CHARTE INFORMATIQUE VILOGIA LOGIFIM

Charte informatique – Mai 2022

Sommaire

1 Généralités

1.1 Préambule

La présente charte remplace les règles d'usage informatique et multimédia ainsi que les règles d'usage équipements nomades.

1.2 Objet des règles d'usage Informatique, Multimédia et Numérique

La présente charte informe les collaborateurs de Vilogia Logifim, de leurs droits et leurs devoirs pour l'utilisation des outils informatiques et de mobilité au sein de Vilogia Logifim, dénommée ci-dessous « l'entreprise » ou « Vilogia Logifim». Elle a pour ambition d'optimiser l'efficacité opérationnelle de ces outils et d'inciter les collaborateurs à les utiliser dans le cadre de leurs fonctions tout en déterminant les règles et les principes de leur bonne utilisation.

1.3 Nature juridique des règles d'usage Informatique, Multimédia et Numérique

Le texte de ces règles d'usage a été établi selon les dispositions légales applicables en la matière dont la Loi Informatique et Libertés du 6 janvier 1978 modifiée, et le Règlement Général sur la Protection des Données (RGPD) applicable dans les Etats membres de l'Union Européenne depuis le 25 mai 2018.

Les présentes règles d'usage, ont valeur de prescriptions générales et permanentes quant à l'usage de l'outil informatique de l'entreprise.

Ce document sera modifié si l'évolution, le développement des outils informatiques ou l'évolution de la législation et de la jurisprudence dans ce domaine le justifient.

1.4 Modalités d'application

L'accès aux outils de l'entreprise ne peut se faire qu'après acceptation par l'utilisateur des modalités de la charte informatique.

Cette dernière est remise à tout nouveau collaborateur (salarié, stagiaire, apprenti, prestataire informatique… etc.) lors de son arrivée dans l'entreprise, et est disponible dans l'Intranet (rubrique "Ressources Humaines").

Cette acceptation se fait à l'occasion de la signature du contrat de travail, de la convention de stage, ou du contrat de prestation, lors de l'arrivée de tout nouveau collaborateur.

Pour l'ensemble des collaborateurs de l'entreprise, la présente charte sera consultable, téléchargeable et imprimable depuis l'Intranet.

1.5 Ressources du SI

Le système d'information et de communication de l'Entreprise est constitué d'éléments matériels et logiciels. Il s'agit notamment d'ordinateurs (fixes ou portables), de périphériques, du réseau informatique (serveurs, routeurs et connectique), de photocopieurs, de téléphones, de smartphones, de tablettes, de logiciels, de fichiers, de données, de bases de données, de messageries, d'intranet, d'extranet, de sites Internet.

Les Ressources du SI sont soumises à des natures de droits différents (propriété, licence, location, abonnement, droit d'utilisation). Ces différences de nature ne font pas obstacle à l'application de la présente Charte.

1.6 Politique de Sécurité de Système d'information (PSSI)

Cette charte s'inscrit dans le cadre de **la Politique de Sécurité du Système d'Information (PSSI)** qui définit la **stratégie de sécurité informatique** de l'entreprise. La PSSI décrit l'ensemble des **enjeux, des besoins, des contraintes, ainsi que des règles à adopter** propres à chaque structure. La PSSI est disponible en ligne sur l'intranet.

Certains articles de cette charte contribuent à la PSSI et sont identifiés par un code d'identification spécifique PSSI-*XXX-99*

2

Règles d'utilisation du système d'information

2.1 Les règles de sécurité - PSSI-ACC-16

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique, et de manière générale tout dysfonctionnement ;
- Ne jamais confier son identifiant/mot de passe à un tiers ;
- Ne pas installer, copier, modifier, détruire des logiciels propriétés de la société sans autorisation ;
- Verrouiller son ordinateur dès que l'on quitte son poste de travail ;
- Ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est douteux ;
- Ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir le responsable des systèmes d'information ;
- Ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage ;
- Ne pas utiliser (même avec leur accord) ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ;
- Ne pas masquer son identité informatique ;
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe doit respecter les règles définies par l'entreprise tel que défini à l'article « 5 - Partage de données » ;
- 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 des ressources du système d'information qu'il pourrait être amené à accéder, manipuler ou échanger. En particulier, il est déconseillé d'utiliser les systèmes de connexion wifi dans les lieux publics et d'utiliser des moyens d'obfuscation dans les transports lorsque des données d'entreprise sont manipulées

Les salariés et les contractants sont régulièrement sensibilisés à ces mesures de sécurité et aux procédures organisationnelles relatives à la sécurité du SI dans l'exercice de leur métier.

2.2 L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte (« login » ou identifiant) fourni à l'utilisateur lors de son arrivée à l'entreprise. Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont personnels et confidentiels. Lorsque l'on quitte momentanément son poste de travail, il est fortement recommandé de verrouiller son ordinateur.

La complexité du mot de passe est à aligner aux recommandations de la CNIL et pourra évoluer selon le niveau de sécurité jugé nécessaire par l'entreprise.

Actuellement, le mot de passe doit être composé de 8 caractères minimum combinant chiffres, lettres majuscules, lettres minuscules et caractères spéciaux (3 des 4 composants). Il ne doit comporter ni le nom, prénom, ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement.

L'accès distant au système d'information de l'entreprise est uniquement attribué aux utilisateurs authentifiés. Un mécanisme d'authentification à deux facteurs est mis en place selon le niveau de sécurité requis.

2.3 Gestion des droits

L'Utilisateur est tenu au respect de la confidentialité des informations sensibles.

Le détenteur d'un document est garant de sa confidentialité, et doit à ce titre le placer dans le répertoire approprié et contrôler sa diffusion. En cas de doute, signaler par écrit au service responsable de la sécurité informatique toute violation ou tentative de violation suspectée de son compte ou tout dysfonctionnement quant à la sécurité.

Chaque Utilisateur règle avec soin les droits d'accès vers les documents qu'il partage, ou qui sont partagés avec lui. A l'inverse, dans le cas où l'Utilisateur se rendrait compte qu'un document sensible aurait des droits anormalement faibles, il en avertira l'auteur et les gestionnaires de ce document afin que le problème soit traité.

Cette règle s'applique également aux courriers électroniques ("email"), messagerie instantanée ("Tchat"), forum, réseau social ou toute autre forme de communication électronique ou non.

De plus, l'Utilisateur s'engage à informer le service en charge des droits et supprimer les informations qui lui auraient été acheminées par erreur et en avertir l'émetteur.

2.4 Protection logiciel & Droits d'auteurs

L'Utilisateur s'interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit. Les copies de sauvegarde, dans les conditions prévues par le code de la propriété intellectuelle, ne peuvent être effectuées que par les personnes habilitées.

Les courriers, documents, œuvres collectives, logiciels, ou toutes autres productions réalisées dans le cadre de la mission du Collaborateur sont la propriété de L'entreprise. Ce dernier ne peut donc pas les céder ou les revendre. De même, il ne peut les récupérer à l'issue de sa collaboration sauf accord écrit de l'entreprise.

Chaque Utilisateur doit détenir les droits d'usage des œuvres artistiques, fichiers numériques et logiciels qu'il introduit sur le lieu de travail.

Plus généralement, l'Utilisateur doit respecter toutes les lois en vigueur (notamment concernant les données à caractère personnel, le droit d'auteur, le droit à l'image, l'ordre public, la diffamation, l'incitation à la haine raciale, la corruption, les bonnes mœurs, etc.) et l'Utilisateur reste pleinement responsable de ses actes.

2.5 Devoir général d'alerte

L'Utilisateur doit alerter les équipes responsables des systèmes informatiques et de communication en cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité des ressources du SI.

Pour illustrer ces situations, dont la diversité suppose de la part de l'Utilisateur attention et discernement, on citera pour exemple (non-exhaustif) :

- Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données,
- L'existence d'informations confidentielles sur des répertoires partagés non appropriés entraînant la diffusion de ces informations à des tiers non habilités,
- L'existence de contenus de caractère offensant contraire aux bonnes mœurs ou à l'éthique de l'Entreprise,
- La présence de personnes non autorisées dans des zones de travail entraînant des risques de perte de confidentialité de documents ou d'informations accessibles dans ces zones,
- Les documents « abandonnés » contenant des informations confidentielles,
- L'activation d'alarmes d'intrusion du bâtiment démontrant un accès non autorisé
- La constatation d'un dégât (eau, électricité, ...) affectant une ressource du SI
- La violation de la sécurité des données,
- La détection d'une action de vandalisme sur le système d'information et de communication.

2.6 Les règles d'usages

Les outils informatiques et numériques mis à la disposition des collaborateurs sont des outils professionnels.

Si l'usage de ces outils à titre privé par les collaborateurs de l'entreprise est admis, il s'agit d'une tolérance, subordonnée à un usage occasionnel et ponctuel, de manière raisonnable et limitée, dans le cadre des nécessités de la vie courante et familiale et dans tous les cas, non contraire à la loi, aux bonnes mœurs ou à l'ordre public.

Les collaborateurs sont tenus d'une exécution de bonne foi de leur contrat de travail et au respect des prescriptions et directives figurant dans la présente charte.

Toutefois, en cas d'abus manifestes, des mesures de contrôle pourront être mises en place de manière proportionnelle :

- à la préservation de l'intérêt légitime de l'entreprise ; et
- au respect de la vie privée des collaborateurs.

Les modalités pratiques des contrôles, pouvant être effectuées par l'entreprise, sont définies au chapitre 10.

La présente charte étant une annexe au Règlement Intérieur, un collaborateur ayant enfreint les principes et les règles d'utilisation de l'outil informatique tels que définis peut encourir une procédure disciplinaire de la part de l'entreprise et s'expose en conséquence à d'éventuelles sanctions.

2.6.1 Usage professionnel de matériels personnels (tolérances)

L'emploi d'équipements personnels (ou provenant d'autres entreprises) est autorisé dans les limites suivantes :

- Il est interdit de raccorder un matériel non fourni par l'entreprise sur une prise réseau de l'entreprise sauf accord du Service Informatique et du Responsable de la Sécurité Informatique. Dans le cas contraire, l'auteur des dommages provoqués, comprenant la perte de productivité de l'entreprise et de chiffre d'affaires induit, pourra faire l'objet de poursuites.

C'est pourquoi une connexion isolée et restreinte à un simple accès Internet est possible après demande à l'informatique et fourniture d'informations d'identification. L'utilisation de cet accès gratuit engage l'Utilisateur, c'est pourquoi il n'est pas anonyme et peut être tracé afin de répondre aux exigences légales.

- Si certains services (comme la messagerie) sont accessibles avec un matériel personnel, l'ensemble des services ne sont pas nécessairement accessibles sans un matériel fourni par l'entreprise ou même à distance. Il appartient à l'utilisateur de s'informer auprès du Service Informatique afin de s'organiser.
- Il appartient à l'Utilisateur lui-même de veiller à la sécurité de son propre matériel. Dans le cas où l'Utilisateur choisirait librement d'utiliser un équipement personnel pour un usage professionnel, il est exigé de se conformer à l'annexe 1 : Bonnes pratiques de sécurité d'un matériel personnel.

2.7 Départ d'un collaborateur de l'entreprise - PSSI-RH-04

En cas de départ d'un collaborateur, toutes les informations présentes sur le Système d'information de l'Entreprise sont qualifiées de professionnelles et appartiennent à l'Entreprise au jour du départ.
Le salarié doit purger ses mails « personnels » ou « privés » avant de quitter l'entreprise.

Lors du départ d'un collaborateur, le responsable de l'administration du système doit être averti afin que ses accès soient révoqués.

Toutes les données non purgées par le collaborateur (mail, documents, …) seront supprimées après 1 mois sauf demande de conservation ou de transfert dans le cadre de l'activité de l'entreprise.

2.8 Espace de travail « propre » - PSSI-PHYS-07

2.8.1 Principe

Des documents ou des données sensibles (éventuellement à caractère personnel) sont susceptibles d'être divulgués intentionnellement ou non à des parties non autorisées lorsqu'ils sont exposés (non classés) ou portés disparus. Un espace de travail « propre » contribue à protéger les données de l'entreprise contre tout accès non autorisé, notamment à une personne non autorisée susceptible d'accéder aux locaux de l'entreprise.

2.8.2. Portée

Ce principe s'applique à tous les employés, sous-traitants, travailleurs temporaires et tout autre personnel pouvant travailler pour le compte de l'entreprise ou dans les locaux de l'entreprise.

2.8.3. Détail

- Toutes les informations sensibles, confidentielles ou personnelles sous forme papier ou électronique doivent être sécurisées à la fin de la journée de travail ou à tout moment lorsqu'elles ne sont pas utilisées activement.
- Les clés des classeurs ou autres espaces de stockage sécurisés ne doivent pas être laissées sur les bureaux ou dans d'autres zones non sécurisées.
- Les sessions utilisateur doivent être verrouillées à tout moment lorsque les ordinateurs ne sont pas utilisés activement.
- Les ordinateurs doivent être éteints à la fin de la journée de travail.
- Les équipements nomades doivent être enfermés dans des tiroirs sécurisés ou doivent être sécurisés avec un câble de verrouillage.
- Les documents imprimés doivent être retirés du bac de l'imprimante sans retard excessif et ne pas être laissés autour de la zone d'impression.
- Lorsqu'ils ne sont plus nécessaires, les documents contenant des informations confidentielles, sensibles ou personnelles doivent être déchiquetés en priorité dans un broyeur ou insérés dans des bacs d'élimination confidentiels.
- Les tableaux blancs doivent être effacés après les réunions ou lorsqu'ils ne sont plus utilisés.

Les moyens informatiques

3.1 Configuration du poste de travail

L'entreprise met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Nuire au fonctionnement des outils informatiques et de communications.

3.2 Règles d'usage des équipements nomades

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, smartphones, clé USB, etc…)

Autant que possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker. L'utilisateur est invité à se rapprocher du service informatique pour s'informer des moyens d'échanges sécurisés à sa disposition

Le collaborateur s'engage à ne pas consulter des sites aux contenus illicites. Le collaborateur s'engage à respecter scrupuleusement les dispositions du *contrat téléphonie* en ligne sur l'intranet.

3.2.1 Accès distant (télétravail, déplacement, bureau à distance, ...) - PSSI-ORG-09

L'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d'information et de communication à distance.

3.2.2 Le téléphone mobile professionnel

L'attribution d'un téléphone mobile ou smartphone est soumise à l'accord du Directeur des Ressources Humaines au regard de la politique d'attribution en cours. Ce téléphone est réservé à un usage professionnel.

Une utilisation engendrant des frais pour l'entreprise est strictement interdite. Le collaborateur s'engage à ne s'abonner à aucun service payant, ni à effectuer des achats dont les frais seraient imputables à l'entreprise (ex : achats multimédias, services vocaux… etc.).

3.2.3 Ordinateur portable / Tablette

L'attribution d'un ordinateur portable ou d'une tablette est soumise à l'accord du Directeur du Service. Le budget imputé est alors celui du service concerné. L'ordinateur portable ou la tablette peuvent être nominatifs ou dédiés à un service. Cet équipement est réservé à un usage professionnel.

De manière générale le bénéficiaire s'engage à :

- Ne pas exposer l'ordinateur ou la tablette à toute source de chaleur ;
- Ne pas mettre l'ordinateur ou la tablette en contact avec toute sorte de liquide ou l'exposer à une humidité ;
- Ne pas endommager le câble ou la prise d'alimentation électrique de l'appareil ;
- Préserver l'ordinateur ou la tablette de tout choc ;
- Ne placer aucun objet sur le clavier de l'ordinateur ouvert ;
- Ne placer aucun objet sur l'ordinateur, même fermé ;
- Ne jamais tenter de réparer l'ordinateur en cas de problème ou d'accéder aux composants internes de l'appareil ;
- Débrancher l'ordinateur en cas d'orage afin de prévenir une éventuelle surcharge électrique risquant d'endommager le matériel ;
- Ne jamais vaporiser directement sur l'appareil de produit d'entretien ;
- Ne pas utiliser d'alcools, d'aérosols ni de produits solvants ou abrasifs susceptibles d'endommager le matériel ;
- Ne pas installer à demeure des programmes ou copies de programmes non fournis par l'entreprise

3.2.4 Accès VPN & TSE

Les accès au réseau de l'entreprise depuis l'extérieur doivent se faire uniquement à travers un tunnel VPN sécurisé.

Le collaborateur qui dispose d'un accès VPN et/ou TSE, s'engage sur une utilisation strictement professionnelle, et doit se conformer aux présentes règles d'usage des équipements nomades.

3.2.5 Responsabilités

Le bénéficiaire est seul responsable de l'utilisation et de la conservation de son matériel. Le matériel doit être conservé en permanence dans un endroit sécurisé et ne jamais être laissé sans surveillance. En cas de casse, perte, vol liés au non-respect de ces consignes, un téléphone d'ancienne génération sera mis à la disposition du collaborateur. Tout détenteur d'un téléphone mobile professionnel doit faire apparaitre son numéro sur ses cartes de visite, et en cas de déplacements professionnels, faire basculer sa ligne fixe vers sa ligne mobile. Il est rappelé que conduire avec un téléphone à la main ou en portant à l'oreille un dispositif audio de type écouteurs, oreillette ou casque est interdit et passible d'une amende et d'un retrait de points du permis de conduire. Seul un dispositif intégré au véhicule est autorisé.

3.2.6 Assistance /Vol / Perte - PSSI-ORG-11

- ✓ Contacter le 5678 pour prise en charge de la désactivation des comptes.
- ✓ Déposer une plainte au commissariat (vol) et la transmettre au service juridique.
- ✓ Contacter votre manager ou l'assistante de votre service

3.2.7 Casse / Dysfonctionnement

Les équipements sont généralement garantis de 1 à 3 ans. En cas de dysfonctionnement, il est nécessaire de contacter le 5678 pour effectuer un premier diagnostic. En fonction du problème, le matériel devra être remis au service informatique pour réparation par le constructeur (si encore garantie). Hors garantie un diagnostic sera établi, une estimation du coût de réparation sera alors soumise au collaborateur, et pour avis au Directeur de Service.

3.2.8 Restitution

L'appareil est à restituer par le bénéficiaire sur simple demande de l'entreprise.
Exemples : lors d'une fin de mission, ou lorsque le poste ne justifie plus l'utilisation d'un téléphone ou d'un PC Portable. Il est à restituer au manager ou l'assistante du service avec tous les accessoires fournis initialement.

3.2.9 Contrôles

L'entreprise contrôle régulièrement les consommations des téléphones et se réserve le droit de demander des explications au bénéficiaire en cas de consommation anormale et générant une dépense non prévue dans le contrat. Un rapport d'utilisation de l'appareil peut être transmis au collaborateur sur simple demande par son manager.

3.2.10 Propriétés

L'entreprise est le seul propriétaire du téléphone, et se réserve ainsi le droit de le récupérer à tout moment sans préavis ni indemnité. Le numéro de téléphone lié au matériel est professionnel et ne pourra à aucun moment être revendiqué par le salarié, y compris en cas de changement d'activité, de portefeuille ou de secteur.

Messagerie électronique Outlook et Office 365

4.1 Accès

Chaque collaborateur dispose d'un accès à la messagerie électronique de l'entreprise. Le service informatique gère la création de tout nouveau « profil utilisateur ».

Les collaborateurs et/ou responsables hiérarchiques ayant accès aux messageries de collaborateurs absents devront impérativement respecter les dispositions du paragraphe " 4.3.2 Mention « personnel » ou « privé » de la présente charte informatique.

4.2 Utilisation professionnelle

4.2.1 Cadre général

Outlook et Office 365 sont des systèmes de messageries électroniques mis à la disposition des collaborateurs par l'entreprise : ils doivent être utilisés principalement et prioritairement à des fins professionnelles à l'intérieur de l'entreprise ou vers des destinataires extérieurs.

Au même titre que le courrier postal ou les communications téléphoniques, les messageries Outlook et Offices 365 répondent à des exigences de confidentialité et de responsabilité pour la rédaction des mails, leur diffusion, l'insertion de fichiers joints et d'accusés de réception, l'archivage.

Les collaborateurs de l'entreprise qui reçoivent des mails à caractère professionnel ne peuvent opposer le secret des correspondances à leur employeur.

4.2.2 Modalités

4.2.2.1 Bonnes mœurs - usages

Il est strictement interdit d'utiliser, à quelque moment que ce soit, les messageries Outlook et Office 365 pour l'envoi et/ou la réception à l'intérieur et/ou à l'extérieur de l'entreprise, de courriels, accompagnés ou non de pièces jointes, ayant un caractère pornographique, pédophile, révisionniste, prosélytiste en ayant pour objet de faire adhérer des personnes à des idées politiques, religieuses, sectaires etc.... ou ayant pour objet d'inciter à la haine raciale... etc.

L'envoi de messages illicites et contraires à l'ordre public ou aux bonnes mœurs dont la divulgation peut altérer l'image de marque de l'entreprise, est interdit.

De plus, le détournement à cet effet de la finalité professionnelle des messageries Outlook et Office 365 ne peuvent qu'être contraire à la productivité et au professionnalisme des collaborateurs mais aussi à la performance matérielle, en volume et en rapidité, de l'outil de communication multimédia en tant que tel.

À ce titre, il est dès lors aussi interdit d'utiliser les messageries Outlook et Office 365 pour l'envoi et/ou la réception de films, d'enregistrements musicaux, de jeux, d'images, de photos... etc. ayant un caractère humoristique ou non et de quelque nature que ce soit, à l'exception d'une utilisation strictement professionnelle.

4.2.2.2 Usages des fichiers volumineux

Certains fichiers volumineux encombrent le réseau lors de leur diffusion.

Les collaborateurs de l'entreprise ne peuvent pas adresser ou recevoir de fichiers et/ou pièces jointes représentant 50Mo ou plus en un seul envoi.

Les fichiers les plus volumineux à usage interne doivent être stockés et/ou partagés sur le SharePoint ou One Drive.

4.2.2.3 Usage de la Copie

Les utilisateurs sont responsables du choix des destinataires de leurs mails :

- L'option « cc » (copie carbone). Cette option suppose que le mail est envoyé pour information : il ne suscite pas forcément de réponse du destinataire. Cette option doit être utilisée pour des destinataires ciblés et privilégiés. Dans un souci de performance du réseau, l'envoi systématique de mails en copie doit être évité ;
- L'option « ccc » (copie carbone cachée). Dans un souci de transparence de la communication interne à l'entreprise les collaborateurs ne peuvent se servir de cette option, sauf en cas de nécessité professionnelle impérative et justifiée.

4.2.2.4 Carnets d'adresses et listes de diffusion

a. Les messageries Outlook et Office 365 fournissent aux utilisateurs un carnet d'adresses personnel : il est demandé de ne pas y recopier les adresses mails et les listes de diffusion du carnet d'adresses de l'entreprise. Le carnet d'adresses de l'entreprise est géré par la Direction des Ressources Humaines : inscriptions, radiations, mise à jour des listes de diffusion.

b. L'envoi de messages à la liste de diffusion VILOGIA GROUPE (l'ensemble des collaborateurs du Groupe) est réservé aux seuls membres du Comité de Direction (ou aux personnes déléguées par celui-ci).

c. Il est strictement interdit d'utiliser la liste de diffusion VILOGIA GROUPE et de façon générale les messageries Outlook et office 365 pour l'envoie de « chaînes de solidarité », des publicités à caractère commercial, des avis de recherche, des collectes d'argent, des petites annonces... etc.

4.2.2.5 Actions contre les spams

a. Afin de lutter contre les spams (envoi massif de mails non-sollicités, pouvant détériorer le réseau informatique de l'entreprise), un système de régulation, a été mis en place. Il filtre tous les messages tout en offrant la possibilité de récupérer les messages filtrés.

b. Les adresses professionnelles des collaborateurs de l'entreprise ne doivent être transmises qu'aux interlocuteurs professionnels dans le cadre de leurs missions.

La communication de cette adresse professionnelle par les collaborateurs est uniquement tolérée dans un cadre restreint, familial ou amical.

En aucun cas, cette adresse professionnelle ne doit être communiquée à des organismes, sociétés, entreprises tierces dont la connaissance d'adresses emails puisse favoriser l'envoi de SPAM : particulièrement pour les sites Internet développant des thèmes ou des activités illégales ou contraires aux bonnes mœurs et à l'ordre public ainsi que pour les sites Internet hébergés hors de France.

Dans un souci d'amélioration continue du dispositif de lutte contre les spams, les collaborateurs sont invités à déclarer comme spams tous les emails reçus et qu'ils jugent indésirables.

4.2.2.6 Nettoyages des boîtes emails

Les collaborateurs de l'entreprise sont responsables de la gestion de leur(s) messagerie(s).

Ils s'engagent à lire régulièrement les emails reçus, à y répondre si nécessaire, à les archiver en cas de besoin et à supprimer les messages « périmés ».

Le pôle informatique a mis en œuvre un archivage automatique des emails de plus de six mois pour les collaborateurs de l'entreprise. Les emails sont alors disponibles dans une boite « Archive » personnalisée pour chaque collaborateur.

Des quotas de stockage sont mis en œuvre sur les boites emails de tous les collaborateurs. Ces quotas dépendent de leur licence Office 365.

Il y a une alerte de capacité lorsque les boites email arrivent à un certain seuil.

4.2.2.7 Contaminations extérieures

Certains fichiers joints en provenance de l'extérieur de l'entreprise sont conçus avec des logiciels incompatibles avec ceux de l'entreprise : les utilisateurs doivent vérifier au préalable la compatibilité de leur lecture avant d'ouvrir ces fichiers.

Certains fichiers expédiés par des tiers extérieurs à l'entreprise peuvent contenir des virus. Pour éviter une « contamination » de l'ensemble du réseau, dans le cas où un message suspect est repéré :

- Le service informatique doit immédiatement être prévenu,
- Le collaborateur ne doit surtout pas y répondre et/ou cliquer sur les liens et pièces jointes contenus dans ce mail douteux.

4.2.2.8 Mail de synthèse (Viva Insights)

Viva Insights prend en charge le Règlement Général sur la Protection des Données (RGPD).

Ainsi :

- En tant qu'utilisateur Viva Insights, vous seul pouvez voir vos propres données.
- Vos données sont stockées et calculées dans votre boîte aux lettres Exchange Online.
- Vous pouvez accepter et refuser à tout moment.
- Viva Insights ne vous montre aucune information d'identification personnelle des collègues au-delà de ce que vous pouvez déjà afficher dans Outlook et Teams.

4.2.2.9 Sensibilisation aux nouvelles menaces

- Le Phishing ou Hameçonnage en Français :

L'hameçonnage reste l'un des principaux vecteurs de la cybercriminalité. Ce type d'attaque vise à obtenir du destinataire d'un email d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers ou administratifs, afin de lui dérober de l'argent.

L'hameçonnage peut également être utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il peut avoir accès. L'objectif est souvent de dérober les identifiants et de s'en servir pour obtenir des renseignements dans les messageries qui auront pour but de réaliser des emails aux services RH ou Comptabilité afin de dérober de l'argent ou de voler des données pouvant être revendues par la suite sur internet (secrets de fabrication, données stratégiques, etc…)

Il est recommandé aux collaborateurs de faire preuve de la plus grande vigilance lorsqu'ils reçoivent des emails, de vérifier la légitimité des demandes formulées dans les échanges, de ne pas cliquer sur des liens dans les emails mais de se connecter aux sites au moyen de leur navigateur, de ne pas ouvrir de pièces jointes sans en mesurer l'impact potentiel au préalable et de signaler tout comportement suspicieux au service informatique ou au RSSI.

- Le Ransomware ou Rançongiciel en Français :

Le Ransomware est une technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant, souvent par email via une campagne de phishing, et qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

La recrudescence de ce type d'attaques et le fait qu'elles constituent aujourd'hui le plus grand risque pour les systèmes d'information des entreprises doit être pris en compte dans l'usage réalisé par les employés des moyens informatiques que leur fournit l'entreprise.

Il est recommandé aux collaborateurs de faire preuve de la plus grande vigilance lorsqu'ils reçoivent des emails accompagnés de pièces jointes, de vérifier la légitimité des demandes formulées dans les échanges, de ne pas cliquer sur des liens dans les emails mais de se connecter aux sites au moyen de leur navigateur, de ne pas ouvrir de pièces jointes sans en mesurer l'impact potentiel au préalable et de signaler tout comportement suspicieux au service informatique ou au RSSI tout en ayant déconnecté, si possible le matériel du réseau d'entreprise.

4.3 Utilisation personnelle

4.3.1 Bon usage

a. Il incombe aux collaborateurs de l'entreprise de ne pas faire un usage abusif des moyens informatiques mis à leur disposition par l'entreprise.
b. S'il est toléré que les collaborateurs utilisent la messagerie électronique de l'entreprise à des fins personnelles, il ne peut toutefois s'agir que d'une utilisation ponctuelle, occasionnelle, raisonnable et limitée dans le seul cadre des nécessités de la vie courante et familiale.
c. En conséquence, les dispositions de l'article « 4.2.2.1 bonnes mœurs – usages » sont aussi applicables même en dehors des heures de travail.
d. L'utilisation à des fins personnelles de Outlook et Office 365 ne doit en outre n'avoir en aucun cas d'impact significatif :
    - Sur l'exécution et la durée du travail,
    - Sur la qualité professionnelle et la productivité du collaborateur,
    - Sur la sécurité du réseau de l'entreprise et le trafic normal des messages professionnels,
    - Sur le coût d'exploitation du réseau de l'entreprise.

4.3.2 Mention « personnel » ou « privé »

a. En l'absence de toute indication permettant d'identifier sans ambiguïté le caractère privé d'un courriel, d'un document ou d'un répertoire déterminé, ces éléments sont présumés revêtir un caractère professionnel et en conséquence l'entreprise peut avoir accès à ceux-ci.
b. Afin de permettre l'application de ce principe tant dans l'intérêt de la préservation de la vie privée des collaborateurs que dans l'intérêt légitime de la bonne organisation des services de l'entreprise, les collaborateurs ont ainsi l'obligation de distinguer et de faire clairement apparaître dans leur boîte aux lettres électronique, la nature de leurs messages « personnels » ou « privés » et fichiers rattachés, notamment au moyen d'une mention spécifique « privé » ou « personnel ».
c. Toutefois, les collaborateurs ont l'obligation de ne pas stocker dans leur(s) boite(s) aux lettres électronique des fichiers volumineux, susceptibles de saturer la mémoire des messageries Outlook et Office 365 (par exemple, des fichiers vidéo ou des fichiers sons), et ce, quelle qu'en soit la nature professionnelle ou personnelle de ces fichiers.

Partage de données

5.1 Accès

L'entreprise fournit aux collaborateurs des moyens d'accès à des données partagées, ces moyens sont limités grâce à une gestion fine des Identités des collaborateurs et/ou partenaires, des accès pouvant leur être attribués du fait de leurs fonctions ou leur position dans l'entreprise. Il est OBLIGATOIRE de bien faire attention aux droits d'accès mis en place lors de partages de documents, et de faire part d'éventuelles erreurs aux gestionnaires des documents afin que les problèmes soient traités sans délai.

5.2 Interdictions et Obligations au regard des données et de leur partage - PSSI-ASSET-03 & PSSI-RSX-8

Il est interdit :

- De céder ou vendre des documents, courriers, ou fichiers de toute nature, réalisés dans le cadre de sa mission. Il faut un accord écrit de l'entreprise pour les récupérer à la fin de collaboration.
- D'introduire des fichiers de toute nature sans en avoir les droits d'usage.
- De violer la confidentialité des informations.
- De conserver des Ressources informatiques après la fin de sa mission ou un accès vers ces Ressources.
- De céder ces accès aux Ressources Informatiques à une autre personne.
- De contourner les mesures de sécurité
- De raccorder un équipement personnel ou venant d'une autre entreprise sur une prise réseau de l'entreprise sauf accord écrit du RSSI au Service Informatique. Il est possible sur demande d'obtenir un accès restreint à Internet via le hotspot wifi ou certaines prises réseau spécifiques.
- De constituer des fichiers de données à caractère personnel (contenant des informations permettant d'identifier une personne comme nom, prénom, dates de naissance, mail, téléphone, photo, numéro de sécurité sociale) sans en référer à son supérieur hiérarchique, au Délégué à la Protection des Données (DPO) ainsi qu'aux services juridiques et informatiques.
- De communiquer les identifiants et moyens d'authentification de l'entreprise sur les forums, les réseaux sociaux ou assimilables autres que ceux validés (plateforme d'échange sécurisé)

Il est obligatoire :

- De bien faire attention aux droits d'accès mis en place lors de partages de documents, et de faire part d'éventuelles erreurs aux gestionnaires des documents afin que les problèmes soient traités sans délai.

- De bien faire attention aux destinataires des mails rédigés, en particulier si ce dernier contient des informations à caractère confidentiel ou personnel. Les échanges de données confidentiels peuvent être réalisés de manière chiffrée ou via un logiciel d'échange sécurisé (ex : Shadline).
- De repérer les informations et fichiers non professionnels par le mot "PRIVE". Ces informations ne doivent pas être stockées sur des serveurs de l'entreprise : Par conséquent, utiliser le stockage local de l'ordinateur, téléphone ou tablette, ou stockage sur internet.
- De stocker les données professionnelles dans des espaces sauvegardés automatiquement par l'entreprise (comme les lecteurs réseaux).
- De signaler par écrit au service responsable de la sécurité informatique toute violation ou tentative de violation suspectée de son compte ou tout dysfonctionnement quant à la sécurité.

6

L'intranet

L'Intranet est un site Internet interne, mis à la disposition des collaborateurs par l'entreprise.

6.1 Actualisation et diffusion des informations

La Direction Communication et Relations Clients administre l'Intranet : il collecte, hiérarchise, fait valider, met en forme et diffuse les informations.

6.2 Confidentialité

a. L'Intranet est un outil de communication interne. La majeure partie des informations qu'il contient ne peut être communiquée à l'extérieur de l'entreprise : photos, textes, illustrations, animations graphiques, lignes directes téléphoniques des collaborateurs... etc.

   En cas de doute et pour toute diffusion à l'extérieur de l'entreprise de ces informations publiées dans l'Intranet, les demandes doivent être faites à la Direction Communication et Relations Clients.

b. L'Intranet propose toutefois, un certain nombre de documents qui peuvent être téléchargés et diffusés (par mail ou par courrier) à l'extérieur de l'entreprise : plaquettes institutionnelles ou commerciales, destinées aux clients, aux prospects et aux partenaires de l'entreprise.

7

Le site Internet de l'entreprise

7.1 Généralités

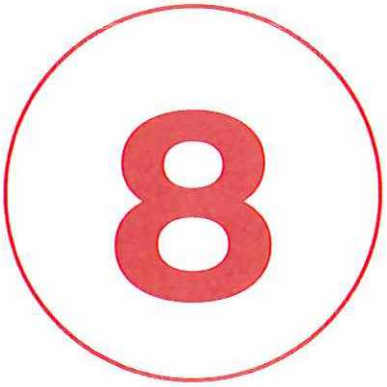
Les sites Internet de l'entreprise sont administrés par la Direction Communication et Relations Clients. La Direction Communication et Relations Clients et le service Juridique sont responsables des déclarations de fichiers liées aux sites.

Les textes, images, photos, animations graphiques sont la propriété de l'entreprise.

7.2 www. « Entreprise ».fr

Ce site Internet, à destination du grand public, des partenaires et de la presse présente l'entreprise et ses différentes activités. Il permet d'accéder à tout le patrimoine locatif des sociétés de l'entreprise (rubrique LOUER/Notre parc), aux programmes disponibles, à l'accession à la propriété (rubrique ACHETER/Nos logements à vendre dans le neuf et dans l'ancien), aux produits et services de l'entreprise.

Les collaborateurs de l'entreprise qui reçoivent en provenance de ce site Internet des emails dans le cadre de leur mission (gestion locative, recrutement, communication), sont tenus de les traiter au même titre que toute autre sollicitation. De même les réclamations de clients-locataires émises via l'Espace Locataire du site Internet, doivent être traitées selon les procédures en cours.



L'accès à Internet

8.1 Utilisation professionnelle

8.1.1 Utilisation principalement et prioritairement à caractère professionnel

L'entreprise met à la disposition des collaborateurs un accès libre à Internet.

Afin de permettre aux collaborateurs de bénéficier des sources d'informations multiples et disponibles sur Internet, cet accès doit principalement et prioritairement avoir un caractère professionnel.

8.1.2 Bonnes mœurs - usages

Il est interdit de se connecter, à quelque moment que ce soit, sur des sites Internet à caractère pornographique, pédophile, révisionniste, prosélyte en ayant pour objet de faire adhérer des personnes à des idées politiques, religieuses, sectaires… etc. ou ayant pour objet d'inciter à la haine raciale... etc.

De manière générale, sont proscrites toutes connexions à des sites Internet illicites contraires à l'ordre public ou aux bonnes mœurs dont les connexions, mêmes occasionnelles, ne peuvent qu'altérer l'image de marque de l'entreprise.

De plus, le détournement de l'usage professionnel de l'outil informatique de l'entreprise pour visiter ces différents sites proscrits pendant le temps de travail ne peut qu'être contraire à la productivité et au professionnalisme des collaborateurs.

À ce titre et pour les mêmes motifs, il est aussi interdit :

- De naviguer sur des sites de jeux (loteries, casinos, etc…),
- De télécharger des programmes de films, de vidéos, de saynètes… etc. humoristiques ou non et de quelque nature que ce soit,
- De connecter des périphériques externes (tels que clés USB, disques durs externes… etc.) dont la provenance n'est pas connue du collaborateur,
- D'installer des fichiers ou logiciels non fournis par l'entreprise sauf accord préalable et expresse du pôle informatique
- De créer des sites internet sans l'autorisation expresse de la Direction Communication et Relations Clients

- D'utiliser l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives.

8.1.3 Interventions sur les forums, groupes de discussions, réseaux sociaux... etc - PSSI-RSX-7 & PSSI-RSX-9 & PSSI-RSX-10

Les collaborateurs de l'entreprise amenés à s'exprimer professionnellement sur internet, (notamment sur des sites spécialisés, des forums, des groupes de discussion ou les réseaux sociaux) par l'intermédiaire de l'accès libre fourni par l'entreprise s'engagent à tenir des propos ou communiquer des informations sérieuses et conformes à la réalité et ce, dans le seul cadre de leurs compétences techniques.

Les propos tenus doivent être mesurés et appropriés au contenu professionnel de l'échange.

Seules les informations publiques peuvent être communiquées sur les forums, réseaux sociaux ou assimilables. Il est strictement interdit de publier des informations réservées à l'usage interne ou confidentielles.

Le dénigrement de l'entreprise ou de ses filiales ou la publication de fausses allégations sont susceptibles de faire l'objet de sanctions.

Dans tous les cas, les collaborateurs de l'entreprise doivent respecter les règles de discrétion et de secret professionnel liées à l'exercice de leurs missions.

8.1.4 Copyright

Les collaborateurs de l'entreprise amenés à copier des documents sur des sites Internet (photos, textes, illustrations) doivent veiller au respect de la législation sur le copyright. Si nécessaire, il est conseillé de consulter au préalable le service Juridique ou la Direction Communication et Relations Clients.

8.2 Utilisation personnelle

8.2.1 Bon usage

a. Il incombe aux collaborateurs de l'entreprise de ne pas faire un usage abusif des moyens informatiques mis à leur disposition par l'entreprise.

   S'il est toléré que les collaborateurs puissent être amenés à utiliser l'accès au Internet à des fins personnelles, il ne peut toutefois s'agir que d'une utilisation ponctuelle, occasionnelle, raisonnable et limitée dans le seul cadre des nécessités de la vie courante et familiale.

   L'employeur peut-être amener à contrôler l'utilisation de l'accès à Internet conformément à la réglementation applicable.

b. En conséquence, les dispositions de l'article 8.1.2 « Bonnes mœurs – usages ludiques » sont aussi applicables en dehors des heures de travail.

c. L'utilisation à des fins personnelles d'internet ne doit en outre n'avoir en aucun cas d'impact significatif :
   - Sur l'exécution et la durée du travail,
   - Sur la qualité professionnelle et la productivité du collaborateur,
   - Sur la sécurité du réseau de l'entreprise et l'usage normal du réseau informatique, - sur le coût d'exploitation du réseau de l'entreprise.

8.2.2 Le télétravail

Les règles de la présente charte s'appliquent à l'Utilisateur dans le cadre du télétravail.

L'Utilisateur s'assure d'utiliser l'équipement informatique mis à sa disposition uniquement pour ses besoins professionnels.
L'Utilisateur s'abstient de mettre à disposition de son cercle privé et familiale l'équipement informatique mis à sa disposition par l'Entreprise.

L'utilisateur en télétravail doit s'assurer de la confidentialité des données.

Lors des déplacements, il lui est conseillé de :

- De garder son ordinateur avec soi et de le surveiller
- De le laisser dans les locaux du Groupe sous clé
- De le mettre dans le coffre de la chambre d'hôtel

8.2.3 Intervention sur les forums, groupe de discussions, réseaux sociaux... etc

N'entrant pas dans le cadre des nécessités de la vie courante et familiale, les collaborateurs de l'entreprise ne sont pas autorisés, même à titre privé, de se connecter sur des forums ou à participer à des groupes de discussions n'ayant pas un caractère professionnel tel que prévu à l'article « 8.1.2 Bonnes mœurs - Usages ludiques ».

8.2.4 L'achat en ligne

L'achat en ligne sur des sites de e-commerce est toléré de manière ponctuelle et occasionnelle en dehors des heures de travail effectives.
Seule la responsabilité du collaborateur peut être engagée dans ce domaine et l'entreprise ne pourrait en aucun cas être mise en cause dans le cas d'un piratage des codes de carte bancaire, ou d'une utilisation frauduleuse des informations bancaires du collaborateur lors d'un acte de commerce électronique par le biais de l'outil informatique de l'entreprise.
Les collaborateurs veilleront en outre à respecter les dispositions du paragraphe « 4.2.2.5 Actions contre les spams ».

8.2.5 Copyright

Les collaborateurs de l'entreprise amenés à copier des documents sur des sites Internet (photos, textes, illustrations) dans le cadre d'une utilisation personnelle telle que définie au paragraphe « 8.2.1 Bon usage », sont responsables à titre personnel de ces copies et de leurs utilisations.
Il leur est toutefois conseillé de procéder à ces copies dans le respect de la législation du copyright et de consulter si nécessaire le service Juridique ou la Direction Communication et Relations Clients.

9

Données à caractère personnel

L'Entreprise et ses entités s'engagent à respecter la réglementation sur la Protection des données personnelles, conformément à la Loi Informatique et Libertés du 06 Janvier 1978 modifiée et au Règlement Général sur la Protection des Données (RGPD).

Cette Règlementation s'applique aux traitements de données qui visent une personne physique identifiable directement ou indirectement.

La Politique de Protection des données personnelles de l'entreprise est accessible pour les collaborateurs via Intranet et pour les clients via le site Internet, l'application mobile et l'Espace Locataire du client.

Chaque collaborateur s'engage donc à respecter la Loi Informatique et Libertés et le Règlement Général sur la Protection des Données personnelles (RGPD).

La Charte éthique de l'entreprise précise également dans son Chapitre III « Utilisation et Protection des informations » les règles à respecter.

Le Délégué à la Protection des Données (DPO) de l'entreprise est votre disposition pour vous apporter son expertise et répondre à vos questionnements, pour être conforme avec la règlementation en vigueur ; vous pouvez le contacter notamment par mail à : dpo-logifim@vilogia-logifim.fr

9.1 Données à caractère personnel concernant les Utilisateurs salariés

Elles apparaissent notamment dans les traitements suivants :

- La gestion administrative : gestion du dossier professionnel tenu conformément aux dispositions législatives et réglementaires, ainsi qu'aux dispositions statutaires, conventionnelles ou contractuelles, gestion des annuaires internes et des organigrammes, réalisation d'états statistiques ou de listes d'employés, gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement, contrôle de l'accès aux locaux, gestion des élections professionnelles, notamment par voie électronique, gestion des réunions des instances représentatives du personnel, gestion de l'action sociale, affiliation aux régimes de prévoyance et de complémentaires santé, affiliation aux contrats collectifs d'épargne ;
- La gestion de la paie ;
- La mise à disposition d'outils informatiques : suivi et maintenance du parc informatique, gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux, mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, gestion de la messagerie électronique professionnelle, intranet ;

- L'organisation du travail : gestion des agendas professionnels, gestion des tâches, gestion du planning et des affectations, dispositif de continuité d'activité ;

- La gestion de votre carrière : évaluation professionnelle, gestion des compétences, validation des acquis de l'expérience, simulation de carrière, gestion de la mobilité professionnelle ;

- La formation : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations.

Les données des Utilisateurs salariés sont transmises par l'Entreprise :

- Aux organismes publics dans le cadre des obligations légales de l'Entreprise ;
- Aux organismes de prévoyance, de complémentaire santé et d'épargne collective à des fins d'affiliations ;
- Au Comité Social Economique (CSE) ou au Comité d'Entreprise, sauf opposition de la part de l'Utilisateur salarié
- Aux sous-traitants techniques et informatiques de l'Entreprise ;
- Aux sous-traitants en matière de formation ou de gestion de carrière.

Elles ne sont en aucun cas cédées à un tiers à des fins commerciales. Elles sont conservées par l'Entreprise pour la durée nécessaire à l'exécution de ses obligations légales et contractuelles.

9.2 Gestion du droit d'accès et de modification des données à caractère personnel

Conformément aux dispositions légales, l'Utilisateur dispose d'un droit d'accès, de rectification, de suppression et d'opposition pour motif légitime, de limitation des données ainsi que d'un droit à l'oubli et d'un droit à la portabilité de ses données. L'Utilisateur a également la possibilité de faire part du sort qu'il souhaite réserver à ses données post-mortem.

Pour exercer ces droits, l'Utilisateur peut agir auprès de l'Entreprise, aux coordonnées suivantes : dpo-logifim@vilogia-logifim.fr .

Les informations collectées sont destinées à la gestion du personnel de L'Employeur.

9.3 Déclaration de nouveaux traitements de données à caractère personnel

Les Utilisateurs souhaitant mettre en œuvre des nouveaux traitements utilisant des données à caractères personnels doivent préalablement prendre contact avec le DPO de l'Entreprise avant d'y procéder.

Le Délégué à la Protection des Données veille au sein de l'Entreprise à la bonne application des règles applicables aux traitements de données à caractère personnel.

9.4 Exercice du Droit d'alerte d'un collaborateur, conformément à la *Charte du Droit d'alerte*

L'entreprise s'engage notamment à ce que les procédures mises en œuvre, pour recueillir les signalements, garantissent une stricte confidentialité de l'identité de l'auteur du signalement, en conformité avec la Loi et règlements applicables.

10 Contrôles d'activité

10.1 Rôle d'administrateur

Les administrateurs s'assurent du fonctionnement normal et de la sécurité des réseaux et systèmes de sécurité informatiques de l'entreprise. Ils disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

10.2 Les modalités d'intervention.

Les administrateurs ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables au contenu des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

10.3 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (« logs »), créés en grande partie automatiquement par les équipements informatiques et de communications électroniques. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'Entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des Utilisateurs et des tiers accédant au système d'information.

Les Utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication mais également pour détecter d'éventuels manquement des collaborateurs aux disposition de la présente charte. Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites Internet ou le téléchargement de fichiers ;
- Aux coûts liés aux communications électroniques (téléphoniques ou données) émises et reçues à partir d'équipements fournis à l'Utilisateur salarié par l'Entreprise

L'attention des Utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges, et ce y compris l'accès à des flux sécurisés. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

10.4 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par l'Entreprise, mais également pour détecter d'éventuels usages abusifs des outils informatiques ou des faits préjudiciables à l'entreprise, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs Utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un Utilisateur, et sauf risque ou événement particulier, l'Entreprise ne peut ouvrir les fichiers identifiés par le salarié comme « Privé » ou « Personnel » contenus sur les Ressources du SI mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ou via une autorisation judiciaire.

10.5 Messagerie

a. L'administrateur peut avoir accès à toutes les messageries de l'entreprise et exercer un contrôle technique permanent sur le flux des emails, émis, reçus, archivés, susceptibles de perturber le bon fonctionnement du réseau, notamment en cas du poids et de la taille des messages, fichiers et dossiers joints.

Il dispose d'un système d'alerte automatique en cas d'emails émis, reçus, archivés susceptibles de perturber le bon fonctionnement du réseau.

b. En cas d'anomalie, l'administrateur réseau est habilité à contrôler ces emails perturbateurs, à en prendre connaissance, qu'ils soient à titre professionnel ou à titre privé, à en bloquer ou à en suspendre leur diffusion.

Les contenus de ces emails sont alors transférés sur un logiciel de traitement et les données sont conservées au moins pendant une période de 6 mois avant leurs destructions.

Le destinataire ou/et l'utilisateur du ou des mails concernés en sont toutefois informés par un email de l'administrateur réseau ou par une note écrite.

c. En outre, dans le cadre du processus de lutte contre les spams, l'administrateur réseau :

- gère la boîte emails dédiées aux spams et leur destruction automatique,
- gère et modifie le fichier d'adresses professionnelles,
- gère la liste et son application, des « expéditeurs d'emails spécifiquement accrédités » par chaque collaborateur de l'entreprise,
- détermine les quotas d'alerte et leurs effets,
- procède aux « nettoyages » des messageries,
- et ce, conformément aux dispositions des paragraphes 4.2.2.5 et 4.2.2.6 du chapitre 4 de la présente charte informatique.

d. L'employeur peut également contrôler le contenu des messages professionnels, dès lors qu'il a un intérêt légitime pour le faire, tels que des problèmes de sécurité ou bien la nécessité d'éviter des usages abusifs ou des faits préjudiciables à l'entreprise. Sauf risque ou événement particulier, l'Entreprise ne peut ouvrir les messages identifiés par le salarié comme « Privé » ou « Personnel » contenus sur les Ressources du SI mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ou via une autorisation judiciaire.

10.6 Réseau informatique

L'administrateur procède aussi à toute intervention utile, pour prévenir et lutter contre toute attaque et/ou contamination de virus, ainsi que pour éviter toutes difficultés d'organisation de fonctionnement et de viabilité du réseau informatique.

a. La sécurité du réseau justifie ainsi que l'administrateur puisse avoir accès à toutes informations utiles pour mener ses interventions préventives ou curatives nécessaires au bon fonctionnement du réseau informatique.

   En conséquence, l'administrateur a :

   - l'accès technique à toutes informations du système d'information utiles contenues dans les postes de travail, les répertoires partagés, les contenus des messageries, les fichiers «logs» ou fichiers de journalisation ainsi que tout autre logiciel permettant le fonctionnement de l'outil informatique de l'entreprise ;
   - la possibilité de prendre connaissance des fichiers, dossiers, messages individuels, à titre professionnel ou à titre privé, ainsi que toutes informations liées à l'usage des postes informatiques des collaborateurs (coordonnées des postes connectés ; heures de connexions et adresses des sites visités ou des emails envoyés ou reçus ; détail des opérations de navigation et de téléchargement… etc.).

b. L'administrateur agit et est identifié en tant que tel. Il ne peut pas prendre l'identité de l'utilisateur ni se substituer à lui.

c. L'administrateur est autorisé à prendre toute mesure utile que la sécurité du réseau impose et, le cas échéant, à rappeler, les règles d'utilisation aux collaborateurs de l'entreprise qui n'en appliqueraient pas correctement les règles et principes.

d. La bonne gestion de l'outil informatique de l'entreprise peut en outre justifier que l'administrateur ait recours à un ou des logiciels de télémaintenance.

Dès lors qu'il a un intérêt légitime pour le faire, tels que des problèmes de sécurité ou bien la nécessité d'éviter des usages abusifs ou des faits préjudiciables à l'entreprise, l'employeur peut également prendre connaissance des fichiers, dossiers, messages individuels, à titre professionnel, ainsi que toutes informations liées à l'usage des postes informatiques des collaborateurs (coordonnées des postes connectés ; heures de connexions et adresses des sites visités ou des emails envoyés ou reçus ; détail des opérations de navigation et de téléchargement… etc.).

En outre, il sera rappelé à toute personne intervenant dans le cadre d'une opération de télémaintenance, notamment lorsque celle-ci est extérieure à l'entreprise, l'obligation de n'accéder qu'aux informations informatiques utiles pour l'accomplissement de ses interventions et d'en assurer la confidentialité.

10.7 Sécurité informatique

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information, différents dispositifs sont mis en place.

10.7.1 Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour l'entreprise et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (Peer to Peer, messagerie instantanée, …).

10.7.2 Les systèmes automatiques de traçabilité

Le pôle informatique de l'entreprise opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisations (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'événement.

Le pôle informatique est le seul utilisateur de ces informations.

10.7.3 Les systèmes automatiques d'analyse

Une analyse des traces de connexion (échecs et succès) est réalisée régulièrement afin de détecter les tentatives d'intrusion ou de malveillance sur le SI.

- Contrôle antivirus : les flux HTTP HTTPS et FTP seront soumis à un contrôle antivirus
- Les logs des équipements actifs de sécurité (firewalls, IDS, passerelles…) sont contrôlés toutes les semaines et font l'objet d'une analyse approfondie une fois par mois,
- Les logs des serveurs critiques sont analysés une fois par mois.

10.8 Obligation de confidentialité – limites

Les collaborateurs du service informatique, en tant qu'administrateur, sont tenus personnellement à une stricte obligation de confidentialité quant aux informations collectées et constatées relatives au non-respect des dispositions des présentes règles d'usage Informatique et Multimédia par les collaborateurs de l'entreprise. Il en est de même pour le contenu des fichiers, dossiers et emails à « caractère personnel » tels que définis au paragraphe 4.3.2 « mention personnel ou privé » du chapitre 4 dont l'administrateur aurait pu avoir connaissance.

L'administrateur n'est pas tenu par cette obligation de confidentialité s'il constate des dérives et peut divulguer le contenu des informations dont il a pu prendre connaissance à sa hiérarchie directe :

- en cas de dispositions législatives particulières le prévoyant ;
- en cas de grave mise en cause du bon fonctionnement ou de l'intérêt ou de la sécurité de l'entreprise.

11

Sanctions - PSSI-RH-07

En cas d'abus manifestes, évoqués par l'administrateur du système d'information, telles que rappelées à l'article 10.4 du chapitre 10 précédent, ou constatées à compter d'informations globales et générales recueillies selon les dispositions rappelées au chapitre 10 précédent, la Direction de l'entreprise pourra toutefois prendre toute mesure utile pour constater et/ou faire constater le non-respect des dispositions des présentes règles d'usage Informatique et Multimédia par les collaborateurs éventuellement concernés (usages abusifs d'Internet, sécurité réseau, non-respect des dispositions des articles 4.2.2.1, 4.3.1 et 8.1.2 de la présente charte, notamment relatives aux messages ou sites contraires aux bonnes mœurs).

Il en sera de même en cas de faits fautifs dans l'exercice des attributions et fonctions des collaborateurs ou en cas de non-respect de la confidentialité et des loyautés liées à leurs contrats de travail.

Toutefois, l'entreprise est tenue de respecter la confidentialité des messages, fichiers, dossiers ayant un caractère « personnel » dans les conditions définies au paragraphe « 4.3.2 mention personnel ou privé » du chapitre 4 de la présente charte informatique. La prise de connaissance du contenu de ces documents ne pourra en conséquence être effectuée que conformément aux règles légales applicables.

Responsabilité civile et pénale des collaborateurs

L'entreprise rappelle que les collaborateurs peuvent être tenus responsables civilement et pénalement du fait de leurs actes commis hors du cadre de leurs fonctions et pouvant constituer en outre des infractions relatives à la Réglementation en vigueur.

Les collaborateurs de l'entreprise peuvent consulter auprès du Département Juridique, la liste des textes comportant, dans ces différents domaines, une infraction pénale.

Dans le cas où la responsabilité de l'entreprise était recherchée du fait d'actes illicites et/ou anormaux de ses collaborateurs, commis en dehors du cadre de leurs fonctions, l'entreprise se réserve le droit d'exercer un recours judiciaire contre le ou les collaborateurs concernés.

13

Publicité, dépôt et révision

La présente charte informatique présente affichée et déposée conformément aux articles L1321-4 et suivants, et R1321-1 et suivants du Code du Travail et entrera en vigueur le 1er février 2023, soit un mois après l'accomplissement des dernières formalités de dépôt et de publicité.

La présente charte informatique a été soumise, pour avis, au Comité Social et Économique (CSE).

La présente charte informatique sera, à la diligence de l'entreprise, adressée en deux exemplaires à l'Inspecteur du Travail, accompagnée du procès-verbal de consultation du Comité Social et Économique.

Un exemplaire a été déposé au greffe du Conseil de Prud'hommes de Lille.

Il oblige tout salarié embauché à l'observation de ses prescriptions et des modifications qu'elle pourrait ultérieurement recevoir.

Toute modification ultérieure à la présente charte informatique sera soumise à la procédure définie à l'article L1321-4 du Code du Travail.

La présente charte informatique est par ailleurs consultable dans l'Intranet.

Fait à Armentières, en 4 exemplaires originaux, le 14 novembre 2022,

Philippe DEHOUVE
Président du Directoire