Hall 32
RÉVÉLEZ-VOUS
DANS L'INDUSTRIE
DE DEMAIN

Annexe 5

Charte informatique

Par Johann GUIRANDE

Responsable informatique

johann.guirande@hall.32.fr

Mis à jour le 23/02/2024

SOMMAIRE

Hall 32 met à la disposition du personnel un Système d'Information et de communication tel que décrit à l'article III.5 ci-dessous (ci-après le SI) pour l'exercice de ses activités professionnelles comprenant notamment un réseau informatique et téléphonique, ainsi que des outils fixes et mobiles.

Son utilisation implique le respect de certaines règles et précautions d'usage dans le but d'assurer la confiance dans le SI et d'en préserver l'intégrité et le bon fonctionnement dans le respect des dispositions légales et réglementaires applicables.

Dans un souci de transparence à l'égard des Utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du SI, la présente Charte (ci-après la « Charte ») pose les règles relatives à l'utilisation du SI et définit les moyens de contrôle et de surveillance de cette utilisation.

I. OBJET

La Charte n'a pas pour objectif de couvrir de manière exhaustive tous les cas de figure possibles, mais de fixer les principes généraux d'utilisation, les précautions d'usage du SI mis à disposition des Utilisateurs, dans le cadre de leur activité professionnelle, ainsi que les responsabilités respectives de l'Entreprise et de l'utilisateur.

II. DOMAINE D'APPLICATION

1. Personnes concernées

Cette Charte est applicable à tout membre du personnel quel que soit son statut et à toute personne liée à l'Entreprise par un contrat prévoyant, directement ou indirectement le respect de cette Charte (notamment aux prestataires de service, consultants, sous-traitants, stagiaires, intérimaires, …) et, de façon générale, à toute personne amenée à créer, développer ou utiliser le SI de l'Entreprise, ci-après désignée par « Utilisateur(s) ».

Cette Charte constitue une adjonction au règlement intérieur de l'Entreprise et annule toutes dispositions contraires contenues dans le règlement intérieur existant, relatives au fonctionnement et à l'utilisation du SI. L'avis du Comité Central d'Entreprise et du CHSCT a été recueilli conformément aux dispositions des articles L.1321-4 et suivants du Code du Travail.

Le non-respect des dispositions de cette Charte expose le contrevenant, membre du personnel de l'Entreprise, aux sanctions prévues à l'article VII ci-dessous.

2. Usages concernés

La présente Charte s'applique à tous les types d'usage, qu'ils aient lieu :

› dans les locaux de l'Entreprise ;
› dans le cadre d'un usage dit « nomade », quel que soit le lieu ;
› dans le cadre d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.).

La présente Charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des moyens informatiques et de communication électronique.

3. Dérogation

Toute demande de dérogation à la présente Charte doit être adressée à l'Entreprise, via le Responsable SI. L'Entreprise se réserve le droit de l'accepter ou de la refuser.

III. DEFINITIONS

1. Administrateurs du SI

Les Administrateurs sont en charge de l'administration du SI, en assurent la protection, le bon fonctionnement, la maintenance et la sécurité.

Dans l'accomplissement de leur mission, ils ont accès, d'une manière générale, à l'ensemble des composants du SI et aux informations relatives à l'Utilisateur (messagerie, connexions à Internet, historique des sites visités, fichiers "log", etc…) y compris celles enregistrées sur le disque dur de son poste de travail. Ils sont donc, dans le cadre et pour l'accomplissement de leur mission, en droit de prendre connaissance de l'ensemble des données accédées, émises ou élaborées par l'Utilisateur.

Les Administrateurs du SI sont tenus au secret professionnel qui leur interdit de divulguer certaines informations dont ils ont connaissance dans le cadre de leurs fonctions. Il s'agit des informations qui relèvent expressément de la vie privée de l'Utilisateur et qui ne mettent pas en cause le bon fonctionnement, la sécurité du SI et/ou tout intérêt de l'Entreprise.

2. Données à caractère personnel

Les données à caractère personnel correspondent à toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

3. Messagerie électronique

La messagerie correspond à l'outil et aux services associés (messagerie instantanée, partage d'écran, vidéo conférence en ligne au poste de travail…) permettant la transmission de tout courrier ou information au format électronique transmis à l'aide des services informatiques mis à disposition de l'Utilisateur.

4. Ressources informatiques

Les ressources informatiques concernent tout moyen informatique utilisé pour les besoins de l'Entreprise entendu au sens le plus large, comme l'ensemble des éléments matériels (tels que les ordinateurs, fixes ou portables, tablettes, et tout autre matériel informatique, connectique ou bureautique y compris les postes de travail, serveurs, routeurs, switchs, réseaux locaux filaires et sans fil, fax, photocopieurs, téléphones, fixes ou portables, smartphones, système de navigation fixe ou portable, agendas électroniques, périphériques incluant notamment les disques durs, etc.), ainsi que les éléments logiciels (contenus dans ou faisant fonctionner, inter opérer ou protégeant en totalité ou en partie lesdites ressources Informatiques, y compris les protocoles de communication utilisés pour la mise en réseau des postes informatiques TCP/IP, DNS, FTP), permettant notamment la création, la consultation, la modification, la suppression, la destruction, l'échange, la circulation, la diffusion, la duplication, la reproduction et le stockage de toutes données, fichiers, bases de données, Intranet, extranet, Internet, sous forme d'images, de sons, de textes, ou tous flux quelconques d'information entre les Utilisateurs ou entre les Utilisateurs et l'extérieur. Bien que ne faisant pas physiquement partie du SI, lorsque le personnel, avec l'accord de l'Entreprise, utilise du matériel personnel connecté au réseau de l'Entreprise ou contenant des informations à caractère professionnel concernant l'entreprise, il doit respecter la Charte.

5. Système d'Information et de communication (SI)

Le système d'information (SI) est un ensemble organisé de ressources qui permet notamment de collecter, stocker, traiter et distribuer de l'information. Cet ensemble englobe des données, des moyens matériels et logiciels ainsi que des procédures.

6. Traitement

Un traitement correspond à toute opération ou ensemble d'opérations portant sur des données à caractère personnel ou non, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, ainsi que le verrouillage, l'effacement ou la destruction de telles données.

7. Utilisateur

L'Utilisateur comprend toute personne, salariée ou non de l'Entreprise, tous statuts juridiques confondus, permanents ou temporaires, autorisés à utiliser le SI.

IV. REGLES D'UTILISATION DU SYSTEME D'INFORMATION

1. Règles générales

La présente Charte s'appuie sur un ensemble de textes législatifs et réglementaires. Il s'agit notamment des lois et des réglementations sures :

› la liberté de la presse ;
› la protection des données à caractère personnel ;
› le droit au respect de la vie privée ;
› le droit de la propriété intellectuelle ;
› la protection des systèmes d'information ;
› la cryptologie ;
› …

Dont certaines dispositions peuvent être passibles de sanctions pénales.

Au regard de ces lois, l'Utilisateur qui contribue, à son niveau, à la sécurité du SI, s'engage à ne pas adopter un comportement de nature à porter atteinte aux droits et/ou à l'image, à la sécurité et à la réputation de l'Entreprise et/ou des tiers. L'utilisateur veillera par son comportement vigilant à traiter avec précaution les éléments provenant de sources externes non vérifiées. Il fera particulièrement attention à ne pas mettre en danger le SI lors d'attaques de Phishing (hameçonnage) ou d'échanges de clés USB ou de fichiers. En cas de doute, l'utilisateur ne doit pas traiter cette information et devra informer le Responsable informatique.

L'Utilisateur reconnaît être conscient que ses actes sont susceptibles d'engager sa responsabilité personnelle pour les infractions (contrefaçons, injures, piratages, etc.) qu'il commet ou les préjudices qu'il cause.

Il est notamment interdit à l'Utilisateur, sans que cette liste soit limitative, de :

- traiter des données à caractère personnel sans respecter les obligations résultant de la loi n°78-17 du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés, modifiée ;
- consulter, communiquer ou stocker des données à caractère illicite, c'est-à-dire dont le contenu est en infraction avec la législation nationale (contenus pédophiles, incitations à la haine raciale, terrorisme, etc.) ;
- porter atteinte à des droits privatifs, tels que des œuvres ou logiciels protégés,
- traiter des informations présentant un caractère mensonger, injurieux, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de porter atteinte à la vie privée des personnes ou à leur dignité ;
- traiter des informations relatives à la race, l'origine nationale, les mœurs, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap ;
- consulter, copier ou télécharger le contenu de fichiers ou de sites à caractère pornographique, pédophile, négationniste, extrémiste ou contraire aux bonnes mœurs ou à l'ordre public ;
- adopter tout comportement pouvant inciter des tiers à adresser à l'Utilisateur de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc. ;
- utiliser le SI à des fins de harcèlement, menace, chantage et, de manière générale, à violer les lois ou réglementations en vigueur ;
- falsifier le contenu et les propriétés d'un fichier ;
- utiliser l'identité d'un tiers à des fins autres que celles pour lesquelles l'Utilisateur a été autorisé ;
- utiliser ses coordonnées professionnelles ou celles de tiers pour s'inscrire sur ou utiliser des sites Internet sans rapport avec son activité professionnelle ;
- commettre toute action susceptible de mettre en cause la sécurité de l'Entreprise, en particulier de porter atteinte aux dispositifs de sécurité interdisant les reproductions ou communications des données professionnelles confidentielles, de porter atteinte à sa réputation ou de constituer pour elle une gêne quelconque ;
- porter atteinte à la sécurité du SI,
- compromettre les intérêts de l'Entreprise,
- commettre tout acte impliquant :
    - tout mode de chiffrement non conforme aux procédures internes de l'Entreprise,
    - et, plus généralement, toute action illégale et/ou contraire à la Charte ou aux procédures applicables à l'Entreprise, ou toute action susceptible d'entraîner la responsabilité civile et/ou pénale de l'Entreprise.

En cas de présomption d'une violation des dispositions de la Charte comme en cas de violation(s) grave(s) ou répétée(s) ou de dépassement des usages privés tolérés, ou d'une disposition légale ou réglementaire, des contrôles portant sur l'utilisation du SI pourront être effectués conformément à l'article V de la présente Charte.

L'utilisation du SI par les représentants du personnel dans l'exercice de leur mandat requiert la conclusion d'un accord préalable.

2. Respect de la propriété intellectuelle

L'utilisation du SI implique le respect des droits de propriété intellectuelle et notamment de la réglementation relative à la propriété littéraire et artistique et au droit du producteur de la base de données.

Pour des raisons de sécurité de fonctionnement et de respect des droits de propriété intellectuelle des tiers, seuls les logiciels autorisés par l'Entreprise peuvent être utilisés et/ou installés au sein du SI, dans les termes et conditions des droits souscrits par elle.

Aucune création (notamment logiciels, bases de données, contenus tels que notamment articles, photographies, pages web, fichiers musicaux ou vidéos), récupération, stockage et diffusion d'informations, protégé par des droits d'auteur et/ou tout autre droit de propriété intellectuelle, ne peut être utilisé sans l'autorisation des titulaires des droits, sous peine de commettre un délit de contrefaçon, passible de sanctions pénales. Conformément à la loi applicable, l'Entreprise veillera à ce que les moyens qu'elle met à disposition de ses salariés ne servent pas à commettre des agissements délictueux (accès à Internet, messagerie etc.) comme par exemple contrevenir aux droits de propriété intellectuelle par un téléchargement illégal d'œuvres protégées par le droit d'auteur.

Aucun message électronique ne doit comporter d'éléments protégés par les lois en vigueur sur la propriété intellectuelle, autres que ceux expressément autorisés par l'Entreprise.

3. Mobilité

Dans le cadre de ses déplacements professionnels, peu importe leur durée ou leur fréquence, l'Utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et du SI auxquels il pourrait être amené à accéder.

A ce titre, l'utilisateur du SI a le devoir de respecter les règles suivantes :

› s'informer, auprès du Responsable SI, des mesures particulières de sécurité et de sûreté relatives au système d'information à observer en fonction de sa destination, s'il s'agit d'un pays étranger ;
› adopter la plus stricte discrétion sur l'Entreprise et ses activités au sein de celle-ci lorsqu'il utilise des moyens informatiques dans des lieux publics, notamment les trains, gares, aéroports, avions, salons professionnels, restaurants et parties communes des hôtels, en veillant notamment à ne pas manipuler ni communiquer d'éléments confidentiels, secrets, sensibles ou stratégiques en de tels lieux ;
› ne pas discuter d'informations confidentielles, secrètes, sensibles ou stratégiques au téléphone, particulièrement si la conversation se déroule dans un lieu public. Ne pas faire directement référence au nom de l'Entreprise dans ces conversations, ni faire mention d'un projet autrement que par son nom de code ou en termes génériques ;
› s'engager à respecter les conditions d'accès des applications. Plus particulièrement, il veillera à ne pas contourner l'usage de certains outils ou services pour accéder par quelque moyen que ce soit à des applications ou services en dehors du cadre prévu.
› veiller à utiliser tous les moyens de prévention de vol (câble antivol, …) et de protection d'informations disponibles (chiffrement, écrans polarisés) et ne pas laisser ses affaires professionnelles sans surveillance, afin de réduire la probabilité d'un vol de matériel ou d'information et d'en limiter les conséquences ;
› mémoriser et ne jamais inscrire les informations de connexion sur papier récapitulant ses codes et accès au SI sauf à ce qu'ils soient conservés dans un coffre sécurisé
› lors d'un voyage en avion, systématiquement conserver son ordinateur portable, son téléphone portable, tablette ainsi que l'ensemble des supports de stockage transportés en tant que bagages à main et de ne jamais les faire voyager en soute ;
› ne jamais laisser sans surveillance les matériels informatiques dans un lieu public (compartiment bagage d'un train, salon d'attente d'aéroport, banquette arrière ou coffre d'un véhicule dont le contenu est visible de l'extérieur) ;
› s'abstenir de consulter ou d'échanger des informations confidentielles, secrètes, sensibles ou stratégiques à partir d'un ordinateur ou terminal téléphonique extérieur (utilisation du standard ou fax

d'un hôtel, utilisation d'un téléphone ou d'un ordinateur mis à disposition par un tiers, même s'il s'agit d'un partenaire ou d'un client) ;
› alerter le Responsable SI dans les plus brefs délais de tout événement suspect (déplacement d'ordinateur portable ou d'objets personnels dans la chambre d'hôtel, fouille et saisie temporaire d'ordinateurs au contrôle des douanes, intérêt manifeste et questionnement sur l'Entreprise de la part de voyageurs tiers, etc.) ;
› alerter le Responsable SI en cas de perte ou de vol de matériel et/ou le Référent Environnement et Prévention.

L'Utilisateur du SI est averti du fait que les formalités douanières de certains pays (Etats-Unis et Chine notamment) permettent, en toute légalité, aux agents assermentés de ces pays, de procéder à une saisie temporaire des matériels informatiques afin d'en examiner le contenu et d'en établir une copie intégrale. Dans un tel cas, l'Utilisateur doit se soumettre à ces formalités et en informer le Responsable SI dès que possible. Toutefois, afin de limiter les conséquences potentielles pour l'Entreprise, il est expressément recommandé aux Utilisateurs de réduire au strict nécessaire la quantité d'informations confidentielles, secrètes, sensibles ou stratégiques présentes sur ces matériels lors de tels déplacements, afin de stocker les données de façon sécurisée. Dans certains cas, il sera préférable d'utiliser un support de stockage distant mis en place par l'Entreprise (disque virtuel, accès aux serveurs de fichiers par tunnel chiffré) pour stocker de telles informations lors d'un déplacement.

4. Utilisation du SI à des fins professionnelles

Les informations manipulées et utilisées sont traitées, enregistrées et échangées exclusivement sur et à partir des ressources informatiques autorisées par l'Entreprise.

L'usage du SI est présumé, sauf preuve contraire, avoir un caractère professionnel. Dès lors, l'employeur est en droit d'accéder aux informations de l'utilisateur, y compris hors la présence de l'intéressé.

Aux termes de la jurisprudence, sont ainsi présumés avoir un caractère professionnel, notamment :

› les documents et les fichiers conservés, transmis ou reçus à partir du SI par un Utilisateur, sauf lorsque celui-ci les identifie expressément comme relevant d'un usage privé, selon les modalités ci-après définies ;
› les connexions établies par un utilisateur sur des sites Internet pendant son temps de travail à l'aide du SI ;
› les messages adressés et reçus par l'utilisateur à l'aide du SI mis à sa disposition par l'Entreprise pour les besoins de son activité professionnelle.

Les messages/fichiers/données créés en utilisant le SI étant présumés professionnels, l'Utilisateur, conformément à son obligation de loyauté, s'engage à ne pas les transformer en messages/fichiers/données à usage personnel et à ne pas insérer dans le SI d'éléments ayant trait à une activité étrangère aux fonctions qu'il exerce au sein de l'Entreprise.

Chaque utilisateur doit veiller, en cas d'absence temporaire, à ce que la continuité du service soit assurée, conformément aux modalités d'organisation du service telles que définies par sa hiérarchie. Par conséquent, en cas d'absence de l'utilisateur pour quelque raison que ce soit, le supérieur hiérarchique est en droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tous documents à caractère professionnel de l'utilisateur, ayant recours si nécessaire aux Administrateurs système.

5. Utilisation du SI à des fins privées

Sous réserve des dispositions de l'article IV.4, un usage privé à des fins non commerciales raisonnable du SI est toléré, à condition :

› d'avoir une utilisation raisonnable et réservée aux impératifs de la vie quotidienne (appel de courte durée, brèves consultations de serveurs, …) de ne pas pénaliser l'activité professionnelle de l'utilisateur,
› de ne pas générer de consommations excessives (surcharge des réseaux, …),
› de ne pas nuire à la sécurité du SI,
› de ne pas en perturber le bon fonctionnement,
› de ne pas nuire à, compromettre, ou mettre en danger, l'intérêt ou/et la réputation de l'Entreprise,
› et de respecter les règles et précautions d'usage définies dans la présente Charte.

L'Utilisateur peut se créer un « espace privé », identifié comme tel, dédié au classement et à la conservation des fichiers et des correspondances privées.

Tous les répertoires informatiques, fichiers, documents ou autre support figurant dans l'« espace privé » ou portant la mention « privé » ou « personnel » seront présumés être de nature privée.

A l'inverse, tous les répertoires informatiques, fichiers, documents ou autre support, figurant dans des espaces autres que l' « espace privé » et n'étant pas identifiés comme « privé » ou « personnel » seront présumés être de nature professionnelle.

Dans le cadre d'un usage non-professionnel de la messagerie professionnelle, l'utilisateur est tenu, s'il souhaite émettre des courriers électroniques ou toute autre forme de message, de mentionner dans l'objet le terme « privé » et/ou « personnel ».

Toutefois, en cas de risque particulier notamment de sécurité, de continuité du service ou d'un risque grave de voir sa responsabilité engagée, l'employeur a le droit d'accès aux messages, fichiers, données, documents ou autres supports identifiés comme privés ou personnels, si l'utilisateur a été dûment convié ou si l'utilisateur est présent.

L'Utilisateur devra effacer toute donnée personnelle avant son départ de l'Entreprise. Dans tous les cas, l'usage privé du système d'information relève de la seule et entière responsabilité de l'Utilisateur, qui dégage en conséquence l'Entreprise de toute responsabilité.

L'espace privé d'un Utilisateur quittant l'Entreprise, s'il n'a pas été détruit par lui, sera supprimé sans copie, ni prise de connaissance préalable du contenu par l'Entreprise. Le départ de l'utilisateur entraîne la fermeture de sa boîte aux lettres en émission et en réception ainsi que de sa boite vocale.

Le raccordement de moyens informatiques privés, sur initiative individuelle, est interdit. Seuls les Administrateurs du SI peuvent être amenés à introduire de nouveaux éléments et à faire de nouvelles connexions au SI.

6. Utilisation de la messagerie électronique

Les messages électroniques sont notamment soumis à un contrôle antiviral et à un filtrage anti-spam.

En raison des risques liés à l'interception des messages électroniques, l'utilisation de la messagerie à destination de l'extérieur du SI doit être limitée aux informations à caractère non confidentiel et non sensible pour l'Entreprise. Les pièces jointes comportant des informations sensibles doivent être chiffrées avec un outil de chiffrement prescrit par l'Entreprise.

Il est rappelé que tout message électronique est un écrit qui doit être conforme aux dispositions des articles IV.1 et IV.4 de la Charte.

L'envoi, le réacheminement et/ou la conservation de messages en masse ou « en chaînes » est strictement interdit lorsqu'ils ne représentent aucun lien avec les fonctions et les attributions de l'Utilisateur au sein de l'Entreprise.

Les règles hiérarchiques d'organisation des pouvoirs internes de signature doivent être respectées. Ainsi, aucun message électronique ne doit être envoyé par un utilisateur qui n'en a pas l'autorité.

Les utilisateurs qui peuvent consulter à distance, par Internet, notamment leur messagerie professionnelle à l'aide d'un matériel personnel devront effacer dès que possible les fichiers qui seraient copiés sur l'appareil utilisé.

Il est demandé à chaque utilisateur de veiller à la confidentialité de sa messagerie notamment en configurant chaque appareil (ordinateurs, smartphones, tablettes, etc.) afin qu'il se verrouille après une brève période d'inutilisation de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

7. Utilisation de l'Internet

L'Internet est un outil de communication mis à la disposition de l'utilisateur pour un usage professionnel.

Lors de sa connexion à Internet, l'utilisateur voit apparaitre une mention relative à l'encadrement de l'utilisation d'Internet et lui demandant d'accepter les modalités applicables.

Lorsqu'il accède à un réseau extérieur, l'utilisateur représente l'Entreprise et est identifié comme tel.

Il est rappelé que les connexions établies par un utilisateur sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel, de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence.

L'utilisateur doit porter une attention particulière à ses activités sur l'Internet car ses données et celles de l'Entreprise peuvent être enregistrées par des tiers et analysées afin d'établir un profil pouvant, entre autres, être utilisé à des fins de prospection commerciale ou d'intelligence économique.

L'Utilisateur s'engage à :

› ne pas se connecter sciemment, ni télécharger, sur des sites contenant des informations contraires aux dispositions de la Charte ;
› ne pas copier ou télécharger tout programme ou élément de programme, application, "plug in" ou mise à jour à partir d'un serveur Internet avant d'avoir obtenu la dérogation figurant à l'article II.3 de la Charte ;
› ne pas utiliser des services en ligne (parfois appelés SaaS) non explicitement autorisés ou sur une black-list publiée sur l'Intranet de l'Entreprise dédié à l'informatique.

8. Utilisation des médias sociaux

Les médias sociaux comprennent notamment les wikis, les réseaux sociaux, les sites de partage de vidéos, les blogs, les mondes virtuels et les autres plateformes collaboratives en ligne, etc.

Lorsqu'il accède à tout média social extérieur à l'Entreprise, l'utilisateur représente l'Entreprise et est identifié comme tel.

Comme pour l'Internet en général, l'utilisateur doit porter une attention particulière à ses activités sur les médias sociaux extérieurs car ses données et celles de l'Entreprise peuvent être enregistrées par des tiers et analysées afin d'établir un profil pouvant, entre autres, être utilisé à des fins de prospection commerciale ou d'intelligence économique.

L'Utilisateur s'engage notamment à :

› ne pas diffuser à l'extérieur de l'Entreprise d'informations non publiques (en particulier celles relevant de la vie privée d'autrui) ou relevant de la classification secret ou confidentialité de Hall 32,
› ne pas émettre ou relayer, en violation de la Charte, des informations relatives à l'Entreprise,
› respecter les dispositions de Charte dans tous les aspects de l'utilisation des médias sociaux.

9. Utilisation du téléphone

L'utilisation privative des téléphones, smartphone est réservée par principe à un usage strictement professionnel. Seule une utilisation raisonnable et réservée aux impératifs de la vie quotidienne (appel de courte durée, brèves consultations de serveurs ...) est tolérée.

Des restrictions d'utilisation par l'utilisateur de certains téléphones fixes ou portables sont mises en place en tenant compte de la mission de l'Utilisateur ; à titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants.

En cas d'utilisation anormale, l'Entreprise se réserve le droit d'accéder aux numéros complets des relevés individuels, sauf pour les salariés protégés lorsqu'ils utilisent leur téléphone dans le cadre de leur mission élective ou syndicale.

10. Utilisation de l'Intranet

L'Intranet fonctionne sous la responsabilité informatique des Administrateurs du SI et sous la responsabilité éditoriale du Service Communication,

Aucun Utilisateur ne peut introduire ou tenter d'introduire d'éléments ou de contenu sur l'Intranet sans l'autorisation expresse du responsable éditorial du site.

V. PROTECTION DU SYSTEME D'INFORMATION

1. Exercice de la protection

Dans le cadre de leur mission, les Administrateurs du SI mettent en place des outils de gestion d'incidents de sécurité, de maitrise des flux de données, d'analyse de trafic et de contrôle des contenus comme indiqué à l'article V.2 ci-après.

Les Administrateurs du SI peuvent notamment utiliser et/ou faire utiliser des logiciels de prise de main à distance pour accéder à l'ensemble des données de n'importe quel poste de travail informatisé de l'Entreprise. Dans ce cas, l'Utilisateur en est informé préalablement et donne son accord en validant un message d'information apparaissant sur son écran. Il veillera à avoir fermé préalablement tous documents sensibles.

En outre, l'Entreprise s'assure en cas d'externalisation de certaines opérations liées au SI que tout prestataire et ses préposés n'accèdent qu'aux données informatiques nécessaires à l'accomplissement de leur mission et qu'ils s'engagent par contrat à respecter la confidentialité sur les informations dont ils ont connaissance au cours de leur prestation.

L'utilisateur, de son coté, peut être amené à détecter des anomalies (tentative de violation du poste de travail ou de fichiers, vol d'équipements…) qu'il s'engage à signaler immédiatement à son hiérarchique et/ou aux Administrateurs du SI.

L'utilisateur est tenu de suivre les formations et/ou consignes dispensées par l'Entreprise en matière de sécurité du SI et de l'information.

2. Mesures techniques de protection

A. Accès sécurisé au SI

Chaque Utilisateur a la charge de contribuer, à son niveau, à la sécurité du SI.

Des identifiants et des mots de passe uniques sont nécessaires à l'Utilisateur pour accéder au SI. Les mots de passe doivent rester confidentiels. Pour certaines applications, des moyens d'authentification forte (par exemple : carte à puce et code « PIN » associé ou autre système) sont utilisés et sont strictement individuels, personnels et confidentiels. L'Utilisateur doit les mémoriser, ne pas les communiquer à un tiers ni les écrire sur des supports apparents ou facilement accessibles par un tiers.

L'Utilisateur est responsable de l'utilisation du SI effectuée à partir de ce droit d'accès.

Le contrôle de l'accès au SI permet d'identifier toute personne utilisant toute ressource informatique. L'utilisateur ne doit accéder qu'aux composants du SI pour lesquels il a un droit d'accès.

Sauf cas explicite de délégation et dans la limite de ce qui entre dans ses activités professionnelles l'utilisateur ne doit pas tenter d'accéder au compte et aux données d'autrui ni modifier ses messages sans son accord ni s'approprier des droits d'accès par quelque moyen que ce soit.

Pour l'accomplissement de certaines missions, des comptes fonctionnels dédiés peuvent être crées et partagés au sein d'une équipe après accord de l'Administrateur du SI. L'utilisation de ces comptes se fait sous la responsabilité et la supervision du propriétaire désigné pour le compte.

L'accès au SI est temporaire et peut être supprimé lorsque l'Utilisateur ne remplit plus les conditions au titre desquelles son accès lui a été autorisé.

B. Dispositifs automatiques de contrôle, de gestion d'incidents de sécurité, de filtrage et de traçabilité

Pour satisfaire aux obligations notamment légales qui incombent à l'Entreprise, tenant à sa capacité à :

› apporter la preuve, le cas échéant, du bon usage professionnel des systèmes d'information mis à la disposition des utilisateurs
› prévenir tout usage illicite de ces mêmes moyens ou assurer le bon fonctionnement du SI,

Il est procédé, dans le respect de l'information des personnes concernées et de la loi informatique et libertés du 6 janvier 1978 modifiée, à la mise en place d'outils de traçabilité (journaux de connexions) de l'ensemble du système d'information, et d'outils de filtrage (des contenus, des URL, etc.)

Les dispositifs susvisés permettent notamment d'aider l'Entreprise à :

› maitriser les flux d'informations ;
› générer des alertes,
› opérer les investigations nécessaires à la résolution de dysfonctionnements du SI ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité ;
› traiter les dysfonctionnements du système d'information,
› restreindre ou contrôler les accès à tout ou partie d'Internet,
› éliminer des messages électroniques non sollicités et/ou non désirés tels que les spams, virus, phishing, etc
› vérifier et/ou filtrer certains types de contenus souvent à l'origine de dysfonctionnements (encombrement du réseau, « cookies », malware etc.),
› tracer de manière individuelle ou collective les flux entrants et sortants qu'ils soient sécurisés ou non,
› sensibiliser et/ou former les utilisateurs à la protection des informations, à la Sécurité du SI et aux menaces de cybersécurité notamment par des campagnes de sensibilisation et de responsabilisation des Utilisateurs.

Dans le respect des principes de transparence et de proportionnalité, l'attention des Utilisateurs est attirée sur le fait que ces dispositifs :

› génèrent des traces de connexion comprenant les informations suivantes :
› adresse IP, identifiant, sites visités, heures des visites, volume de trafic, éléments téléchargés (leur nature : texte, image, vidéo ou logiciels) s'agissant de la navigation sur Internet ;
› expéditeur, destinataire(s), objet, nature et analyse de la pièce jointe, et éventuellement texte du message s'agissant des messages envoyés et reçus.
› permettent de procéder à des analyses techniques (bande passante, volume de données/Utilisateur, pics de charge, …) et filtrent les accès à Internet.

Afin de ne pas accentuer davantage l'encombrement du réseau, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

Il pourra être procédé à l'analyse des traces de connexions individuelles et au déchiffrement des flux sécurisés HTTPS entrants et sortants depuis les postes de travail des salariés, à l'exception des flux pour lesquels la règlementation ou les besoins de confidentialité l'imposent. (Par exemple, les sites Internet afférents à la Santé/Finance).

Les traces de connexion sont conservées pendant 3 mois. Les données d'alerte extraites des analyses sont également conservées pendant 3 mois.

C. Contrôle de l'utilisation du SI

L'Entreprise se réserve notamment le droit de :

› contrôler l'origine licite et autorisé des logiciels installés ;
› prendre connaissance des messages électroniques professionnels ;
› contrôler l'usage de la Messagerie électronique ;
› surveiller le contenu du SI.

Des contrôles systématiques ou par échantillonnage ou en fonction des éléments indiquant une utilisation anormale peuvent être réalisés par l'Entreprise sur l'ensemble du SI, à n'importe quel moment, et ce, afin de prendre toute mesure pour se prémunir contre une utilisation non conforme pouvant notamment porter préjudice à l'Entreprise.

Les téléphones mis à la disposition des utilisateurs par l'Entreprise peuvent également faire l'objet de contrôles, en cas de consommation anormale ou abusive, ou en vue d'établir des statistiques utiles à l'analyse des besoins des utilisateurs.

3. Maintenance

La mise à disposition des ressources informatiques implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité du système d'information et ne nécessite pas, pour l'utilisateur, de communiquer ses identifiants et mots de passe.

Si, à l'occasion d'opérations de maintenance, une utilisation anormale ou un contenu illicite ou préjudiciable est identifié, l'Entreprise se réserve le droit d'en tirer toutes les conséquences au regard de la situation rencontrée.

L'utilisateur est tenu de maintenir à jour son poste de travail et ne doit pas modifier ou altérer les procédures mises en oeuvre dans l'Entreprise.

VI. PROTECTION DES DONNEES A CARACTERE PERSONNEL

Hall 32 procède à un traitement des données à caractère personnel afin :

› D'assurer la gestion des contrats d'apprentissage et toute action inhérente à ce dernier, au niveau administratif et financier,
› D'assurer un accompagnement spécifique pour les apprentis en situation de handicap ;
› D'accompagner les acteurs (employeurs, maîtres d'apprentissage, apprentis) en proposant notamment des formations,
› De s'assurer du suivi pédagogique de l'apprenti (mise à disposition d'outils pédagogiques à travers une plateforme numérique : APIBOX, Livret Electronique d'Apprentissage, visites en entreprise),
› D'assurer le suivi des aides destinées aux apprentis,
› De réaliser des enquêtes dans un format anonymisé et par des moyens sécurisés afin d'assurer le pilotage, l'évaluation et l'amélioration de nos services et à des fins statistiques,

Sur le fondement de l'article 6. § 1 alinéa c du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

Les personnels autorisés de Hall 32 sont destinataires des Données à Caractère Personnel.

Les informations mentionnées dans l'inscription sont transmises par des moyens sécurisés aux parties prenantes du dispositif apprentissage (Frances Compétences, OPCO, Rectorat, DIRECCTE, Région, Chambres consulaires, ASP, Unités de Formation par Apprentissage), pour la bonne gestion du contrat d'apprentissage et à des fins statistiques au niveau régional et international.

Hall 32 peut être amené à transmettre les Données à Caractère Personnel de la personne concernée sans son accord préalable afin de se conformer à une exigence légale. A ce titre, la personne concernée accepte que Hall 32 puisse transmettre des Données à Caractère Personnel si ces derniers doivent se conformer à une assignation judiciaire, un mandat, jugement ou ordonnance, ou à une autorité

compétente dans le cadre d'une mission d'enquête particulière et notamment pour la défense de leurs droits.

Les Données à Caractère Personnel sont conservées par Hall 32 dans un environnement sécurisé pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Cette durée ne pourra pas excéder dix (10) ans.

Conformément au RGPD et à la loi n°78-du 6 janvier 1978 (loi informatique et libertés), telle que modifiée par la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, la personne dispose d'un droit d'accès et de rectification des données la concernant, ainsi que le droit de définir des directives post-mortem relatives à leur communication. La personne concernée dispose d'un droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

La personne concernée peut exercer ces droits, en s'adressant au référent à la protection des données de Hall32 :

› par courrier à : Hall 32 – Référent à la protection des données – 32 rue du Clos Four – 63100 CLERMONT-FERRAND
› par courriel à : rgpd@Hall 32.fr

Afin de pouvoir traiter les demandes d'exercice de droits, celles-ci doivent être signées et les personnes doivent justifier de leur identité par tout moyen. En cas de doute raisonnable quant à leur identité, HALL 32 peut exiger des informations supplémentaires et nécessaires, y compris, lorsque la situation l'exige, la photocopie d'un titre d'identité portant la signature de la personne concernée.

VII. RESPONSABILITE ET SANCTIONS

L'Entreprise est responsable de :

› la mise à disposition des systèmes d'information,
› la maîtrise technique des systèmes d'information ;
› la protection de l'information et des systèmes d'information

L'Utilisateur est responsable de l'utilisation du SI en conformité avec la Charte.

Toute utilisation non conforme aux lois et règlements ainsi qu'aux conditions et limites définies par cette Charte comme en cas de violation délibérée et répétée est passible de sanction pouvant aller jusqu'au licenciement.

En conséquence, le non-respect des règles figurant dans cette Charte ainsi que des textes et des lois en vigueur expose l'Utilisateur aux sanctions disciplinaires prévues dans le règlement intérieur de l'Entreprise et est susceptible d'engager sa responsabilité pénale et/ou civile.

VIII. ENTREE EN VIGUEUR

En tant que partie du règlement intérieur de l'Entreprise, la Charte a été affichée conformément à l'article R. 1321-1 du Code du travail et a été déposée au secrétariat-greffe du Conseil de Prud'hommes de Clermont-Ferrand.

Elle a été soumise et communiquée à l'Inspecteur du travail.

La présente version de la Charte se substitue à la précédente et s'applique un mois après l'accomplissement des formalités de consultation, dépôt et affichage.

Je soussigné·e …….

Déclare avoir pris connaissance de la charte informatique et m'engage sur l'honneur à la respecter.

Fait à : ……. Le : ……

Signature de l'employé / de l'apprenant·e :

Signature des parents (si mineur·e)