Charte Informatique et Sécurité de la Société Manpower France

La présente Charte règlemente l'utilisation du Système d'Information de l'Entreprise. Elle constitue une annexe de son règlement intérieur.

Sommaire

INTRODUCTION

Les données informatisées et, plus généralement, toutes les informations stockées et/ou traitées par Manpower France constituent un élément de patrimoine d'une grande valeur qu'il convient de protéger. L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images), transmise par des réseaux informatiques privés ou Internet, par la poste, oralement et/ou par téléphone,...

L'utilisation de nouvelles technologies et d'Internet constitue pour Manpower France une source de richesse mais l'expose également à des menaces chaque jour plus nombreuses et plus sophistiquées telles que l'intrusion d'un pirate informatique dans le système informatique, la dégradation du site Internet, ou encore la divulgation d'informations confidentielles.

La survenance de tels incidents pourrait causer un préjudice très lourd à Manpower France, notamment parce qu'ils seraient de nature à porter atteinte à sa réputation ou à engager sa responsabilité et pourraient remettre en question la confiance que ses interlocuteurs (candidats, intérimaires, prestataires et clients) lui témoignent.

Pour protéger la confidentialité, l'intégrité et la disponibilité des données et informations traitées/stockées ou détenues par Manpower France, les règles de sécurité raisonnables et pertinentes édictées par la présente Charte doivent être impérativement respectées par tous les Utilisateurs du Système d'Information.

1. DISPOSITIONS GENERALES

LES DISPOSITIONS GENERALES S'APPLIQUENT A L'ENSEMBLE DE LA CHARTE INFORMATIQUE

1.1 Définitions

Les termes spécifiques utilisés dans ce document sont définis ainsi :

« Charte » ou **« Charte Informatique »** : le présent document.

« Direction Informatique » : la DSI (Direction des Systèmes d'Information de Manpower France).

« Entreprise » : Manpower France.

« Ressources » : les Ressources mises à disposition par l'Entreprise se distinguent en 3 catégories :

- les ordinateurs, fixes ou portables, et tout autre matériel informatique, connectique ou bureautique y compris les serveurs, hubs, câbles du réseau, fax, photocopieurs, téléphones, fixes ou portables, tablettes, smartphones …
- les logiciels contenus dans ces matériels ou équipements, et destinés à leur fonctionnement, leur interopérabilité ou leur protection… (les réseaux informatiques et téléphoniques/les protocoles de communication destinés au transport des données et de la voix sont assimilés à des logiciels ; les applications ; les services informatiques) ; et
- les données et informations stockées dans le réseau informatique ou sur tout autre support (ordinateur portable, smartphone ou tout autre appareil portable, CD, DVD, lecteur à mémoire flash, clefs USB, disques durs externes …) y compris papier.

« Système d'Information » : l'ensemble des Ressources.

« Tiers Habilités » : toute personne extérieure à l'Entreprise qui est autorisée à accéder au Système d'Information de l'Entreprise pour des missions et/ou des durées définies, notamment les personnels de prestataires extérieurs (consultants, sous-traitants…), intervenants techniques, auditeurs, commissaires aux comptes, formateurs externes, partenaires commerciaux et clients, ainsi que, le cas échéant, les salariés intérimaires.

« Utilisateurs » : tous les salariés permanents de l'Entreprise (quelque soit la forme ou la durée de leur contrat de travail (CDI, CDD, contrat d'apprentissage, stagiaires …) qui accèdent au Système d'Information, et les Tiers Habilités.

1.2 Champ d'application de la Charte

La Charte s'applique à l'ensemble des Utilisateurs.

1.3 Mise à disposition des Ressources et Privilèges Informatiques

Autorisation d'accès aux Ressources

L'utilisation des Ressources est soumise à autorisation préalable de la Direction de l'Entreprise ou ses délégataires dans ce cadre (Direction des Ressources Humaines, Direction Informatique). Elle se concrétise par l'ouverture d'un compte informatique et/ou téléphonique, la communication d'identifiants de connexion et/ou la mise à disposition de Ressources.

L'utilisation des ressources informatiques sans autorisation et/ou en violation des Privilèges Informatiques accordés peut être assimilée à une intrusion dans le Système d'Information de l'Entreprise, et, à ce titre, sera considérée comme une infraction (Article 323-1 et suivants du Code pénal). Toute personne accédant sans autorisation à des Ressources autres que celles mise à disposition du public par l'Entreprise sera dans ce cas.

Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement, à un tiers.

En cas de non respect de ces règles, la Direction de l'Entreprise se réserve le droit de retirer à tout moment cette autorisation d'utilisation des Ressources, et ce, sans préavis.

Adéquation des Ressources mises à disposition aux besoins professionnels

L'Entreprise met à la disposition des Utilisateurs des équipements informatiques, des moyens de communication ainsi que des informations et données lorsque ces Ressources sont utiles voire nécessaires à l'accomplissement de leur mission. **La mise à disposition des Ressources n'est donc pas uniforme et dépend des besoins professionnels de chaque Utilisateur.**

Adéquation des Privilèges Informatiques aux besoins professionnels

Différents niveaux d'accès aux données (« Privilèges Informatiques ») ont été mis en place afin de protéger les données contenues dans le Système d'Information de l'Entreprise.

Les Utilisateurs ne pourront en aucun cas se voir accorder des Privilèges Informatiques excédant ceux strictement nécessaires à l'accomplissement de leurs fonctions.

Chaque responsable hiérarchique doit s'assurer de l'adéquation des Privilèges Informatiques accordés avec le travail confié à chaque Utilisateur.

La limitation des Ressources et des Privilèges Informatiques de chaque Utilisateurs à ceux qui sont strictement nécessaires à l'exercice de leurs fonctions répond à plusieurs finalités :

- le respect des obligations légales, notamment au regard de la Loi Informatique et Libertés du 6 janvier 1978 modifiée,
- le respect du Code d'éthique et de Déontologie de l'Entreprise,
- la réduction des risques de survenance d'accidents ou d'actes de malveillance, qui peuvent être fortement préjudiciables à l'Entreprise.

Changements dans la situation des Utilisateurs

Chaque responsable hiérarchique doit informer les personnes qui administrent le Système d'Information de tout mouvement de personnel.

1.4 Principes généraux applicables à l'utilisation des Ressources

Seules les Ressources validées et/ou mise à disposition par l'Entreprise doivent être utilisées par les Utilisateurs dans le cadre de leur activité professionnelle.

Toute autre utilisation des Ressources est interdite, sauf utilisation personnelle dans les conditions définies ci-après.

- Il est interdit d'utiliser le Système d'Information pour se livrer à une activité concurrente de celle exercée par l'Entreprise, ou pour mener des affaires pour d'autres sociétés ou personnes.

Tout Utilisateur est responsable de l'usage qu'il fait des Ressources mises à sa disposition.

- Chaque Utilisateur ne doit pas utiliser les Ressources afin de commettre un acte répréhensible, notamment :

    - contrefaçon,
    - diffamation,
    - apologies de crimes de guerre, révisionnisme,
    - racisme,
    - accès à des contenus pédophiles,
    - accès frauduleux à un système informatique, ou
    - tout acte susceptible de porter préjudice à des tiers ou à d'autres Utilisateurs (heurter les susceptibilités personnelles, par exemple confessionnelles, porter

atteinte à la vie privée d'autrui, procéder à des actions de concurrence déloyale ou de dénigrement…).

De plus, il est interdit d'utiliser les Ressources pour :

- accéder à des sites Internet :
    - pornographiques, qui approuvent la violence, les dérives sectaires, l'intolérance, l'abus de drogues / d'alcool, les activités criminelles ou tout autre comportement illégal ;
    - qui permettent ou approuvent les paris ou les jeux d'argent en ligne ;
    - pour télécharger tout fichier (programme, images, photos, musique, film…) étranger aux fonctions exercées au sein de l'Entreprise par l'Utilisateur.
- publier tout document interne à l'Entreprise ou information de l'Entreprise sur un réseau social ou sur tout site Internet autre que le site officiel de l'Entreprise sauf autorisation préalable de cette dernière. Ces documents ou informations doivent être à jour et pertinents. Le cas échéant, la Direction de la Communication, la Direction Marketing et/ou la Direction Juridique pourront identifier au préalable (notamment sur l'Intranet) les documents et information qui peuvent être communiqués à l'extérieur de l'Entreprise.

Enfin, les Utilisateurs ne peuvent stocker ou transmettre, par l'intermédiaire des outils de communication fournis par l'Entreprise :

- des documents sexuellement explicites ou suggestifs ;
- des document qui approuvent le harcèlement ou le dénigrement des personnes basé sur leur sexe, race, orientation sexuelle, âge, nationalité, handicap, leurs croyances religieuses ou leurs opinions politiques ;
- tout document ou élément ayant un caractère diffamatoire, menaçant, injurieux, calomnieux ou portant atteinte à la vie privée d'une autre personne.

Par ailleurs, toute utilisation des Ressources par des personnes autres que les Utilisateurs est strictement interdite, à l'exception des postes libre service définis pour permettre un accès à Internet dans les agences.

Chaque Utilisateur doit prendre soin des Ressources qui ont été mises à sa disposition.

- Lors de l'utilisation des Ressources à l'extérieur des locaux de l'Entreprise, les Utilisateurs sont soumis à une obligation de discrétion et de réserve nécessaire à la préservation de la propriété et de l'intégrité du Système d'Information de l'Entreprise.
- Les Utilisateurs doivent se conformer aux prescriptions techniques et aux recommandations de la Charte, de la Direction Informatique, des constructeurs ou des installateurs des Ressources. Ils doivent utiliser les identifiants et codes d'accès qui leur ont été attribués ou qu'ils ont choisis et les modifier conformément aux instructions de l'Entreprise.

1.5 L'exception d'utilisation personnelle des Ressources

Par exception aux principes des Dispositions Générales (Partie 1), il est rappelé que l'utilisation des Ressources à des fins privées est tolérée si elle reste dans les limites du raisonnable, notamment si elle :

- présente un caractère ponctuel et de courte durée et n'interfère pas avec la capacité de l'Utilisateur à accomplir les tâches attendues,
- n'affecte pas l'activité professionnelle des autres collaborateurs,
- ne provoque pas des ralentissements excessifs du travail ou des détériorations de la performance du Système d'Information pour les autres Utilisateurs,
- n'occasionne ni préjudice, ni embarras pour l'Entreprise.

Les données privées ou personnelles devront être explicitement désignées et il appartient à l'Utilisateur de procéder à cet effet. Tout fichier, dossier ou message qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'Entreprise peut y accéder hors la présence de l'Utilisateur.

L'Utilisateur s'engage à ne pas « transformer » de mauvaise foi des informations professionnelles en personnelles.

L'Utilisateur est invité à effacer toute donnée personnelle avant la fermeture de son compte informatique à son départ de l'Entreprise.

1.6 Accès aux Ressources par l'Entreprise

Les Utilisateurs sont informés que l'Entreprise peut accéder à tout moment aux Ressources qui sont mises à leur disposition, et notamment en cas d'absence, quelqu'en soit le motif (congés, arrêt maladie, décès, départ de l'Entreprise…), et ce, pour la poursuite des activités de l'Entreprise, pour la réalisation d'opérations de maintenance ou en cas de contrôle.

Ces accès seront réalisés dans le respect de la vie privée et du secret des correspondances des Utilisateurs, conformément à la règlementation en vigueur et notamment des dispositions de l'Article 9 du Code civil et 226-15 du Code pénal.

Il est rappelé que le principe du secret des correspondances peut être levé dans le cadre d'une instruction pénale ou par une décision de justice.

1.7 Sanctions

Le non respect de la Charte engage la responsabilité personnelle des Utilisateurs.

- **Le non respect de la Charte expose les Utilisateurs appartenant au personnel de l'Entreprise à l'une des sanctions disciplinaires visées par le règlement intérieur.**

- **Le non respect de la Charte expose les Utilisateurs Tiers Habilités et/ou leur employeur ou commettant à des poursuites judiciaires devant les juridictions civiles et/ou pénales ; de plus, un tel non respect permet à l'Entreprise de résilier immédiatement et de plein droit les contrats en cours avec ces Tiers Habilités, leur employeur ou commettant.**

1.8 Diffusion de la Charte

La Charte est diffusée auprès de tous les Utilisateurs.

- Auprès du personnel permanent de l'Entreprise :

La Charte est remise à tout salarié permanent au moment de son recrutement et demeure accessible à tout moment sur l'Intranet de l'Entreprise.

Elle est également remise à chaque représentant du personnel.

La Charte fait l'objet d'un affichage par l'Entreprise et pourra ainsi être consultée par les Utilisateurs. Un exemplaire est également remis par la Direction des Ressources Humaines à tout salarié qui en ferait la demande.

- Auprès des Tiers Habilités :

Un exemplaire de la Charte leur est remis dans le cadre du contrat de prestation conclu avec le Tiers Habilité ou la société pour laquelle il intervient.

1.9 Informations complémentaires sur la sécurité du Système d'Information de l'Entreprise

La Direction Informatique veille à la protection, à la maintenance et au bon fonctionnement du Système d'Information.

Elle agit en concertation avec les services compétents (Direction des Ressources Humaines, Direction Juridique) afin de se conformer aux dispositions légales, d'effectuer toutes formalités ou déclarations, en particulier celles exigées par :

- la loi 78-17, « Loi Informatique et Libertés » du 6 janvier 1978 modifiée,
- la loi 2004-575, « Loi pour la Confiance dans l'Economie Numérique » du 21 juin 2004,
- les dispositions applicables du Code des postes et des communications électroniques,
- les dispositions relatives aux atteintes aux systèmes de traitement automatisé de données, définies par le Code pénal.

La Direction Informatique se tient à la disposition des Utilisateurs qui sont invités à la contacter pour toutes les questions relevant de la sécurité des données de l'Entreprise.

1.10 Droit d'accès

Conformément à la règlementation en vigueur, les Utilisateurs ont la possibilité de consulter toutes les données à caractère personnel les concernant et que l'Entreprise peut détenir.

A cette fin les Utilisateurs identifiés peuvent contacter le service dédié en adressant une demande mentionnant leurs nom, prénom, matricule, par le moyen de leur choix :

- Par courrier postal à : Manpower France - Droit d'Accès CNIL
  13 rue Ernest Renan – 92723 Nanterre Cedex

- Par courrier électronique à : droitdacces-cnil@manpower.fr

Pour aller plus loin…

- *Privilèges Informatiques*

L'information relative au changement de situation des Utilisateurs a pour but de s'assurer que les niveaux d'accès et les privilèges des Utilisateurs sont strictement adaptés à la nature et au contenu de leurs fonctions ; et que les Utilisateurs dont le contrat ou la mission a pris fin n'ont plus accès au Système d'Information.

- *L'exception d'utilisation personnelle des Ressources*

Conformément à l'état de la jurisprudence, tout fichier, dossier ou message que contiennent les Ressources mis à la disposition des Utilisateurs est présumé être professionnel. Ainsi, l'employeur peut accéder à ces informations hors de la présence de l'Utilisateur, excepté si elles ont été identifiées comme personnelles.
Pour ce faire, l'Utilisateur placera les données personnelles dans un dossier « privé » ou « personnel », ou indiquera « personnel » dans l'objet d'un courrier électronique considéré comme privé.

- *Information et Droit d'accès aux données à caractère personnel*

Les traitements des données à caractère personnel des Utilisateurs sont mis en œuvre conformément à la législation en vigueur.

Une Notice d'information sur les traitements de données est tenue à la disposition des Utilisateurs. Cette Notice d'information détaille notamment les catégories de données traitées, les finalités des traitements de données à caractère personnel mis en œuvre par l'Entreprise, les catégories de destinataires et, le cas échéant, les transferts internationaux de données.

La procédure d'exercice des droits des Utilisateurs est rappelée dans la Notice d'information du personnel permanent de Manpower France sur le traitement des données à caractère personnel ; cette Notice est accessible dans les mêmes conditions que la Charte.

Certaines Ressources peuvent faire l'objet d'une Notice spécifique complémentaire.

2. ACCES AU SYSTEME D'INFORMATION PAR LES UTILISATEURS

2.1 Identifiant Utilisateur

Chaque Utilisateur dispose d'un identifiant unique qui l'authentifie et lui permet d'accéder aux applications du Système d'Information.

L'identifiant peut être composé :

- du *nom d'utilisateur (ou matricule)*, personnel à chaque Utilisateur;
- d'un *mot de passe*.

Les autorisations d'accès sont strictement personnelles et **il est interdit de communiquer à quiconque, de quelque manière que ce soit, son mot de passe**. En effet, toutes les connexions sous l'identifiant de l'Utilisateur sont présumées avoir été réalisées par lui.

2.2 En cas d'absence

Avant un départ en congés, l'Utilisateur est invité à rendre accessibles certaines des informations de sa messagerie ou des fichiers partagés via la délégation (en autorisant un collègue à accéder en lecture à ces données) ou en activant le renvoi des messages vers l'adresse d'un collègue. Aucun système ou application ne justifie la communication du mot de passe.

L'Utilisateur autorise, en cas d'absence imprévue, son supérieur hiérarchique à prendre la main sur le compte de l'Utilisateur pour configurer un message d'absence.

2.3 Sécurisation des mots de passe

Chaque Utilisateur doit veiller à préserver la confidentialité de son mot de passe.

Tous les mots de passe doivent (sous réserve que les moyens informatiques le permettent) :

- comporter au moins 8 caractères,
- être un mélange de caractères alphanumériques (minuscules, majuscules) et caractères spéciaux,
- être modifiés au moins tous les 90 jours,
- être inutilisés pendant au moins 6 itérations,

En cas de compromission avérée ou suspectée, l'Utilisateur doit immédiatement changer son mot de passe.

Après 5 tentatives d'ouverture de session infructueuses, le compte de l'Utilisateur sera désactivé et ne pourra être réactivé qu'à la demande de l'Utilisateur associé à l'identifiant.

3. UTILISATION D'INTERNET

3.1 Navigation sur l'Internet

Seuls ont vocation à être consultés les sites Web présentant un lien direct et nécessaire avec l'activité professionnelle exercée.

Il est rappelé aux Utilisateurs que, lorsqu'ils « naviguent » sur Internet, un identifiant relatif à la Ressource utilisée est **enregistré** (cet identifiant permettant au gestionnaire du site visité de faire le lien avec l'Entreprise). Il conviendra donc d'être particulièrement vigilant lors de l'utilisation d'Internet et à ne pas mettre en danger l'image ou les intérêts de l'Entreprise.

En dehors de ses missions professionnelles, chaque Utilisateur salarié de l'Entreprise s'interdit de fournir son adresse e-mail professionnelle ou ses coordonnées professionnelles sur Internet (blogs, réseaux sociaux, etc…).

3.2 Accès au réseau Wifi Invités

L'Entreprise met à disposition des tiers qui interviennent à Eureka (siège social de l'Entreprise) un réseau Wifi public nommé « Wifi Invités » pour leur permettre d'accéder à Internet au cours de leur mission ou fonction.

Pour se connecter au réseau Wifi Invités, les tiers doivent :

- avoir été identifiés au préalable auprès de la Direction Informatique qui transmet les identifiants nécessaires,
- avoir reçu et respecter les Conditions Générales d'Utilisation du réseau Wifi Invités.

3.3 Accès aux postes de travail et à Internet en agence en Session Invité

L'Entreprise peut mettre à disposition des candidats et des salariés intérimaires dans son réseau d'agence des postes de travail connectés à Internet.

Pour se connecter à une Session Invité, les candidats et salariés intérimaires doivent :

- utiliser la session « libre_service »
- avoir reçu et respecter les Conditions Générales d'Utilisation de Session Invité.

3.4 Usage des réseaux sociaux

Si dans le cadre de ses fonctions l'Utilisateur est amené à utiliser des réseaux sociaux « professionnels » (Viadeo, Linkedin…), l'Utilisateur doit se comporter sur ces réseaux conformément aux directives qui lui sont communiquées par sa hiérarchie et aux recommandations de la Direction de la Communication ou de la Direction Marketing.

Pour aller plus loin…

- *La navigation sur Internet*

Chaque Utilisateur doit avoir conscience que l'usage d'Internet à des fins privées accroit les risques d'altération du Système d'information (infection par des virus informatiques ou autres programmes malveillants, volume accru de courriels indésirables, diminution de la performance du Système d'Information). C'est notamment pour cette raison que cet usage doit rester raisonnable.

De plus, il est rappelé aux Utilisateurs que les données les concernant (sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à leur insu, etc.) peuvent être enregistrées par des tiers, analysées pour en déduire leurs centres d'intérêt, les préoccupations de l'Enterprise, et utilisées à des fins notamment commerciales.

4. UTILISATION DES OUTILS DE COMMUNICATION ELECTRONIQUE

4.1 Conditions générales d'utilisation des outils de communication électronique

L'utilisation de comptes de messageries personnelles est interdite pour la conduite des affaires pour le compte de l'Entreprise.

De plus, à moins que cela ne fasse partie d'une exigence professionnelle comme définie et approuvée par l'Entreprise, **les outils de communication électronique ne doivent pas être utilisés pour** :

- envoyer des messages en masse (courriels indésirables à des adresses aléatoires, parfois appelés « pourriels » ou « spams »).
- lancer ou poursuivre des « chaînes » de messages (c'est-à-dire tout message avec des instructions demandant de le faire suivre à d'autres personnes, ainsi que ceux comprenant les avertissements factices concernant les virus).
- envoyer des messages avec des logiciels exécutables en pièce jointe.
- envoyer des informations pouvant être considérées comme étant confidentielles ou couvertes par un droit de propriété intellectuelle ou industrielle.

Sera également considéré comme fautif :

- le fait d'envoyer des messages sous le nom d'un autre Utilisateur sauf autorisation de celui-ci ou sous un nom d'emprunt quel qu'il soit ;
- le fait d'accéder à des données concernant d'autres Utilisateurs sans leur autorisation, sauf sur autorisation de la Direction des Ressources Humaines ou en cas d'accès par les équipes habilitées de la Direction Informatique pour les opérations de maintenance ou supervision.
- le fait d'utiliser un autre identifiant/mot de passe que le sien.

Par ailleurs, il est strictement interdit qu'un Utilisateur disposant d'une boîte à lettre individuelle attribuée par l'Entreprise (@manpower.fr) en transfère automatiquement le contenu vers une adresse privée.

Enfin, aucun message électronique ne doit être envoyé par un Utilisateur à un destinataire extérieur à l'Entreprise, si l'Utilisateur n'en a pas l'autorité.

4.2 Connexion à des réseaux wifi publics ou semi-publics (nomades)

Lors de leurs déplacements, les Utilisateurs sont invités à se connecter au réseau VPN de l'Entreprise afin de sécuriser les échanges de données (y compris pour accéder à des sites Internet).

4.3 Réseaux et équipements téléphoniques

Les Utilisateurs disposant de matériel type GSM doivent utiliser un code PIN autre que 0000. Ce code devra être restitué à la Direction Informatique en cas de changement ou remise du GSM.

Pour aller plus loin…

Les outils de communication électronique désignent notamment la messagerie électronique ainsi que tous les outils de communication instantanée (Skype, Microsoft Office Comminicator, etc.).

Il est rappelé aux Utilisateurs que la plupart des outils de communication électronique permettent aux participants à tout échange d'enregistrer et de conserver ces échanges.

- *Objectif des règles d'utilisation des outils de communication électronique*

Les règles d'utilisation des outils de communication électronique ont pour but de :

- *Protéger les ordinateurs, les réseaux et les données de l'Entreprise contre tout problème provenant de l'utilisation inappropriée de ses équipements ;*
- *protéger les équipements de l'Entreprise contre toute surcharge d'activité qui n'est pas directement en rapport avec l'activité professionnelle ;*
- *protéger la réputation de l'Entreprise en veillant à ce que des documents ou informations inappropriés ne soient pas diffusés au moyen des équipements fournis par l'Entreprise.*

- *Valeur juridique des courriers électroniques*

Il est rappelé aux Utilisateurs que le courrier électronique (courriel/email) ou le message court (SMS, MMS) est un écrit pouvant engager l'Entreprise et être reconnu comme preuve valable pour établir un fait ou un acte juridique. Les règles hiérarchiques et d'organisation des pouvoirs internes de signature, d'engagement, et de validation doivent être respectées.

- *Connexion à des réseaux wifi publics ou semi-publics (nomades)*

Il est important de rappeler que la connexion d'un PC portable de l'Entreprise, ou de tout autre équipement, à un réseau wifi public (fourni par une ville, un aéroport, hôtel, restaurant,…) ne garantit pas la sécurité des informations qui transitent (sur ces réseaux, il est facile de réaliser des écoutes, de voler les mots de passe,…)

Un réseau VPN (Virtual Private Network) crée un tunnel sécurisé entre le poste de l'Utilisateur et le réseau de l'Entreprise.

5. UTILISATION DES RESSOURCES MATERIELLES

5.1 Fourniture et règles générales d'utilisation

Fourniture et configuration des Ressources matérielles

Les matériels mis à disposition par l'Entreprise sont placés sous la garde des collaborateurs qui en font usage. Leur protection requiert en toute circonstance soin et vigilance. Ils doivent être utilisés conformément à leur usage et maintenus en bon état de fonctionnement.

Tout matériel ne peut être installé et configuré que par les personnes dûment autorisées par l'Entreprise.

L'Entreprise se réserve le droit de désactiver ou de retirer tout matériel.

Lorsqu'un Utilisateur éprouve le besoin de disposer d'un nouveau matériel ou d'utiliser un équipement non standard, il doit solliciter la Direction Informatique et obtenir son autorisation avant toute installation, y compris à titre provisoire, à des fins de démonstration ou d'essai. Aucune modification de ces matériels, de leurs périphériques, ou du réseau de télécommunication qui les met en relation ne peut être effectuée sans l'autorisation expresse de la Direction Informatique ou des personnels habilités.

Par ailleurs, à l'exception des équipements dédiés à une utilisation nomade, les équipements ne doivent pas être déplacés, sans l'intervention de la Direction Informatique.

5.2 Équipements nomades

L'accès au réseau de l'Entreprise (et à tout équipement connecté à ce dernier) à partir d'un lieu éloigné est autorisé au moyen d'outils exclusivement fournis ou approuvés par l'Entreprise.

La Direction Informatique publie les procédures et règles applicables pour se connecter à distance au réseau de l'Entreprise. Ces règles doivent être scrupuleusement respectées par les Utilisateurs.

Dans le cadre de ces procédures d'accès au Système d'information, il peut être utilisé ou demandé des éléments d'identification personnels de l'Utilisateur pour faciliter et/ou authentifier la personne (nom, prénom, matricule, numéro de téléphone, adresse email…) lesquels feront le cas échéant l'objet d'une sauvegarde sécurisée conformément à la réglementation en vigueur.

Afin de protéger le Système d'Information et les données qui y sont stockées contre tout préjudice, vol ou toute utilisation abusive :

- Tous les appareils informatiques portables (tels que les ordinateurs portables, les « smartphones » ou téléphones de dernières générations permettant l'enregistrement de fichiers) doivent être protégés physiquement contre la perte ou le vol.
- Les Utilisateurs doivent s'assurer que leurs appareils sont sécurisés physiquement chaque fois qu'ils sont laissés sans surveillance.
- Cette sécurisation peut être réalisée grâce à une station d'accueil susceptible d'être verrouillée, à un câble antivol correctement fixé ou au rangement dans un tiroir ou un classeur à tiroirs fermé à clé.
- Les Utilisateurs ne doivent jamais laisser les appareils informatiques ou téléphoniques portables sans surveillance dans les lieux publics.
- Le vol ou la perte d'appareils informatiques doit être immédiatement signalé auprès du service support informatique de l'Entreprise (Helpdesk), de son supérieur hiérarchique. Le cas échéant, il peut être demandé à l'Utilisateur de fournir copie du procès verbal de perte ou vol. Dans le cas d'un vol du smartphone fourni par l'Entreprise, la procédure d'effacement des données à distance doit être déclenchée sur l'application de messagerie accessible depuis Internet dans les plus brefs délais.

5.3 Protection des systèmes inactifs ou laissés sans surveillance

Les Utilisateurs sont invités, en cessant l'utilisation d'une Ressource, éteindre, déconnecter ou verrouiller celle-ci et, en tout état de cause, ne pas empêcher sa mise en veille automatique.

L'Utilisateur doit systématiquement verrouiller son poste de travail par toute méthode en vue d'en empêcher l'accès à tout utilisateur non autorisé (économiseur d'écran).

Les Utilisateurs doivent également fermer les sessions des systèmes et des applications chaque fois qu'elles ne sont pas utilisées pendant une longue durée.

Les fermetures de sessions doivent au minimum avoir lieu à la fin de chaque journée de travail.

Les règles de fermeture de session figurent dans le manuel d'utilisation de chaque Ressource.

Pour aller plus loin…

- *Utilisation des supports amovibles*

Les supports amovibles de mémoire (clé usb, disque dur externe, carte mémoire flash…) constituent un vecteur très important de transmission des virus et impliquent lors de leur utilisation la vérification de leur contenu. Leur usage doit être limité aux échanges avec l'extérieur. La messagerie et les espaces d'échanges mutualisés (partages réseau, Sharepoint,…) doivent être préférés pour les échanges internes.

- *Equipements nomades*

Afin de prévenir les risques de vol des équipements nomades, chaque Utilisateur est invité à :

- *Ne pas laisser les appareils portables sans surveillance dans son bureau ou dans les locaux de clients, prestataires ou tout autre Entreprise à moins qu'ils ne soient convenablement sécurisés au moyen d'un câble antivol ou d'un autre mécanisme.*
- *S'assurer qu'en cas d'utilisation d'un câble antivol, celui-ci est attaché à un objet fixe qui ne peut être facilement déplacé, soulevé ou volé avec l'ordinateur.*

Par ailleurs, en cas de voyage à l'étranger (notamment aux Etats-Unis), les services de douanes peuvent avoir le pouvoir de conserver, de manière discrétionnaire, tout équipement informatique ou téléphonique susceptible de conserver des données informatiques. Ainsi, les Utilisateurs sont invités à se renseigner et à suivre les recommandations de la Direction Informatique avant tout voyage à l'étranger, et notamment sur l'opportunité d'emporter les équipements fournis par l'Entreprise.

- *Protection des systèmes inactifs ou laissés sans surveillance*

Dans le but de protéger la confidentialité et l'intégrité des données, l'accès au réseau est automatiquement fermé lorsque la station de travail est inactive pendant une certaine durée (time out). Le paramétrage de cette fonction est de la responsabilité de la Direction Informatique. Il ne peut en aucun cas être modifié ou annihilé par l'Utilisateur.

NB : *Le contenu du manuel de chaque Ressource est porté à la connaissance de l'Utilisateur au travers d'une aide en ligne ou de tout moyen approprié.*

6. UTILISATION DES LOGICIELS

6.1 Logiciels fournis par l'Entreprise

Seuls les logiciels ayant été approuvés par l'Entreprise et pour lesquels elle dispose des droits d'utilisation peuvent être installés dans le Système d'Information.

Les développeurs peuvent néanmoins, dans le cadre de leur mission, être amenés à utiliser des programmes non fournis par l'Entreprise. Ils doivent au préalable demander l'accord du service d'architecture logicielle de la Direction Informatique.

Les logiciels sont protégés par les lois relatives à la propriété intellectuelle ou au copyright. **Les licences relatives à tous les logiciels fournis par l'Entreprise sont la propriété de l'Entreprise.** Les Utilisateurs ne peuvent utiliser les logiciels que dans les limites et les conditions stipulées par l'Entreprise.

Seuls les techniciens chargés des installations de logiciels sont autorisés à réaliser ou distribuer des copies des logiciels fournis par l'Entreprise.

La désinstallation, sur l'initiative d'un Utilisateur, d'un logiciel mis en place sur son poste de travail, quelle qu'en soit la nature et la finalité, est strictement interdite. De même, la modification, sur l'initiative d'un Utilisateur, des paramètres de sécurité d'un logiciel installé sur un poste de travail est strictement interdite.

Par ailleurs, pour des raisons liées à l'accomplissement des missions qui leurs sont confiées, les collaborateurs de la Direction Informatique sont habilités, après approbation de leur hiérarchie et sous le contrôle de celle-ci, à installer sur leur poste de travail des configurations logicielles non standard. Cette éventualité ne doit en aucun cas affecter les logiciels de sécurité standards installés sur les stations de travail.

6.2 Services applicatifs en ligne

L'Entreprise peut concéder à des Utilisateurs des codes d'accès leur permettant d'accéder à des services en ligne. Ces services peuvent être associés – ou non – à des comptes personnels de l'Utilisateurs.

Lors de l'usage de services en applicatifs en ligne, l'Utilisateur est invité à se conformer aux instructions de configuration et d'utilisation qui lui sont communiquées par l'Entreprise. En cas de besoin, les Utilisateurs sont invités à se tourner vers les services d'assistance mis en œuvre par l'Entreprise.

En cas de départ de l'Entreprise, l'Utilisateur doit restituer à l'Entreprise les codes d'accès à ces services et cesser d'utiliser les services correspondants.

Pour aller plus loin…

- *Objectif des règles d'utilisation des logiciels*

Ces règles permettent d'empêcher que les Utilisateurs ne violent les termes et conditions stipulées dans les contrats de licence d'Utilisateur final des logiciels fournis par l'Entreprise.

L'installation sur plusieurs ordinateurs d'un logiciel doté d'une licence pour un seul Utilisateur, les copies de logiciels sans permission expresse ou l'utilisation d'un logiciel sans licence valable pour la version utilisée constituent tous des exemples de violation des lois relatives à la propriété intellectuelle.

La violation de la licence peut avoir pour conséquences la perte d'utilisation, la confiscation de l'équipement, ou des sanctions pénales et civiles (dommages et intérêts, amendes, prison).

7. UTILISATION DE L'INTRANET

Mise en place et Fonctionnement

Aucun Utilisateur ne peut introduire ou tenter d'introduire un élément de contenu sur l'Intranet sans l'autorisation préalable de la Direction habilitée à cet effet. Les Utilisateurs peuvent formuler toute suggestion aux services compétents quant au contenu ou fonctionnement de l'Intranet.

8. UTILISATION DE MATERIEL EXTERNE

Généralités

La connexion d'un matériel externe (personnel ou n'appartenant pas à l'Entreprise) au réseau de l'Entreprise (en Wifi ou Ethernet) non validée par la Direction Informatique est interdite.

En revanche, il est possible de se connecter aux applications de l'Entreprise accessibles depuis Internet à partir d'équipements externes (PC personnel, smartphone, tablette, PC externe,…).

La connexion de médias amovibles personnels (clés ou disques durs USB, mémoire flash,…) sur des postes de travail de l'Entreprise est tolérée pour des besoins professionnels seulement.

Stockage de données

La synchronisation de la messagerie de l'Entreprise sur un smartphone (ou tablette) personnel ou externe via Internet est soumise à des conditions précises :

- Le stockage d'Informations Confidentielles et d'Informations à Diffusion Restreinte n'est pas autorisé ;
- La durée de conservation des messages dans les paramètres de synchronisation doit être définie au maximum à 7 jours pour limiter les données de l'Entreprise sur l'équipement ;
- L'équipement personnel :
    - doit être protégé par un mot de passe d'au moins 6 caractères.
    - doit être à mis à jour régulièrement (correctifs de sécurité)
    - doit permettre l'effacement à distance de ses données (cas des smartphones et tablettes)
    - doit être équipé d'un antivirus à jour (a minima sur Android)
    - ne doit pas avoir été « jailbreaké » (débridé) pour installer une version non supportée du système d'exploitation
    - doit supporter le chiffrement des données
    - ne doit pas être prêté à des tiers
- L'Utilisateur accepte le risque d'effacement total des applications et données à distance de son équipement personnel pour protéger les données de l'Entreprise. Il est seul responsable de la sauvegarde de ses données personnelles.

Dans le cas où le smartphone n'est plus la propriété de l'Utilisateur (restitution, vente,…) ou dans le cas où l'Utilisateur quitte l'Entreprise, les données de l'Entreprise pouvant se trouver sur le téléphone doivent être supprimées (contacts, messages,…).

Dans le cas où un smartphone (ou tablette) personnel ou externe est volé ou perdu, l'incident doit être signalé à la Direction Informatique dans les délais les plus brefs et l'effacement des données à distance doit être déclenché sur l'application de messagerie accessible depuis Internet.

Le stockage de données de l'Entreprise sur tout autre matériel personnel ne respectant pas ces conditions est interdit.

9. PROTECTION ET CONFIDENTIALITE DES INFORMATIONS

Toutes les informations traitées ou conservées par l'Entreprise sont classées en trois catégories, selon leur degré de confidentialité. A chaque catégorie correspond un régime particulier de protection que les Utilisateurs doivent respecter.

Ces mesures de protection s'appliquent à toutes les informations, qu'elles figurent sur des documents originaux ou des copies.

En cas de doute sur la catégorie de rattachement d'une information, les Utilisateurs sont invités à consulter la Direction Juridique.

Les définitions ci-dessous offrent une vue élargie des différences entre les catégories :

Catégorie « Informations Confidentielles »

Il s'agit de données :

- présentant un caractère confidentiel ou sensible ; ou
- dont l'accès n'est autorisé qu'aux personnes ayant à en connaître dans le cadre de leur activité ; ou
- dont la divulgation peut entraîner la mise en jeu de la responsabilité civile et /ou pénales de l'Entreprise (notamment pour violation de la vie privée).

Le régime de protection minimal à respecter pour cette catégorie de données est le suivant :

- Toutes les Informations Confidentielles contenues dans un équipement informatique portable (tel que ordinateur portable, smartphone…) doivent être chiffrées ;
- Les Informations Confidentielles ne doivent pas être stockées sur des média amovibles (tels que CD, DVD, bandes, clé USB, disque dur, mémoires flash…) ;
- La divulgation d'Informations Confidentielles en dehors de l'Entreprise est interdite sauf autorisation personnelle expresse (par exemple, prévue par une procédure légale, ou par un document contractuel conclu par l'Entreprise avec ses clients ou partenaires, ou par une procédure validée par l'Entreprise) ;
- Dans tous les cas, la divulgation d'Informations Confidentielles n'est autorisée que si elle est strictement nécessaire ;
- Lorsqu'ils ne sont plus utilisés, les supports contenant des Informations Confidentielles doivent être détruits ou stockés de manière sécurisée.

Catégorie « Informations Internes »

Il s'agit d'informations consultables par n'importe quel employé de l'Entreprise mais non diffusable à l'extérieur.

Le régime de protection minimal à respecter pour cette catégorie de données est le suivant :

- Ces informations ne nécessitent pas de précaution particulière lorsqu'elles sont manipulées à l'intérieur de l'Entreprise ;
- Lorsque des motivations professionnelles l'exigent, contact avec un fournisseur par exemple, elles peuvent être diffusées à l'extérieur de l'Entreprise. Toutefois des précautions doivent être prises pour éviter leur divulgation à des personnes non autorisées à l'extérieur de l'Entreprise.

Catégorie « Informations Publiques »

Il s'agit d'informations disponibles pour le grand public.

Il n'y a pas de précautions particulières requises pour la manipulation de ces informations. Elles peuvent être diffusées à l'extérieur.

Chiffrement des informations[1] :

Tant pour des raisons de sécurité du Système d'Information que pour la confidentialité des informations :

- Il est interdit de stocker des fichiers ayant été chiffrés avec un logiciel de chiffrement non fourni ou approuvé par la Direction Informatique ; il est également interdit d'utiliser une clé de chiffrement non fournie par la Direction Informatique.

- Si un Utilisateur est contraint d'adresser à l'extérieur des informations à caractère confidentiel, stratégique ou sensible, outre la signature préalable d'un engagement de confidentialité conforme aux règles imposées par la Direction Juridique de l'Entreprise, l'Utilisateur devra demander au responsable de la sécurité des systèmes d'information de l'assister pour le chiffrement de l'information.

Pour aller plus loin…

- *Objectif des règles de protection des informations*

Les règles de protection des informations appartenant à l'Entreprise sont un moyen de permettre aux Utilisateurs d'en préserver la confidentialité, l'intégrité et la disponibilité.

En outre, l'Entreprise peut avoir des obligations contractuelles à l'égard de ses clients afin de conserver en sécurité de telles informations.

Les Utilisateurs doivent respecter ces règles afin de prévenir notamment le vol, ou la simple perte des informations. De cette manière, la vie privée des salariés, partenaires et clients est protégée, et il en est de même de la réputation et de l'image de l'Entreprise.

- *Exemples pour chaque catégorie de données*

  - *Constituent des informations confidentielles :*

    - *les données à caractère personnel suivantes des salariés de l'Entreprise : numéro de sécurité sociale, numéro de passeport, date de naissance, numéro national d'identité, numéro de permis de conduire, numéro de compte en banque, numéro de téléphone, salaire, avantages professionnels, adresses physiques ou e-mail, formation, compétences, références et évaluations professionnelles, l'expérience professionnelle, les préférences relatives au travail, les prétentions salariales, les CV ;*
    - *les informations concernant la sécurité interne tel que le paramétrage des firewalls ou d'autres équipements.*
    - *les informations personnelles appartenant à des personnes travaillant pour des clients, ou des fournisseurs telles que des coordonnées, données concernant les conditions de facturation ou de taxation ;*
    - *les informations concernant les produits, les procédés, les ventes et le marketing, des données techniques, des secrets commerciaux, des brevets et des inventions, des données relatives à la connaissance des clients, des données financières, des prix, des remises ou des ristournes, des propositions commerciales.*

  - *Constituent des informations internes :*

    - *Les lettres d'information de l'Entreprise ou d'une Direction ;*
    - *L'Annuaire des lignes téléphoniques directes.*

  - *Constituent des Informations Publiques :*

    - *La liste téléphonique des agences et autres bureaux ;*
    - *La communication institutionnelle de l'Entreprise et du Groupe ;*
    - *Les communications publicitaires ;*
    - *Les conditions générales de ventes (ex. : verso des contrats de mises à disposition).*

Lors de l'utilisation d'outils externes (tels que outils de communications en ligne), les Utilisateurs sont invités à bien identifier la catégorie des informations qu'ils manipulent et qu'ils peuvent être amenés à communiquer et/ou à partager.

[1] Le chiffrement est une opération qui consiste à transformer un message à transmettre inintelligible pour un tiers, n'ayant pas la clé.

10. PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS

Il est strictement interdit d'introduire sciemment dans le Système d'Information des codes informatiques conçus pour entraver le fonctionnement, les performances ou l'accès au Système d'Information (par exemple : virus informatiques, vers, chevaux de Troie et autres programmes malveillants).

Par ailleurs, les Utilisateurs ne doivent en aucun cas diffuser des virus ou des messages d'avertissement concernant des programmes malveillants auprès d'autres individus, en particulier par l'intermédiaire de la messagerie électronique.

10.1 Logiciel anti-virus

Les postes de travail sont équipés de logiciels antivirus à jour fournis ou approuvés par l'Entreprise. Afin de garantir leur efficacité, les Utilisateurs doivent veiller à :

- ce que les logiciels antivirus soient toujours actifs ;
- les utiliser pour détecter la présence d'un virus lorsque celui-ci est suspecté ;
- signaler immédiatement à la Direction Informatique tout problème lié soit à la détection, soit l'éradication des virus (securite.dsi@manpower.fr) ;
- se conformer immédiatement à toutes les directives communiquées par le personnel autorisé de l'assistance technique en vue de limiter, réparer ou prévenir une infection par un virus informatique.

L'installation d'autres logiciels antivirus non fournis ou non approuvés par l'Entreprise est interdite, cette installation pouvant provoquer d'autres problèmes, notamment des conflits sur le système, une baisse de performance du système, et des pannes inopinées.

L'Utilisateur vérifiera, à l'aide de l'antivirus mis à disposition, le contenu de tout support mobile de stockage qu'il est amené à connecter ou à lire avec son ordinateur (CD, DVD, clé USB, disque dur, lecteur MP3, carte mémoire flash,…).

10.2 Application des corrections du système de sécurité

La sécurité du système implique une mise en œuvre régulière des correctifs de sécurité et des mises à jour de l'antivirus.

Les Services de la Direction Informatique sont en charge de tester et vérifier ces correctifs et mises à jour, et notamment leur compatibilité avec les logiciels déployés.

En aucun cas les Utilisateurs ne doivent télécharger des correctifs ou des mises à jour provenant de toute autre source que le réseau de l'Entreprise.

11. SIGNALER LES INCIDENTS DE SECURITE

Tout incident réel ou suspecté relatif à la sécurité des informations doit être signalé sans délais par l'Utilisateur à la Direction Informatique (securite.dsi@manpower.fr) et à son supérieur hiérarchique immédiat. Il en va de même des comportements suspects d'un programme ou d'une application ou si l'Utilisateur pense avoir été victime d'ingénierie sociale.

Pour aller plus loin…

- *Objectif de l'alerte d'incidents de sécurité*

Le recueil des rapports d'incidents de sécurité réels ou suspectés peut permettre de détecter une activité malveillante et réduire le risque d'incident de sécurité pour l'Entreprise. Les retards de signalement peuvent entraîner des pertes supplémentaires pour l'Entreprise.

- *Règles de prudence et de vigilance*

Certains pirates informatiques se font passer pour des membres de l'Entreprise pour solliciter des renseignements qui peuvent ensuite être employés pour attaquer ou compromettre d'une manière ou d'une autre les systèmes.

*Ces techniques, appelée **« ingénierie sociale »** consistent à manipuler les Utilisateurs pour obtenir des informations nécessaires pour forcer les systèmes de sécurité informatique de l'Entreprise. Par conséquent, les Utilisateurs devront se montrer vigilants et ne communiquer aucun renseignement concernant le Système d'Information (et notamment des informations relatives aux modalités d'accès, fonctionnement du Système d'Information) par quelque moyen que ce soit (courriel, téléphone...) sauf si l'identité de la personne qui les demande a été vérifiée, s'il est établi qu'elle a une raison valable de les connaître et si elle est autorisée à les recevoir. Il est de même pour toute information ou donnée contenu dans le Système d'Information, celles-ci devant être manipulées conformément aux règles d'utilisation définies au Chapitre « Protection des informations » de la Charte.*

12. CONTROLES

Dans le seul but de protéger son Système d'Information et pour s'assurer du respect des dispositions de la Charte par les Utilisateurs, l'Entreprise procèdera à des contrôles. A ce titre, l'Entreprise pourra exercer un contrôle général :

- des équipements matériels connectés et/ou utilisés pour accéder au Système d'Information,
- des logiciels installés sur les équipements mis à disposition des Utilisateurs,
- de l'utilisation d'Internet

12.1 Principes

La nécessité de protéger l'Entreprise et son Système d'Information, particulièrement lorsque des indices sérieux et concordants permettent d'identifier l'existence d'une utilisation illicite ou frauduleuse contraire aux prescriptions de cette Charte, justifient les dispositions qui suivent, dans le respect du principe de proportionnalité de l'article L.1121-1 du Code du travail. Ces dispositions visent également à rendre impossible ou à faire cesser toute infraction aux lois et règlements commise avec les Ressources de l'Entreprise.

12.2 Filtrage

L'Entreprise met en place des systèmes de protection spécifiques qui ont pour objectif de :

- protéger les données du Système d'Information;
- sécuriser le serveur et les postes informatiques des virus et tous programmes malveillants circulant sur Internet et d'autres programmes dont l'installation ou l'utilisation présente un risque pour l'Entreprise ;
- respecter les obligations légales de l'Entreprise et des Utilisateurs concernant les activités illégales et/ou contraires à l'intérêt collectif des Utilisateurs telles que l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, la pornographie, la pédophilie…

Ces systèmes **enregistrent et stockent l'ensemble des connexions effectuées** (« Logs ») par les Utilisateurs du Système d'Information, et notamment Internet, et **identifient les sites consultés par eux**.

Les systèmes de protection pourront identifier et bloquer automatiquement toutes les tentatives d'accès et d'utilisation de certains services et/ou sites en raison de leur nature ou des modalités de fourniture de ces derniers.

La Direction Informatique peut, après vérification et sur demande d'un Utilisateur compte tenu de la nature de ses fonctions et/ou des tâches à réaliser, débloquer les accès à certains sites ou services.

Le seul fait, pour un Utilisateur, de tenter d'accéder en vain à une page Web dont l'accès n'est pas permis par le système de protection n'est pas en soi susceptible de faire l'objet d'une quelconque mesure disciplinaire.

12.3 Informations objet des contrôles

Au sein de l'Entreprise, toute opération est susceptible de déclencher l'enregistrement :

- de l'heure de la connexion ;
- de l'identifiant de l'Utilisateur ayant déclenché l'opération ;
- de l'identification de l'équipement à partir duquel a eu lieu la tentative d'accès à un site bloqué ;
- du système auquel il est accédé ;
- du type de transaction réalisé (copie, impression, transfert vers une autre machine, etc.) ;
- de la durée de la connexion, le cas échéant de son coût ;
- des tentatives infructueuses notamment celles concernant les opérations interdites.

Ces enregistrements permettent d'analyser les traces à fin d'études statistiques et de surveillance du Système d'Information et peuvent permettre d'identifier notamment :

- la liste des applications les plus sollicitées et/ou la liste des sites Internet les plus visités ;
- les temps de connexion et la fréquence des connexions,
- le nombre de messages émis et reçus classés par volume et par nature des pièces associées ;
- le coût des connexions le cas échéant ;
- les causes et les conditions de toute violation et/ou utilisation non autorisé du Système d'Information.

L'Entreprise peut également avoir recours à des moyens électroniques pour effectuer un inventaire de tous les programmes informatiques présents sur tout ordinateur ou équipement connecté au réseau de l'Entreprise.

Les informations objet des contrôles sont conservées pour une durée conforme aux lois et réglementations en vigueur.

12.4 Réalisation des contrôles et enquête personnalisée

La Direction Informatique est habilitée à prendre connaissance de tous les dossiers, fichiers, messages, informations système ou de journalisation contenues dans le Système d'Information, sous réserve des dispositions spécifiques aux éléments identifiés comme personnels.

Lorsqu'à l'occasion de ses activités de surveillance du bon fonctionnement des Ressources ou d'un contrôle effectué dans les conditions ci-dessus, le service informatique décèle des éléments permettant d'identifier une utilisation non conforme, illicite ou frauduleuse, ou susceptible de causer un préjudice à l'Entreprise ou à un tiers, il en informe les Directions compétentes, notamment Direction des Ressources Humaines, Direction Juridique, Direction Générale.

Informée, la Direction compétente, en lien avec la Direction des Ressources Humaines, peut décider, à la vue des éléments obtenus a priori, soit de s'en contenter si elle les trouve suffisants, soit de procéder à une enquête personnalisée visant certaines Ressources et/ou certains Utilisateurs.

La présente Charte autorise l'Entreprise à procéder à une telle enquête personnalisée dans la mesure où :

- celle-ci est justifiée par les éléments obtenus a priori par l'Entreprise, et
- le ou les Utilisateurs concernés ont été informés et/ou invités à participer à celle-ci.

En cas de refus ou d'impossibilité d'un Utilisateur de participer à cette enquête, ou si le contexte ne lui permet pas de participer à celle-ci, l'Entreprise pourra y procéder sans son consentement, voire en son absence. Par ailleurs, l'Entreprise pourra procéder à la mise sous séquestre d'une Ressource avec le concours d'un huissier le cas échéant, ou d'un représentant du personnel, conformément à la réglementation en vigueur.

La Direction des Ressources Humaines est en charge de la définition des procédures applicables dans ces cas d'enquête personnalisée, dans le respect de la règlementation en vigueur et de la jurisprudence.

12.5 Intervention en cas d'urgence

En cas de nécessité, et notamment d'urgence, le service informatique est autorisé à prendre toute mesure de nature à faire cesser un trouble manifestement illicite à la sauvegarde des données ou à la notoriété de l'Entreprise. Par ailleurs, la Direction Informatique pourra prendre toute mesure de nature à garantir la sauvegarde et l'intégrité des Ressources, y compris pour écarter toute suspicion de modification d'un élément qui pourrait être retenu contre un Utilisateur.

Le personnel de l'Entreprise en charge de ces contrôles est soumis à une obligation stricte de confidentialité en ce qui concerne le contenu de tous dossiers, fichiers ou messages auxquels il peut accéder. En tout état de cause, ce personnel est soumis à une obligation de discrétion sur l'ensemble des éléments qui lui serait connu du fait de l'exercice de ses missions. A ce titre, ce personnel ne portera les informations connues du fait de ces contrôles qu'à la connaissance de ses supérieurs hiérarchiques, de la Direction des Ressources Humaines, de la Direction Juridique et/ou aux autorités compétentes (justice/police).

Manpower

13. DISPOSITIONS FINALES

La présente Charte est annexée au règlement intérieur du personnel Permanent de Manpower France.

Elle a été soumise à l'avis du Comité Central d'Entreprise ainsi qu'à l'avis des membres des CHSCT pour les dispositions relevant de leurs compétences.

La présente Charte est soumise aux mêmes procédures de consultation, de communication, de publicité et de dépôt que celles du règlement intérieur.

Toute modification ultérieure serait, conformément au Code du Travail, soumise à la même procédure.

L'entrée en vigueur de la présente Charte est fixée au 8 décembre 2014.

Fait à Nanterre, le 24 octobre 2014.

Jean- François TOUSCHE
Directeur des Ressources Humaines