Confiance et transparence dans l'usage des systèmes d'information

Annexe du règlement intérieur

PREAMBULE

Pour servir nos ambitions, nous agissons en nous appuyant sur un socle commun, des valeurs de confiance et d'autonomie permettant à chaque collaborateur d'être acteur dans un monde qui change, d'être ouvert, connecté, utile et de se réaliser.

Pour y parvenir, ensemble, nous innovons, testons, expérimentons, interagissons avec nos communautés, ce qui implique plus de technologies, plus d'échanges et de partages de données. En résumé, à la fois plus de numérique et d'humain.

Dans le même temps, les réglementations nationales et européennes évoluent vers un renforcement de la protection des systèmes d'information et particulièrement des données à caractère personnel des clients habitants comme des collaborateurs.

En parallèle, le risque lié à la cybercriminalité est de plus en plus élevé et rend l'ensemble des collaborateurs acteurs de la protection de l'Entreprise et de son Système d'Informations.

Dans ce contexte, la sécurité des systèmes d'information est essentielle au soutien de nos ambitions. C'est un facteur de confiance pour :

Les clients habitants, collaborateurs, partenaires, acteurs de notre écosystème,

L'image de marque de notre Entreprise et sa capacité à répondre aux projets de ses clients habitants,

Et, au final, l'Entreprise elle-même

En tant qu'utilisateur des systèmes d'information, chaque collaborateur est concerné, et y contribue.

Le présent document a pour objet de faire connaître et faire comprendre les principales règles d'usage des systèmes d'information de l'Entreprise.

Il me permet, en tant que collaborateur-utilisateur, de contribuer à la réalisation de nos ambitions en adoptant un comportement responsable et des pratiques respectueuses de la sécurité des systèmes d'information.

Un système d'information est un ensemble organisé de Ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

Une ressource peut désigner un matériel (ordinateur, imprimante, serveur, équipement réseau, périphérique…), un logiciel (système d'exploitation, logiciel bureautique…), une application (Pyxis, Saveo…), un outil de communication numérique (messagerie électronique, communautés collaboratives d'Entreprise, partage de fichiers, accès Internet…), un service externe (offre d'hébergement, service Cloud…) ou tout simplement une information (sous forme unitaire ou de base de données).

La sécurité des systèmes d'information est l'ensemble des moyens et mesures techniques, organisationnels, juridiques et humains visant à prévenir, détecter ou réagir à un impact sur une ressource d'un système d'information concernant :

- sa disponibilité, c'est-à-dire son usage aux moments choisis,
- son intégrité, c'est-à-dire sa capacité à rester exacte, complète et fiable,
- sa confidentialité, c'est-à-dire son accès aux personnes, entités ou Ressources autorisées,
- sa traçabilité, c'est-à-dire sa capacité à prouver l'origine et la date de toute action réalisée.

CHAMP D'APPLICATION

Ce document, associé au règlement intérieur des différents sites, s'applique aux entreprises de l'unité économique et sociale Leroy Merlin (UES Leroy Merlin, ci-après l'Entreprise) ainsi qu'aux utilisateurs de ses systèmes d'information.

Le terme « utilisateur » représente ici toute personne physique :

- travaillant au service de l'Entreprise, quel que soit son statut ou son contrat : dirigeant, salarié à temps plein ou temps partiel, personnel intérimaire, stagiaire…
- ayant accès aux systèmes d'information de l'Entreprise, à tout ou partie de ses données, et par tout type d'équipement (clé USB, ordinateurs, serveurs…).

PARTIE 1 : MOI ET MON USAGE DES SYSTEMES D'INFORMATION

1.1- Je préserve la confidentialité de mes moyens d'accès

Dans le cadre de mes fonctions, je dispose d'un accès aux systèmes d'information de l'Entreprise dans les conditions définies par l'Entreprise.

Mes accès sont effectués à partir d'identifiants (email, login informatique à 8 chiffres…) et d'authentifiants (mot de passe, code PIN, certificat…). Ils assurent mon identité et mes droits d'accès sur les systèmes d'information de l'Entreprise.

Mes authentifiants sont personnels. Je ne les donne pas à un tiers, même temporairement, même à un administrateur des systèmes d'information de l'Entreprise. Je ne cherche pas à connaître ni utiliser les authentifiants d'un autre Utilisateur.

Mes authentifiants sont dédiés à un usage professionnel, je ne les utilise pas pour avoir accès à un service qui n'est pas à destination de l'entreprise.

On appelle ici Administrateur, toute personne physique ayant des accès de modifications sur les mécanismes de fonctionnement technique, applicatif ou de sécurité d'un matériel, logiciel, application, ou service des Systèmes d'Information de l'Entreprise. Il peut donc s'agir de développeurs, responsables applicatifs, administrateurs réseaux, systèmes, base de données, web, sécurité, administrateurs fonctionnels métiers .

Je garantis la sécurité de mes authentifiants :

- En respectant les règles de création et de renouvellement des mots de passe définies par l'Entreprise,

  8 caractères minimum, des minuscules, majuscules, chiffres, et caractères spéciaux. Pas de prénom, année de naissance, ou mot du dictionnaire. A renouveler tous les trois mois.

- En mémorisant mes mots de passe ou en les stockant dans un outil adapté et fourni par l'Entreprise (comme un coffre-fort électronique de mots de passe),
- En différenciant les mots de passe utilisés sur Internet de ceux utilisés au sein de l'Entreprise.

Ainsi, toute action ou accès effectué avec mes authentifiants est réputé avoir été réalisé par moi-même.

1.2- J'utilise de manière responsable mes accès et mes équipements

J'accède, utilise, modifie ou supprime uniquement les ressources des systèmes d'information de l'Entreprise qui entrent dans le cadre de ma mission.

Je m'interdis d'accéder ou de copier des informations d'autres utilisateurs ou d'autres départements sans leur consentement exprès.

Je n'installe, n'utilise, ne développe ou ne diffuse pas de Ressources mettant en risque la sécurité des données ou des systèmes d'information de l'Entreprise. Ainsi :

- Je télécharge, installe et utilise uniquement des logiciels de source de téléchargement fiables, autorisés par l'Entreprise et dont les licences ont été acquittées. En cas de doute, je contacte le support informatique.
- Je connecte uniquement des périphériques ou supports de stockage dont je connais la provenance et la sécurité. De nombreuses attaques sont en effet réalisées par l'envoi ou le dépôt ciblé de clés USB infectées.

Je n'arrête, ni ne contourne les dispositifs de sécurité (antivirus, mises à jour, outils d'inventaire, filtrage internet...) mis en place par l'Entreprise pour lutter contre les menaces.

En cas d'absence temporaire, je verrouille systématiquement ma session Utilisateur.

> Par exemple, lorsque je suis sollicité par un client en magasin ou lorsque je dois me déplacer dans un rayon du magasin, je verrouille ma session Utilisateur même si mon absence est brève.

Je protège mes équipements mobiles (ordinateur, téléphone mobile, tablette, support de stockage…) contre le vol via un câble antivol mis à disposition par l'Entreprise ou par un stockage dans un emplacement fermé.

1.3- Je protège les données de l'entreprise

Je stocke systématiquement mes données professionnelles au sein des emplacements de stockage informatique proposés par l'Entreprise (Emplacement partagé du service, du magasin ou dédié à mon usage – Google drive partagés, Disque réseau partagé…) afin d'assurer la sauvegarde de ces données et leur restauration en cas d'incident.

> Les fichiers stockés sur les disques-durs locaux des ordinateurs utilisateurs ou les supports de stockage externes (clés USB…) ne sont pas sauvegardés : en cas de perte ou de vol, les fichiers sont définitivement perdus.

Je transmets des données de l'Entreprise qu'à des personnes autorisées. Je limite l'accès aux données uniquement aux personnes autorisées. Pour cela, je m'assure avec le propriétaire de l'information de la légitimité du destinataire (d'autant plus si le document est confidentiel ou secret) et je veille à utiliser une méthode de partage adaptée à la sensibilité des informations échangées. En effet, certaines données, comme celles de nos collaborateurs ou clients-habitants, doivent faire l'objet de protections spécifiques.

> En cas de doute sur la méthode de partage, j'utilise par défaut les solutions de partages de fichiers sécurisées :
> - Partage Google Drive avec accès nominatifs
>
> Attention notamment à l'usage des répertoires partagés comme P:\Public accessibles à tous. Attention également à l'envoi d'e-mails sur des adresses externes à l'entreprise : ces messages peuvent être interceptés et modifiés.

Je ne copie pas d'informations de l'Entreprise pour archive personnelle ou au profit d'une société tierce. Ces données sont la propriété exclusive de l'Entreprise. De plus, elles peuvent bénéficier d'une protection spécifique au titre du secret des affaires, du savoir-faire de l'Entreprise ou encore d'un droit de propriété intellectuelle (droit d'auteur, brevet, marque, dessin et modèle). En conséquence de quoi, ces données doivent être exploitées et maîtrisées exclusivement par l'Entreprise.

Je stocke uniquement si nécessaire des données professionnelles sur un support de stockage (disque-dur, clé USB…) uniquement après avoir activé, si besoin avec l'aide du support informatique, la protection en chiffrement du support. En cas de vol ou de perte, les données seront inaccessibles par un tiers.

Par exemple, sur Windows 10, je fais un clic-droit sur le lecteur lié à la clé USB ou au disque-dur. Je clique sur « Activer Bitlocker » puis je configure le mot de passe de chiffrement.

1.4- Je protège les données à caractère personnel des collaborateurs, de nos partenaires et des clients-habitants

Une donnée à caractère personnel représente toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. *Par exemple : nom, prénom, adresse, date de naissance, photographie, adresse IP, adresse email, numéro de téléphone.*

Un traitement de données représente toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données, telles que 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, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. *Par exemple : création d'un fichier client, organisation d'un jeu concours, location de matériel.*

Un responsable de traitement est la personne qui détermine les finalités et les moyens d'un traitement. En général, il s'agit du représentant légal de la société ou de l'un de ses délégataires.

Le Délégué à la protection des données (DPD) est la personne physique désignée par l'Entreprise pour être l'interlocuteur privilégié concernant la protection des données à caractère personnel.

Le comité Data Compliance est un comité pluridisciplinaire, composé notamment du référent RH, du référent Marketing, du référent Sécurité SI, du référent Légal et du DPD, ayant notamment pour rôles :

- La définition et la mise à jour des règles d'Entreprise concernant le traitement des données à caractère personnel;
- La définition et la mise en œuvre de la gouvernance d'Entreprise concernant la gestion des données à caractère personnel et de leurs traitements au regard des obligations réglementaires.

Avant de mener un traitement de données à caractère personnel (collaborateurs, partenaires ou clients-habitants), je contacte le Délégué à la protection des données afin de :

- Vérifier le respect du cadre juridique applicable. S'il s'agit d'un nouveau traitement, il conviendra de le soumettre préalablement à sa mise en œuvre au comité Data Compliance pour validation,
- Connaître les mesures de sécurité applicables et de les mettre en œuvre,
- Connaître les formalités préalables relatives à la mise en œuvre de ce traitement.

1.5- J'utilise la messagerie professionnelle (électronique ou instantanée)

L'Entreprise met à disposition des messageries électroniques et instantanées professionnelles. Ainsi, j'utilise uniquement les messageries professionnelles dans le cadre de mes fonctions. Je ne renvoie aucun message professionnel vers mon compte de messagerie personnelle.

Au même titre que pour le courrier traditionnel, je suis responsable de la forme et du contenu des messages que j'échange. Je dois veiller à ce que leur contenu ne porte pas atteinte directement ou indirectement à l'image ou à la réputation de l'Entreprise. En cas de transfert d'un message, je n'en altère pas le contenu, à moins de mettre clairement en évidence les changements apportés.

Je communique mon adresse de messagerie professionnelle de manière raisonnée, ceci afin de limiter l'apparition de courriers non sollicités (« spams »). De plus, je veille à ce que la diffusion de mes messages soit limitée aux seuls destinataires réellement concernés ou habilités. Je ne propage pas de messages collectifs, qui ne visent pas l'accomplissement de ma mission de travail.

En cas de message provenant d'un émetteur suspect, je n'ouvre pas le message. Si le message est déjà ouvert et que son contenu s'avère suspect, je ne réponds pas à l'émetteur du message, ni ne clique sur aucun lien ou aucune pièce-jointe et préviens immédiatement le support informatique.

Un message est suspect lorsque :
- l'expéditeur ne m'est pas connu,
- l'orthographe est approximative ou le message est peu lisible,
- le contenu du message est inhabituel par rapport au contexte ou aux échanges précédents,
- le contenu évoque un gain financier ou demande des informations,
- il évoque un caractère d'urgence,
- il me demande d'effectuer un virement bancaire au nom de l'Entreprise,
- il présente une des caractéristiques listées ci-dessus quand bien même le message comprendrait le logo d'un organisme officiel,

Et d'autant plus s'il contient un lien ou une pièce-jointe.

1.6- Je surfe sur Internet

Un accès à Internet m'est attribué dans le cadre de mes fonctions afin de me permettre de visiter des portails de contenus sous le nom de l'Entreprise.

Je veille à ne pas surcharger de manière abusive les ressources de l'Entreprise par le transfert de fichiers volumineux ou l'accès à certaines ressources multimédia.

Si je doute de la fiabilité ou de la sécurité d'un site Internet, je stoppe ma navigation et contacte le support informatique. En effet, certains sites contiennent des virus qui pourraient compromettre nos systèmes d'information.

1.7- J'utilise les médias sociaux Internet (Twitter, Facebook, Linkedin…)

L'utilisation, dans le cadre de mes fonctions, d'espaces de discussion et des médias sociaux publics sur Internet est conditionnée par le respect des mêmes règles de courtoisie que la messagerie sur les contenus publiés. Par ailleurs, je ne porte pas atteinte à travers mes propos à l'image de marque de l'Entreprise. Tous propos et contenus que je publie sur ces espaces sont susceptibles d'engager ma responsabilité ainsi que celle de l'Entreprise, je dois donc être particulièrement vigilant sur leur teneur.

Pour échanger entre collaborateurs sur des sujets internes à l'Entreprise (fonctionnement, axes d'amélioration…), il est recommandé d'utiliser les communautés collaboratives d'Entreprise (Workplace). Attention notamment aux publications sur certaines communautés Internet d'apparence privées qui utilisent le nom de l'Entreprise (ex : groupes Facebook, forums…). Ces publications, accessibles à plusieurs milliers de personnes, sont considérées comme publiques et engagent l'image de l'entreprise.

Je publie sur Internet uniquement des informations strictement nécessaires et publiques. Je m'interdis de publier des informations ou des données sur nos collaborateurs, clients-habitants, partenaires, ou projets sensibles de l'Entreprise.

Des personnes malveillantes récoltent les informations publiques, ou privées de manière frauduleuse, afin de déduire des mots de passe ou de mener des malversations.

1.8- Je participe aux communautés collaboratives de l'Entreprise

Les communautés de la plateforme collaborative de l'Entreprise sont modérées (exemple : Workplace). Si certains contenus venaient à ne pas respecter les conditions générales d'usage de ces médias, les modérateurs prendront l'initiative de supprimer les contenus en question. Pour information, certains de nos clients-habitants accèdent à nos communautés, il convient de faire preuve de prudence et de vigilance sur les contenus publiés.

1.9- J'utilise les services Cloud

J'utilise uniquement les services Cloud (partage, stockage, travail collaboratif…) validés et mis à disposition par l'Entreprise en particulier la suite de logiciel Google. En effet, les autres services n'offrent pas de garantie contractuelle de protection de nos données et peuvent être dangereux pour la sécurité de nos systèmes d'information.

1.10- Je respecte le droit à l'image

Avant de mettre à disposition ou d'exploiter l'image d'un collaborateur ou d'un tiers, je dois recueillir son consentement à l'utilisation de son image. En cas de besoin, je contacte le service juridique pour connaître les modalités d'obtention de ce consentement ou des droits.

1.11- Je respecte la propriété intellectuelle

Je ne télécharge, reproduis, copie, diffuse, modifie ou n'utilise pas d'œuvres protégées par un droit de propriété intellectuelle (musiques, extraits de films, logiciels…), sans avoir obtenu le consentement préalable des titulaires de ces droits ou s'être acquittés des droits y afférents (Sacem…). En cas de besoin, je contacte le service juridique pour connaître les modalités d'obtention de ce consentement ou des droits.

Les copies de sauvegarde (par exemple, celles d'un logiciel acquis par l'Entreprise), dans les conditions prévues par le code de la propriété intellectuelle, ne peuvent être effectuées que par les personnes habilitées (par exemple, les administrateurs des systèmes d'information de l'Entreprise).

1.12- J'utilise un smartphone professionnel

Lorsque l'Entreprise met à ma disposition un smartphone professionnel, je dois observer les règles d'usage suivantes :

- Je n'installe que les applications nécessaires depuis des magasins d'applications officiels (App Store Apple, Google Android Store…),

- Je ne bloque pas les mises à jour proposées par le système,
- En plus du code PIN qui protège la carte SIM, je définis un mot de passe pour sécuriser l'accès au smartphone (autre que 0000, 1234 ou ma date de naissance) et le configure pour qu'il se verrouille automatiquement,
- J'effectue des sauvegardes régulières de mes contenus professionnels sur mon répertoire réseau personnel afin de pouvoir les restaurer en cas de perte ou de vol,
- Je suis prudent lorsque je consulte mon smartphone dans des lieux publics (transports publics, gare, restaurants).

Des solutions de protection des appareils mobiles (logiciel antivirus par exemple) peuvent être mises en place afin d'assurer la protection des données et services de l'entreprise contenus dans ces derniers. Je n'arrête, ni ne contourne les dispositifs de sécurité mis en place par l'Entreprise sur les smartphones..

Si j'utilise mon smartphone personnel pour des besoins professionnels, voir la partie « Je peux utiliser mes équipements personnels »

1.13- J'accède à distance aux systèmes d'information

Dans le cadre de ma mission, et sur validation par l'Entreprise, je peux accéder à distance à certaines ressources des systèmes d'information de l'Entreprise (une fonction ou un geste métier sensible peut, de par sa criticité ou sa spécificité technique, ne pas faire l'objet d'un accès à distance).

Un accès à distance représentant une opportunité d'intrusion par des tiers (concurrents, pirates informatiques …), j'utilise mon accès à distance uniquement en cas de nécessité et dans le cadre strict de mes fonctions.

L'accès à distance est protégé par une connexion à plusieurs facteurs, ainsi on me demandera mes identifiants et une validation supplémentaire (par exemple sur smartphone avec PingID). Sans cette authentification multi-facteur je ne peux me connecter aux outils de l'entreprise à distance

De plus, je respecte les règles suivantes en situation de mobilité :

- J'utilise un filtre de confidentialité dans les transports et les lieux publics.
- Je garde mes équipements (ordinateur, téléphone, tablette…) sur moi ou constamment sous surveillance, même un court instant.
- Je limite autant que possible le recours aux réseaux sans-fil publics (Wifi gare, aéroport, restaurants, café…).
- Je n'utilise pas d'équipement d'une tierce personne ou en libre-service pour un besoin métier (y compris consulter sa messagerie professionnelle, ou son Google Drive sur les équipements précités). De même, je ne connecte pas de support de stockage professionnel sur un équipement dont je ne connais ni la provenance ni la sécurité.
- Je ne branche aucun équipement d'une tierce personne sur mon ordinateur (clés USB, téléphones…).

- Je préviens immédiatement le support informatique si un tiers a pu avoir accès à mes équipements (y compris en cas d'inspection ou de saisie de mon matériel par des autorités – et dans ce cas, prévenir également la direction Juridique).

1.14- Je peux utiliser à titre privé les systèmes d'information

Un usage personnel occasionnel et modéré des systèmes d'information de l'Entreprise (notamment du service d'accès à Internet) m'est permis dans le cadre des nécessités de la vie courante et familiale, et cela sans mettre en danger la bonne exécution de ma mission, ni le bon fonctionnement ou la sécurité des systèmes d'information. Ainsi, cet usage ne peut être mené à des fins personnelles lucratives, de promotion, de publicité ou de démarchage.

Cas de mes fichiers et mes messages électroniques

Comme toute donnée stockée sur les systèmes d'information de l'Entreprise est réputée être professionnelle, je dois explicitement désigner celles qui relèvent de ma vie privée. Cela s'applique également aux fichiers présents sur ma clef USB personnelle, celle-ci et son contenu étant réputés être professionnels dès l'instant où je la connecte au Système d'Information de l'Entreprise.

> Dans le cas d'un répertoire de fichiers sur mon ordinateur professionnel ou sur une clef USB connectée à celui-ci, je stocke mes fichiers personnels dans un répertoire nommé « Privé » ou « Personnel ». Dans le cadre d'un échange personnel d'e-mails, je mentionne dans l'objet le terme « Privé » ou « Personnel ».

Ces données privées bénéficieront alors du droit au respect de la vie privée ou du secret des correspondances. L'Entreprise a le droit de consulter les fichiers et messages identifiés comme relevant de ma vie privée en ma présence, ou en mon absence si celle-ci relève d'une mauvaise foi caractérisée de ma part, ou en cas d'urgence, ou en cas de suspicions graves à mon égard (risque particulier notamment de sécurité, de continuité de service, d'atteinte à l'information ou aux intérêts de l'Entreprise, ou d'un fait pouvant engager ma responsabilité).

Je m'interdis de mener des activités contraires au règlement intérieur ou au présent document sous couvert de la mention « Privé » ou « Personnel ». Ainsi, je ne stocke ou n'échange notamment aucune information ou fichier professionnel via cette mention.

Je demeure responsable de la gestion de mes données privées : leur sauvegarde régulière ainsi que leur suppression lors de mon départ définitif de l'Entreprise.

Cas du surf sur Internet

Un usage personnel occasionnel et modéré d'Internet m'est permis dans le cadre des nécessités de la vie courante et familiale, et ce sans entraver la bonne exécution de ma mission, ni le bon fonctionnement ou la sécurité des systèmes d'information. Je surfe uniquement sur des sites qui ne portent pas atteinte à la loi, à l'éthique, aux bonnes mœurs et à l'ordre public.

> Par exemple : je ne télécharge pas de films ou de musiques de manière illégale, je ne consulte pas de site à caractère pornographique, faisant l'apologie du terrorisme, incitant à la haine...

Cas des réseaux sociaux

Dans le cadre privé, je n'exprime pas sur Internet des opinions, des avis au nom et pour le compte de l'Entreprise, ni ne me présente comme un représentant officiel, sans être autorisé par l'Entreprise à remplir ce rôle. Ainsi, je m'assure que mes propos soient bien perçus comme des propos tenus et exprimés à titre personnel par les lecteurs.

Ainsi, de manière générale, que mes propos relèvent de la sphère privée ou publique, je m'assure qu'ils ne sont pas diffamatoires, injurieux, calomnieux ou dénigrants.

> La loi reconnaît un droit à l'image pour tous. L'utilisation croissante des réseaux sociaux amplifie le risque d'atteinte à ce droit. Il convient d'être particulièrement vigilant sur les réseaux sociaux, au regard des risques qui y sont attachés.

1.15- Je peux utiliser mes équipements personnels dans l'exercice de mes fonctions

L'usage de mes équipements personnels (ordinateur, téléphone, tablette…) dans le cadre de mes fonctions m'est permis dans la mesure où cet usage ne met pas en danger le bon fonctionnement ou la sécurité des systèmes d'information. Ainsi,

- L'Entreprise se doit de connaître les équipements qui se connectent à ses systèmes d'information (notamment réseau filaire, wifi « GroupeADEO », Gsuite). Pour certains accès sensibles, mes équipements personnels devront être enregistrés préalablement auprès du support informatique pour bénéficier de l'accès.

- Les équipements utilisés doivent assurer un niveau de sécurité similaire à celui de l'Entreprise, ceci afin de protéger les données professionnelles stockées et les services accédés. Je prends donc connaissance et applique les mesures de sécurité communiquées par le support informatique pour les équipements concernés.
  L'entreprise peut conditionner l'autorisation à se connecter au système d'information avec mon équipement personnel à ces mesures de sécurité.

> Exemples de mesures : Protection par mot de passe de l'équipement, installation d'un antivirus, automatisation des mises à jour, chiffrement du disque ou possibilité d'effacement à distance en cas de vol, usage d'une authentification renforcée pour les accès aux ressources de l'Entreprise, aucune extraction de données à caractère personnel collaborateurs ou clients-habitants…

En l'absence de sécurité adaptée, je ne stocke aucune Information professionnelle sur mes équipements personnels (y compris par transfert d'email ou support de stockage).

A l'issue de mon contrat de travail, je m'engage à effacer l'ensemble des données professionnelles stockées sur mes équipements.

1.16- J'alerte en cas de comportement anormal ou d'incident

En cas de comportement anormal d'un de mes équipements professionnel ou personnel connecté au Système d'Information de l'Entreprise, je préviens immédiatement le support informatique ainsi que mon manager. Je déconnecte alors mon équipement en débranchant le câble réseau ou en forçant le mode « Avion ».

> Exemples de comportements suspects : impossibilité de se connecter, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés…).

En cas de perte ou de vol de mon badge d'accès aux locaux ou de l'un de mes équipements professionnels ou personnel contenant des données de l'Entreprise, je contacte immédiatement le support informatique notamment pour faire changer mes authentifiants.

PARTIE 2 : L'ENTREPRISE ET SON USAGE DE MES INFORMATIONS

Cette partie décrit les principaux usages de mes informations par l'Entreprise.

2.1- Généralités

Afin d'assurer l'octroi des accès et le bon fonctionnement des systèmes d'information, l'Entreprise utilise mes données suivantes :

- Mon nom et prénom associés à mes coordonnées professionnelles, au sein de l'annuaire de l'Entreprise,
- Mon dossier professionnel contenant les données d'identité et de contact, familiales, de recrutement, de rémunération et avantages sociaux, et d'évaluation.
- Mes formations suivies,
- Mes identifiants (LDAP ou email) sur l'ensemble des ressources des systèmes d'information de l'Entreprise auxquelles j'ai accès.

2.2- Badge nominatif sur le lieu de travail

Sur le lieu de travail, le port du badge nominatif est obligatoire. Il sert notamment au contrôle des accès aux locaux, à la gestion des temps de travail (hors collaborateur soumis au forfait jour et cadre dirigeant), ainsi qu'à la gestion de la restauration d'Entreprise.

Chaque passage d'un badge dans un lecteur permet l'enregistrement de données relatives à son détenteur (notamment date et heure de passage, numéro du badge et action effectuée).

Les enregistrements collectés sont mis à disposition :

- Pour le contrôle d'accès aux locaux : aux services généraux,
- Pour la gestion du temps de travail : à la Direction du développement des Hommes,
- Pour la restauration d'Entreprise : au prestataire de restauration.

Ces enregistrements sont conservés pour une durée maximale de 5 ans après mon départ, sauf si des dispositions légales ou réglementaires venaient à imposer des délais de conservation plus importants.

2.3- Ligne téléphonique (fixe ou mobile)

Dans certains cas, l'Entreprise met à ma disposition, pour l'exercice de mon activité professionnelle, une ligne téléphonique fixe et/ou mobile.

L'Entreprise s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de téléphonie ou un suivi des lignes téléphoniques spécifiques à l'usage des représentants du personnel et des représentants syndicaux dans le cadre de leur mandat. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants pour vérifier que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

L'Entreprise procède à la comptabilisation statistique des flux téléphoniques entrants et sortants au niveau d'un service pour imputer les dépenses téléphoniques au dit service. Lorsque des relevés téléphoniques sont établis, les quatre derniers chiffres des numéros téléphoniques sont occultés. Ils sont disponibles à ma demande.

La durée de conservation des données relatives à l'utilisation des services de téléphonie n'excède pas un an, sauf si des dispositions légales ou réglementaires venaient à imposer des délais de conservation plus importants.

2.4- Supervision des systèmes d'information

Afin de détecter les signaux révélateurs de dysfonctionnement, d'attaques informatiques (intrusion, fraude, fuite d'information…), de pratiques illégales ou abusives, l'Entreprise met en œuvre sur le Système d'Information des protections et des outils de supervision automatisés : sur les flux réseaux (internes ou partenaires), les flux internet (qu'ils soient chiffrés ou non), les messages (reçus ou envoyés), les équipements utilisateurs (ordinateurs, smartphones, etc), les serveurs (via antivirus, outil de gestion de parc), les partages de fichiers, les produits digitaux.

Les traces émises par ces outils peuvent contenir :

- La date et l'heure d'un événement,
- Les équipements concernés par l'évènement (source et destination s'il s'agit d'un échange),
- L'action concernée par l'évènement (ex : changement d'un RIB fournisseur),
- Le compte informatique utilisé (ex : compte applicatif, compte administrateur, compte utilisateur),
- L'état de l'action : réussite ou échec.

Afin d'assurer une capacité d'investigation en cas d'incident de sécurité, les traces et les alertes sont conservées pendant une durée maximale de cinq ans, sauf si des dispositions légales ou réglementaires venaient à imposer des délais de conservation plus importants.

Cas particulier des flux internet

Les flux de données en provenance ou vers Internet sont souvent utilisés pour mener des attaques informatiques (prise de contrôle, intrusion, fuite d'information, fraude…).

L'Entreprise met en œuvre un déchiffrement et une analyse automatisée de l'ensemble des flux en provenance ou vers Internet afin de détecter ces attaques. Aucune analyse manuelle ou individuelle de la navigation Internet n'est menée sauf en cas d'alerte sécurité ou d'incident révélé par les outils de détection automatique. De plus, par respect des libertés individuelles, l'ensemble des flux à destination des administrations, des banques et des messageries en ligne ne sont pas déchiffrés.

2.5- Messages électroniques

Les messages électroniques sont, selon la licence d'usage octroyée, archivés pour une durée maximale de 5 ans.

Les demandes d'accès ponctuelles aux messages professionnels font l'objet d'une procédure formelle à ma demande (pour mes propres messages) ou à la demande de mon manager (en mon absence et uniquement afin de ne pas compromettre le fonctionnement des activités). Je suis systématiquement en copie du ou des messages qui ont été transférés.

En cas d'absence prolongée (congés de longue-durée, arrêt de travail), de départ ou de décès, mon manager peut, via une procédure formelle, récupérer une archive contenant mes messages professionnels ou demander la configuration d'un message automatique pour informer les émetteurs de mon indisponibilité et de la nouvelle adresse à contacter.

En respect du secret des correspondances, les messages explicitement marqués comme relevant de ma vie privée (avec la mention « Privé » ou « Personnel ») ne seront pas fournis sauf en ma présence, ou si j'ai été dûment appelé, ou en cas de risque particulier notamment de sécurité, de continuité de service, d'atteinte à l'information ou aux intérêts de l'Entreprise, ou d'un risque grave de voir ma responsabilité engagée.

PARTIE 3 : MA VIE INFORMATIQUE AU SEIN DE L'ENTREPRISE

3.1- J'exerce mon droit d'accès, de rectification, d'opposition et de suppression de mes données personnelles

Conformément à la législation, les traitements de mes données personnelles sont recensés dans un registre interne listant l'ensemble des traitements de données à caractère personnel.

Je peux demander à l'Entreprise de me communiquer toutes les informations me concernant. J'ai le droit de faire rectifier ou supprimer les informations erronées. J'ai également le droit de m'opposer, pour des motifs légitimes à ce que des données à caractère personnel me concernant soient enregistrées dans un fichier informatique, sauf si celui-ci résulte d'une obligation légale ou réglementaire. Ce droit s'exerce auprès de mon Délégué à la protection des données.

3.2- Je suis informé des conditions de retrait de mes accès aux systèmes d'information

L'Entreprise peut être amenée, selon le cas et les circonstances, à restreindre, suspendre ou supprimer mes accès à une ou plusieurs Ressource(s), temporairement ou définitivement, en cas :

- de rupture du contrat de travail pour quelque motif ou quelque cause que ce soit,
- de défaillance technique ou continuité de service,
- d'usage avéré mettant en cause les intérêts, le bon fonctionnement ou la sécurité des systèmes d'information de l'Entreprise,
- de suspension du contrat de travail, de mise à pied conservatoire, de dispense d'activité.

La mise en œuvre de ces mesures s'effectuera, sauf impossibilité ou circonstances particulières, avec mon information et de telle sorte qu'elle n'aura pas pour effet d'entraver l'exercice des mandats électifs, désignatifs ou représentatifs que je possèderais.

A mon départ de l'entreprise, je supprime mes données personnelles de ma messagerie professionnelle et de mes espaces de stockage professionnels (disque U:\ ou Google Drive). Je remets à l'Entreprise le matériel professionnel qui m'a été confié (ordinateur, téléphone, tablette, supports de stockage…) ainsi que l'ensemble de mes données professionnelles (emails, documents…).

3.3- Que se passe-t-il si je ne respecte pas les règles contenues dans ce document ?

Les règles contenues dans ce document sont essentielles au bon fonctionnement et à la sécurité des systèmes d'information de l'Entreprise.

Leur non-respect engage ma responsabilité personnelle et peut entraîner des sanctions de natures différentes, qui ne sont pas exclusives les unes des autres :

- Sanctions disciplinaires prévues par le règlement intérieur du site de rattachement,

- Poursuites civiles et/ou pénales engagées à la demande de l'Entreprise en cas de manquement grave et avéré aux lois en vigueur.

ADOPTION ET PUBLICITÉ DU PRÉSENT DOCUMENT

Ce document a été adopté après information et consultation des instances représentatives du personnel de l'UES Leroy Merlin. Il est applicable à compter du 1er mars 2023.

Le présent document est porté à la connaissance de chaque utilisateur par toute voie jugée nécessaire par l'Entreprise et sous toute forme de communication utile, conformément au code du travail.

Ce document est publié sur le site Intranet de l'Entreprise. Des actions de sensibilisation et de communication sont organisées régulièrement afin de rappeler les règles décrites ici. En cas de questions sur certaines parties du document, je peux contacter à tout moment mon manager ou mon département RH.