d'un Outil d'IA est réalisée par les services compétents de l'Entreprise, notamment la Direction des Systèmes d'Information et, lorsque la nature ou l'usage de l'outil le justifie, la Direction Juridique, le Délégué à la Protection des Données, la Direction des Ressources Humaines ou la Direction Recherche & Développement.

Cette évaluation porte notamment sur les conditions de sécurité, de confidentialité, de traitement et d'hébergement des données ainsi que sur le respect des réglementations applicables, notamment le RGPD et l'AI Act.

Il n'appartient pas à l'Utilisateur de déterminer lui-même qu'un Outil d'IA satisfait à ces exigences.

4.5.2. Protection des informations et des données

L'Utilisateur ne doit transmettre à un Outil d'IA que les informations strictement nécessaires à l'accomplissement de la tâche autorisée.

Il est interdit de transmettre à un Outil d'IA des Informations Confidentielles, secrets d'affaires, informations protégées par des droits de propriété intellectuelle, Données Personnelles ou documents internes lorsque l'Outil d'IA n'a pas été expressément autorisé pour le traitement de cette catégorie d'informations.

Lorsque l'utilisation d'un Outil d'IA impliquant de telles informations a été expressément autorisée, l'Utilisateur respecte les conditions, restrictions et mesures de protection déterminées par l'Entreprise.

Les données et documents transmis doivent, lorsque cela est possible au regard de la finalité recherchée, être préalablement anonymisés, pseudonymisés ou expurgés des informations qui ne sont pas nécessaires au traitement.

4.5.3. Contrôle humain

Les résultats produits par un Outil d'IA ne doivent pas être considérés comme exacts, exhaustifs ou juridiquement, techniquement ou scientifiquement fiables sans vérification appropriée.

L'Utilisateur demeure tenu d'exercer un contrôle humain adapté sur les résultats obtenus avant toute utilisation, transmission ou prise de décision sur leur fondement.

Une décision produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative ne peut être fondée exclusivement sur un traitement automatisé que dans les cas autorisés par la réglementation applicable et après validation des services compétents, notamment de la Direction Juridique et du DPO lorsque des Données Personnelles sont concernées.

4.5.4. Usages relatifs aux ressources humaines

Toute utilisation d'un Système d'IA dans le cadre du recrutement, de la sélection de candidats, de l'affectation des tâches, de l'évaluation de la performance ou du comportement professionnel, de la surveillance des collaborateurs, de la promotion, de la gestion de carrière ou de la cessation de la relation de travail doit faire l'objet d'une validation préalable de la Direction des Ressources Humaines, de la DSI et, selon le cas, de la Direction Juridique et du DPO.

Une telle utilisation fait préalablement l'objet d'une analyse permettant notamment de déterminer les obligations applicables au titre du RGPD, de l'AI Act et du droit du travail.

4.5.5. Intégration de l'IA dans les produits et processus

Toute intégration d'un Système d'IA dans un produit, service ou processus du Groupe doit être préalablement soumise aux directions compétentes.

Cette analyse doit notamment permettre de déterminer le rôle juridique de l'Entreprise au titre de l'AI Act, le niveau de risque du Système d'IA et les obligations applicables en matière de gouvernance, documentation, contrôle humain, sécurité, transparence et protection des Données Personnelles.

4.5.6. Transparence

Lorsque la réglementation impose d'informer une personne qu'elle interagit avec un Système d'IA ou qu'un contenu a été généré ou manipulé par un Système d'IA, les mesures d'information, d'identification ou de marquage requises doivent être mises en œuvre.

L'Utilisateur respecte les instructions et procédures définies par l'Entreprise à cette fin.

4.5.7. Inventaire des usages

L'Entreprise tient, selon des modalités qu'elle détermine, un inventaire des Outils d'IA autorisés et des principaux cas d'usage identifiés afin d'en permettre le suivi et la réévaluation régulière au regard des évolutions techniques et réglementaires.

Les Utilisateurs fournissent aux services compétents les informations nécessaires à la tenue de cet inventaire lorsqu'elles leur sont demandées.

4.5.8. Incidents et violations de données

Tout incident, utilisation non autorisée, transmission accidentelle d'informations, suspicion de fuite ou de violation de données impliquant un Outil d'IA doit être signalé immédiatement à la DSI et, lorsque des Données Personnelles sont susceptibles d'être concernées, au DPO.

L'incident est analysé et documenté conformément aux procédures internes applicables. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, le responsable du traitement procède, lorsque les conditions réglementaires sont réunies, à sa notification à l'autorité de contrôle dans les délais applicables.

4.5.9. Responsabilité de l'Utilisateur

L'Utilisateur est tenu de respecter les règles d'utilisation qui lui sont applicables et les autorisations qui lui ont été accordées.

Il demeure responsable de la vérification et de l'utilisation professionnelle des contenus qu'il produit ou diffuse à l'aide d'un Outil d'IA, sans préjudice des responsabilités propres incombant à l'Entreprise, aux fournisseurs ou aux autres acteurs concernés au titre de la réglementation applicable.

Tout manquement aux présentes règles est susceptible d'entraîner les conséquences prévues à l'article 10 de la présente Charte.

Article 5 – INTERNET & RESEAUX SOCIAUX

Tout Utilisateur doit faire un usage réfléchi et approprié d'internet et des réseaux sociaux. Cet usage doit être conforme à la présente Charte, dès lors que celui-ci a une incidence sur l'Entreprise ou que l'Utilisateur est amené à faire référence à celle-ci. En tout état de cause, le comportement de l'Utilisateur sur internet et les réseaux sociaux ne doit pas nuire à la réputation ou à l'image de l'Entreprise.

5.1. Internet

Chaque Utilisateur peut, au regard des fonctions exercées au sein de l'Entreprise, disposer d'un accès à internet afin de permettre la consultation des sites du monde entier sous le nom de l'Entreprise.

A chaque accès, l'identifiant ainsi que les sites visités sont enregistrés dans les limites prévues par la loi.

En outre, 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.

Ainsi, à l'occasion de ses connexions professionnelles ou privées, l'Utilisateur s'interdit :

- De consulter et de télécharger des contenus contraires aux lois et aux bonnes mœurs ou à caractère raciste, antisémite, xénophobe, homophobe, sexiste, pornographique, terroriste, susceptibles de porter atteinte au respect et à la dignité de la personne humaine ou portant sur tout autre comportement dégradant ou illicite ;
- De s'exprimer au nom de l'Entreprise sans disposer au préalable des autorisations internes. A ce titre, l'Utilisateur ne peut publier de contenu, sous quelque forme que ce soit et sur quelque plateforme que ce soit (blog, réseaux sociaux, site internet, forum…etc) sans avoir consulté le responsable de la division de l'Entreprise dont il dépend et avoir obtenu son autorisation écrite. En cas de doutes sur la personne à contacter, l'Utilisateur s'adresse directement à la direction juridique de l'Entreprise.
- D'inscrire son adresse électronique professionnelle sur des sites Internet sans lien direct avec ses fonctions et ses attributions ;

- D'alimenter des sites, des blogs ou des pages personnelles dont le contenu serait contraire aux lois et bonnes mœurs ou à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, homophobe, sexiste, pornographique, terroriste, susceptibles de porter atteinte au respect et à la dignité de la personne humaine ou portant sur tout autre comportement dégradant ou illicite et ce, tant à l'égard des autres Utilisateurs que de tout tiers extérieur à l'Entreprise.
- De télécharger des logiciels, progiciels, programmes protégés par les lois en vigueur sur la propriété intellectuelle, sans autorisation préalable de l'Administrateur du Système d'information et des ayants droit.

5.2. Réseaux sociaux

Sauf autorisation expresse, l'Utilisateur n'est pas autorisé à s'exprimer au nom de l'Entreprise ni à publier du contenu appartenant à celui-ci. Sauf autorisation expresse, l'Utilisateur n'est pas autorisé à créer ou à utiliser un compte faisant apparaître une dénomination sociale, un nom commercial, une marque ou tout autre signe distinctif appartenant à l'Entreprise. De manière générale, l'Utilisateur ne doit pas donner l'apparence qu'il agit au nom de l'Entreprise sans y être dûment autorisé.

Il n'appartient pas à l'Utilisateur de publier des informations sur ses collègues ou sur toute autre personne liée à l'Entreprise. En particulier, l'Utilisateur s'interdit de publier des photos de ses collègues ou Données Personnelles sans leur autorisation. En conséquence, avant de partager sur les réseaux sociaux toute forme de contenu, l'Utilisateur doit s'assurer au préalable qu'il ne s'agit pas de contenu confidentiel, illicite ou portant atteinte aux droits de l'Entreprise ou de tiers.

Si l'Utilisateur utilise certains réseaux sociaux, notamment les réseaux professionnels, sur lesquels il mentionne son poste et/ou ses activités au sein de l'Entreprise, il doit les mettre à jour en fonction de son évolution professionnelle pour que ses comptes et/ou profils sur les réseaux sociaux mentionnent le poste et/ou la fonction qu'il occupe réellement.

Il est rappelé à l'Utilisateur qu'il n'est pas autorisé à publier du contenu protégé tant par des droits de propriété intellectuelle appartenant à l'Entreprise ou à tout autre tiers que par des obligations de confidentialité souscrites par l'Entreprise auprès de tiers.

5.3. Monitoring et traçage

5.3.1. Monitoring et contrôle interne

Les connexions établies par l'Utilisateur sur des sites internet pendant son temps de travail, grâce à l'outil informatique mis à sa disposition par l'Entreprise et pour l'exécution de son travail, sont présumées avoir un caractère professionnel de sorte que l'Administrateur du Système d'information peut les rechercher aux fins de les identifier, hors de la présence de l'Utilisateur. Une utilisation privée d'internet et des réseaux sociaux est néanmoins tolérée à condition que celle-ci soit faite avec discernement et qu'elle soit adaptée, raisonnable et non abusive dans la durée.

L'Administrateur du Système d'information opère un monitoring de ce dernier, ce qui peut l'amener à contrôler les connexions de l'Utilisateur. Ces contrôles portent sur :

- La fréquence des connexions [de façon globale/par service/par Utilisateur] ;
- La durée des connexions [de façon globale/par service/par Utilisateur] ;
- Les sites les plus visités [de façon globale/par service/par Utilisateur] ;

- Les données de connexion à Internet recueillies dans le cadre de ces contrôles sont conservées pendant une durée maximale de 12 mois, et les autres fichiers journaux sont conservés pendant une durée de 12 mois.

L'Administrateur du Système d'information peut limiter la durée de connexion, imposer des configurations de sécurité du navigateur et des limites de taille au téléchargement de contenus par note de service. A ce titre, et pour garantir le maintien en condition opérationnelle du Système d'information, l'Administrateur du Système d'information pourra être amené à interrompre et/ou interdire à tout moment l'accès à certains sites internet et aux réseaux sociaux.

L'Administrateur se réserve la possibilité d'effacer du Système d'information, toute trace de logiciels, progiciels, programmes ou fichiers introduits dans le Système d'information de l'Entreprise, en violation des droits de propriété intellectuelle des tiers et de dénoncer tout acte délictueux aux autorités, sans préjudice de l'application des sanctions prévues par la présente Charte.

Enfin, à 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.

5.3.2. Traçage externe

Toutes les activités de l'Utilisateur ainsi que les données concernant l'Utilisateur (sites consultés, messages échangés, données fournies à travers des formulaires, données collectées à l'insu de l'Utilisateur, etc…) peuvent être enregistrées par des tiers, analysées pour en déduire ses centres d'intérêt, les préoccupations de l'Entreprise, etc… et utilisées à des fins commerciales ou autres. Toutes précautions doivent être prises par l'Utilisateur à cet égard.

Article 6 – GESTION DES DONNEES DE L'ENTREPRISE

6.1. Confidentialité

La sauvegarde des intérêts de l'Entreprise nécessite le respect par l'Utilisateur d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et des données dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

L'Utilisateur est tenu de respecter la confidentialité des Informations Confidentielles dont il a connaissance par le biais du Système d'information et dont il est dépositaire. Il contribue autant que possible à la sûreté du Système et à la sécurité des informations.

Le respect de cette obligation implique notamment de :

- Veiller à ce que les tiers non autorisés n'aient pas connaissance d'Informations Confidentielles et ne pas transmettre à un tiers toute Information Confidentielle, et ce, quel que soit le support et le mode de communication utilisés (notamment par papier, messagerie électronique, utilisation d'internet ou des réseaux sociaux) ;
- N'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres Utilisateurs ;

- Ne pas extraire les Informations Confidentielles et ne pas les reproduire sans l'accord préalable du supérieur hiérarchique et/ou les détourner de leur utilisation normale à des fins non professionnelles ;
- D'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein de l'Entreprise.

L'ensemble des informations contenues dans l'Intranet de l'Entreprise et notamment, les données à caractère personnel figurant dans l'annuaire de l'Entreprise ainsi que les documents non rendus publics et figurants dans l'Intranet, revêtent un caractère strictement confidentiel.
Aucune diffusion de ces informations en dehors de l'Entreprise n'est autorisée sans l'accord préalable de la hiérarchie.

En outre, l'accès par les Utilisateurs aux informations et documents conservés sur le Système d'information doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres Utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux messages privés de type courrier électronique dont l'Utilisateur n'est destinataire ni directement, ni en copie.

De même, chaque Utilisateur est soumis à un devoir de réserve en ce qui concerne les Informations Confidentielles auxquelles il a accès et en particulier les informations, projets, réunions et autres activités internes liées à la vie et à l'avenir de l'Entreprise et il doit s'abstenir de publier, transférer, diffuser ou commenter toute Information Confidentielle qui ne serait pas divulguée avec l'accord de l'Entreprise.

L'Utilisateur ne doit pas, sauf autorisation préalable, commenter tout évènement lié à des affaires juridiques ou à des litiges impliquant l'Entreprise.

6.2. Données personnelles

L'Entreprise traite les données à caractère personnel relatives aux Utilisateurs conformément à la réglementation applicable en matière de protection des Données Personnelles.

Les traitements mis en œuvre sont recensés dans le registre des activités de traitement lorsque la réglementation l'exige et font l'objet des mesures d'information appropriées.

Lorsque des Données Personnelles concernant un Utilisateur sont diffusées sur l'Intranet ou au moyen d'un autre outil interne, notamment son identité, ses coordonnées professionnelles ou son image, celui-ci est préalablement informé du traitement réalisé, de sa finalité et des droits dont il dispose.

Tout Utilisateur peut exercer, dans les conditions prévues par la réglementation applicable, les droits dont il bénéficie à l'égard de ses Données Personnelles, notamment ses droits d'accès, de rectification, d'effacement, de limitation et, lorsqu'il est applicable, son droit d'opposition.

Les demandes relatives à l'exercice de ces droits peuvent être adressées au Délégué à la Protection des Données à l'adresse suivante : rgpd@novarc.com.

Pour plus d'informations, les Utilisateurs sont invités à consulter la documentation relative à la protection des Données Personnelles mise à leur disposition par l'Entreprise.

6.3. Propriété intellectuelle

L'Utilisateur doit avoir conscience qu'il est soumis à la loi et que ses actes sont susceptibles non seulement d'engager sa responsabilité personnelle pour les délits (contrefaçon, injure, piratage) qu'il commet et les préjudices qu'il cause, mais aussi d'engager la responsabilité de l'Entreprise.

Aussi, il s'interdit de porter atteinte, notamment, aux droits des tiers, aux droits des cocontractants de l'Entreprise et aux droits de l'Entreprise.

Il devra notamment veiller à respecter les droits de propriété intellectuelle, en particulier les droits des auteurs et titulaires de droits d'exploitation de logiciels (copyrights, droits prévus au contrat du prestataire) ;

Il est donc interdit à l'Utilisateur :

- De faire du streaming à usage privé,
- De télécharger illégalement un contenu protégé par des droits d'auteur,
- De contourner ou de tenter de contourner les mesures techniques de protection des logiciels et des programmes appartenant à l'Entreprise ou qui lui sont concédés par des licences d'utilisation ;
- D'effectuer des copies permanentes ou temporaires des logiciels et des programmes appartenant à l'Entreprise ou qui lui sont concédés par des licences d'utilisation sur quelque support d'enregistrement que ce soit ;
- De diffuser auprès de tiers les logiciels et programmes appartenant à l'Entreprise ou qui lui sont concédés par des licences d'utilisation ;
- De modifier les programmes et logiciels appartenant à l'Entreprise ou qui lui sont concédés par des licences d'utilisation ;
- D'extraire des données des bases de données de l'Entreprise, notamment par « scraping » ;
- De télécharger, reproduire, utiliser, modifier ou diffuser des photographies, vidéos, images, musiques, textes ou tout autre contenu protégé par un droit de propriété intellectuelle sans disposer des droits, licences ou autorisations nécessaires à cette utilisation ;
- De copier tout ou partie de l'architecture des bases de données qui sont la propriété exclusive de l'Entreprise.

Article 7 – SECURITE

7.1. Moyens techniques

L'Entreprise utilise des dispositifs techniques pour empêcher l'intrusion de virus informatiques. Il est impératif que chaque Utilisateur procède selon les instructions de l'Administrateur du Système d'information, à une mise à jour régulière des procédés techniques installés sur leur Poste de travail, afin que celui-ci soit protégé de manière efficace.

7.1.1. Dispositifs de protection contre les attaques informatiques

Plusieurs dispositifs sont mis en œuvre (pare feux, antivirus, anti-spam…). Ces dispositifs contrôlent le flux de données échangées mais également la présence de logiciels malveillants dans les fichiers, courriels etc…

Tous ces dispositifs sont évolutifs et mis en place par l'Administrateur du Système d'information en fonction de l'évolution des menaces et des pratiques délictuelles et criminelles.

Ces dispositifs peuvent notamment amener l'Entreprise à détenir une trace :

- De l'activité de l'Utilisateur sur internet : sites visités, heures des visites, éléments téléchargés, leur nature (texte, image, vidéo ou logiciels),

- Des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe.

L'Utilisateur devra opter pour la double authentification, aussi appelée validation ou vérification en deux étapes (ou encore « 2FA » ou « MFA ») lorsque le choix lui est laissé pour la connexion à son Poste de travail ou à l'un quelconque des logiciels de l'Entreprise et qu'il dispose d'un téléphone portable et/ou d'un dispositif spécifique, mis à sa disposition par l'Entreprise. L'Utilisateur veillera à ne pas faire suite à des messages/mails répétés lui demandant de confirmer une demande qu'il n'aurait pas initiée.

7.1.2. Backups

Pour assurer la sécurité des données de l'Entreprise, l'Utilisateur doit impérativement stocker le contenu de son travail et les données concernant l'Entreprise sur les serveurs de cette dernière. Toute donnée présente sur le Poste de travail de l'Utilisateur en « local » est susceptible d'être définitivement perdue. Dans les cas où l'Utilisateur est contraint de disposer de données en « local » sur son Poste de travail, il se rapproche de l'Administrateur du Système d'information pour qu'une solution de sauvegarde automatique de son Poste de travail soit mise en œuvre (par exemple OneDrive)

L'Entreprise a mis en place un grand nombre de moyens techniques permettant d'assurer la confidentialité, l'intégrité et la disponibilité des données de l'Utilisateur et notamment ceux permettant d'assurer la sauvegarde de secours des données en cas de défaillance d'un espace de stockage du Système d'information.

Ceci implique entre autres que la suppression par un Utilisateur d'un fichier de son Poste de travail, n'est pas absolue et qu'il en reste potentiellement une copie :

- Sur le dispositif de sauvegarde ou miroir,
- Sur un serveur,
- Sur les dispositifs de sécurité,
- Chez un hébergeur.

L'Administrateur du Système d'information fixe la fréquence et les modalités de ces sauvegardes pour chaque Utilisateur ou groupe d'Utilisateurs.

7.2. Moyens organisationnels

L'Entreprise met en place en plus de mesures techniques, des moyens organisationnels afin de préserver l'intégrité et la sécurité du Système d'information.

Pour diffuser l'ensemble de ces mesures au sein de l'Entreprise, les Utilisateurs sont amenés à recevoir des notes de service et suivre des formations/sensibilisations aux bonnes pratiques sur l'utilisation des outils informatiques. L'Administrateur met également en place des stratégies de groupe (« GPO ») afin d'assurer le respect de ces bonnes pratiques.

Les moyens organisationnels peuvent porter sur les sujets/pratiques énumérés de façon non-exhaustive, ci-dessous :

- Interdiction de télécharger tout programme ou élément de programme, application, "plugin" ou mise à jour à partir d'un serveur internet, quand bien même serait-il incité à le faire par son éditeur ;

- Interdiction de connecter un équipement informatique n'appartenant pas à l'Entreprise au Système d'information de celle-ci. Cela concerne notamment la connexion d'une clé USB personnelle au Poste de travail de l'Utilisateur ou la connexion de l'ordinateur personnel de l'Utilisateur à un réseau local de l'Entreprise (filaire ou wifi) ;

- Interdiction de modifier un équipement informatique appartenant à l'Entreprise ;

- Ne pas oublier de récupérer sur les imprimantes ou photocopieurs, les documents sensibles qui sont envoyés, imprimés ou photocopiés ;

- Ne pas laisser en libre accès des supports informatiques (disquette, clé USB, disque dur externe…) contenant des données confidentielles dans un bureau ouvert ou dans des lieux publics sans surveillance ;

- Ne pas déposer des données confidentielles sur des espaces cloud en libre accès à tout le monde (ex : partages Teams à tout le monde,) Ne pas répondre aux courriels et messages de masse ou en chaîne ;

- Ne pas ouvrir de pièces jointes/fichiers s'ils apparaissent douteux ;

L'ensemble de ces mesures organisationnelles sont amenées à évoluer au fur et à mesure de l'état des connaissances dans le domaine de la sécurité informatique et de l'évolution des règles et usages en la matière sous la gouvernance du RSSI.

Article 8 – ENGAGEMENT DE L'UTILISATEUR

La présente Charte est applicable à l'Utilisateur dans l'ensemble de ses dispositions. Dès lors, il s'engage à la connaitre et à l'appliquer sans réserve.

Tout manquement caractérisé d'une ou plusieurs dispositions de la présente Charte par l'Utilisateur pourra faire l'objet de sanctions, conformément à l'article 10 des présentes.

Article 9 – AUDIT

L'Entreprise pourra procéder périodiquement, par tous moyens, à des audits de contrôle de la bonne application de la présente Charte, dans les limites prévues par la loi.

Article 10- SANCTIONS

Pour les salariés soumis au règlement intérieur de l'Entreprise, tout manquement aux obligations résultant de la présente Charte est susceptible de constituer une faute pouvant donner lieu à l'application d'une sanction disciplinaire dans les conditions prévues par la réglementation et le règlement intérieur applicables.

Indépendamment de toute sanction disciplinaire, l'Entreprise peut, lorsque la sécurité du Système d'information ou la protection de ses intérêts le justifie, suspendre, limiter ou supprimer tout ou partie des droits d'accès d'un Utilisateur, dans le respect des dispositions applicables.

Pour les Utilisateurs tiers, tout manquement à la présente Charte peut entraîner la suspension ou le retrait des droits d'accès au Système d'information et, lorsque les stipulations contractuelles et la réglementation applicables le permettent, la résiliation de la relation contractuelle, sans préjudice de toute demande de réparation du préjudice subi par l'Entreprise.

Lorsqu'un manquement est susceptible de constituer une infraction pénale ou de donner lieu à une procédure judiciaire ou administrative, les informations légalement collectées dans le cadre de l'utilisation du Système d'information peuvent être conservées et communiquées aux autorités ou juridictions compétentes dans les conditions prévues par la réglementation applicable.

Le non-respect de la présente Charte peut également engager la responsabilité civile ou pénale de l'Utilisateur dans les conditions prévues par la loi.

Article 11- FORMATION / SENSIBILISATION

L'Entreprise organise les formations nécessaires à chaque Utilisateur pour appliquer les règles et prescriptions de sécurité prévues par la présente Charte.
Elles comprennent notamment :

- Une formation sur la sécurisation du poste de travail et l'accès aux applications de l'Entreprise ;
- Un rappel des procédures de demandes d'accès aux applications de l'Entreprise.

Chaque Utilisateur doit se former aux techniques de sécurité et maintenir son niveau de connaissance en fonction de l'évolution de ces techniques.

Des campagnes de sensibilisation sont organisées par l'Entreprise. L'ensemble des modules dispensés à ces occasions sont obligatoires.

Les Utilisateurs amenés à utiliser des Outils d'IA dans le cadre de leurs fonctions bénéficient d'une information, d'une sensibilisation ou d'une formation adaptée aux caractéristiques des outils et à leurs conditions d'utilisation.

Cette sensibilisation porte notamment sur les limites des Systèmes d'IA, la vérification des résultats produits, la protection des Données Personnelles et des Informations Confidentielles, les risques de sécurité, les droits de propriété intellectuelle et les règles internes relatives à l'utilisation de l'IA.

L'Entreprise veille à maintenir un niveau approprié de maîtrise et de sensibilisation des personnes utilisant des Systèmes d'IA pour son compte, en tenant compte de leurs connaissances, de leur expérience et du contexte dans lequel ces systèmes sont utilisés.

Article 12 – VIGILANCE

Il est demandé à chaque Utilisateur de signaler toute tentative de violation de son Poste de travail, de ses fichiers ou de ses données, dès qu'il en a connaissance, auprès de son responsable hiérarchique et de l'Administrateur du Système d'information afin de permettre une réaction immédiate et pertinente. Pour contacter l'Administrateur au sujet de l'utilisation des ressources du Système d'information, l'Utilisateur doit se référer à la procédure de gestion de crise « cyber ».

Si, dans l'accomplissement de son travail, l'Utilisateur est amené à constituer des fichiers entrant dans le champ d'application de la règlementation Informatique et Libertés, il devra en informer l'Administrateur du Système d'information ou la direction de l'Entreprise, afin de procéder aux formalités CNIL qui seraient susceptibles d'en découler.

Enfin, en cas d'attaque informatique, l'Utilisateur ne doit surtout pas éteindre sa machine ni effacer de fichiers. Dans un tel cas de figure, l'Utilisateur doit contacter l'Administrateur du Système d'information sans délai.

novarc
GROUPE



815 C Chemin du Razas
Z.I. Les plaines
26780 Malataverne
Tel : +33 (4) 75 90 58 00

SIREN : 380 765 131
SIRET (siège) : 380 765 131 00020
Inscription au RCS : 380 765 131 R.C.S.
Romans Numéro de TVA : FR28380765131
Forme juridique : SA à directoire
Capital social : 3 900 446,75 €