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

1. 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 constituent pour l'Entreprise une source de richesse mais l'expose également à des menaces, chaque jour, plus nombreuses et plus sophistiquées.

Ainsi, l'intrusion d'un pirate informatique dans le système informatique, la dégradation du site Internet, la divulgation d'informations confidentielles sont autant de risques rendus possibles par l'utilisation de nouvelles technologies et d'Internet au sein de l'Entreprise.

La survenance de tels incidents pourrait causer un préjudice très lourd à l'Entreprise, 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 clients* lui témoignent.

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

* Par client il faut entendre : candidats, intérimaires et entreprises clientes.

2. DISPOSITIONS GENERALES

2.1 Champ d'application de la Charte – Définitions

On entend par « Utilisateurs »,

- Tous les collaborateurs permanents de l'Entreprise (quelque soit la forme ou la durée de leur contrat de travail (CDI, CDD, contrat d'apprentissage...)

- Tous les tiers habilités à accéder aux Systèmes d'Information de l'Entreprise pour des missions définies et des durées limitées (stagiaires, personnel de prestataires extérieurs (dont consultants, sous-traitants...), personnel intérimaire en cas de recours exceptionnel, intervenants techniques, auditeurs et commissaires aux comptes, formateurs externes, partenaires commerciaux, clients...), ci-après les « Tiers Habilités »

  La Charte ne s'applique pas, en principe, aux collaborateurs intérimaires mis à disposition de ses clients par l'Entreprise, sauf si un tel intérimaire répond à la définition d'Utilisateur ci-dessus.

On entend par « Ressources »,

- 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, organiseurs...

- les logiciels contenus dans ces matériels ou équipements, et destinés à leur fonctionnement, leur interopérabilité ou leur protection.... (les protocoles de communication destinés au transport des données et de la voix sont assimilés à des logiciels).

- les données et informations stockées dans le réseau informatique ou sur tout autre support (ordinateur portable, assistant numérique personnel ou tout autre appareil portable, CD, lecteur à mémoire flash ...) y compris papier.

L'ensemble des Ressources est dénommé « Système d'Information » de l'Entreprise

2.2 Mise à disposition des Ressources et Privilèges Informatiques

Adéquation des Ressources mises à disposition aux besoins professionnels

Manpower France 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

En outre, 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 accordés avec le travail confié à chaque Utilisateur.

La limitation de l'accès des Utilisateurs aux données et moyens informatiques qui sont strictement nécessaires à l'exercice de leurs fonctions réduit ainsi les risques de survenance d'accidents ou d'actes de malveillance, qui peuvent être fortement préjudiciables à l'Entreprise.

Changements Intervenants dans la situation des Utilisateurs

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

Les Privilèges Informatiques accordés à ces Utilisateurs seront rapidement modifiés conformément aux changements intervenus dans la situation des Utilisateurs.

L'objectif de cette politique est 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 a pris fin, n'ont pas accès au Système d'Information de Manpower France.

2.3 Principes généraux applicables à l'utilisation des Ressources Informatiques

Les données, les logiciels et les ressources du réseau informatique de Manpower France sont mis à la disposition des Utilisateurs par l'Entreprise dans un but exclusivement professionnel.

- **Toute autre utilisation des données, logiciels et des ressources du réseau informatique est interdite, sauf utilisation personnelle limitée.**

  Il est notamment interdit, sauf utilisation personnelle limitée, d'utiliser les équipements de stockage du Système d'Information de l'Entreprise (poste de travail, réseaux centraux, supports externes...) pour conserver des données personnelles (notamment : photos, musique, vidéos ou toute autre donnée qui n'est pas directement en rapport avec l'activité professionnelle exercée pour le compte de Manpower France et / ou du Groupe ou de ses partenaires commerciaux....).

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

- Par ailleurs, il est interdit d'utiliser le Système d'information de Manpower France 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, ou qu'il permet de faire, 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, commerce de toute sorte...) 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...)

- Par ailleurs, toute utilisation du Système d'Information de l'Entreprise (notamment le réseau, les données qui y sont stockées, les logiciels de l'Entreprise) par des **personnes autres que les Utilisateurs** est strictement interdite.

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'Informations de l'Entreprise.

- Les Utilisateurs doivent se conformer aux prescriptions techniques et aux recommandations 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.

2.4 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 ou leur employeur ou commettant à des poursuites judiciaires diligentées par l'Entreprise en réparation de son préjudice.**

2.5 Diffusion de la Charte

La Charte est diffusée auprès de tous les Utilisateurs du Système d'Information.

- Auprès du personnel permanent de l'Entreprise :

  La Charte est communiquée à l'ensemble du personnel permanent de l'Entreprise et demeure accessible à tout moment sur l'Intranet de l'Entreprise. Elle est remise à tout employé au moment de son recrutement.

  La Charte pourra être consultée sur les panneaux d'affichage de l'Entreprise. Un exemplaire est également remis par la Direction des ressources humaines à tout employé 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.

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

La Direction du Système d'Information de Manpower France (« DSI ») veille à la protection, à la maintenance et au bon fonctionnement du Système d'Information. Elle acquiert, pour le compte de l'Entreprise, les droits d'usage ou de propriété intellectuelle des logiciels nécessaires au fonctionnement du Système d'Information.

Elle agit en concertation avec les services compétents afin de se conformer aux dispositions légales, d'effectuer toutes formalités ou déclarations, en particulier celles exigées par la Loi Informatique et Libertés du 6 janvier 1978.

Elle 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.

3. ACCES AU SYSTEME D'INFORMATION PAR LES UTILISATEURS

3.1 Identifiant Utilisateur

Chaque Utilisateur dispose d'un identifiant unique pour accéder à chaque application du Système d'Information de Manpower France.

Cet identifiant permet d'authentifier chaque Utilisateur lors de sa connexion au Système d'Information.

Les identifiants communs à usage générique, partagé ou temporaire sont en principe interdit sauf dérogation accordée par la Direction du Système d'Information.

L'identifiant permet également d'identifier un Utilisateur qui utilise telle ou telle Ressource du Système d'Information de Manpower France, ce qui implique que **chaque Utilisateur pourra être tenu responsable de toute opération effectuée au moyen de son identifiant.**

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

L'association du nom d'utilisateur (ou matricule) et du mot de passe permet d'accéder au Système d'Information de Manpower France.

Chaque Utilisateur, est personnellement responsable de toutes les actions effectuées avec son identifiant. Par conséquent,
- Il est recommandé à l'Utilisateur de ne pas divulguer son nom d'utilisateur, sauf si celui-ci est demandé par le personnel autorisé de Manpower France (soit l'administrateur ou la Direction du Système d'Information) pour la réalisation de tâches administratives ou de maintenance informatique.
- Par ailleurs, **il est interdit de communiquer à quiconque et de quelque manière que ce soit, son mot de passe.**

3.2 Sécurisation des mots de passe

- Chaque Utilisateur doit avoir conscience que le mot de passe constitue le moyen de protection le plus important dont dispose l'Entreprise pour protéger l'accès à ses données contre les utilisateurs non autorisés et les tiers non habilités.
- Il est en fin de compte, l'ultime élément qui protège les informations confidentielles d'un utilisateur non autorisé.
- Par ailleurs, chaque Utilisateur ne doit jamais oublier qu'il pourra être tenu responsable des actions réalisées avec son identifiant.

Précautions de base

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

L'Utilisateur ne doit en aucun cas communiquer son mot de passe (même par souci de politesse, ou de gain de temps.

Tous les mots de passe doivent,

- comporter au moins 6 caractères
- être un mélange de caractères alphanumériques
- être modifiés au moins tous les 60 jours
- être inutilisés pendant au moins 6 itérations,

sous réserve que les moyens informatiques le permettent

Si l'utilisateur suspecte à tort ou à raison que son mot de passe est compromis, il 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.

Précautions supplémentaires

Les mots de passe doivent être mémorisés.
Ils ne doivent pas être écrits sur un document, ni prononcés à voix haute.

Si l'Utilisateur fait le choix d'écrire son mot de passe, il devra prendre toutes les mesures nécessaires pour protéger correctement le papier sur lequel le mot de passe est noté.
Il devra notamment conserver ce papier dans un emplacement sûr, en dehors de la zone de travail. Ainsi, l'Utilisateur ne devra en aucun cas conserver ce papier sous son tapis de souris, près de son écran, ou à proximité de son poste de travail.

Chaque Utilisateur, doit choisir un mot de passe facile à retenir mais difficilement devinable par les tiers.

Quelques astuces mentionnées ci après peuvent être utilisées:

1. Utiliser une combinaison de lettres, chiffres, majuscules, minuscules et caractères spéciaux.
2. Ne pas utiliser le nom et/ ou prénom ou celui de membres de la famille de l'Utilisateur, numéro de téléphone, ou adresse.
3. Ne pas utiliser un mot ou une liste de mot du dictionnaire, un nom propre, un nom de lieu, ou une série de nombres.
4. Ne pas utiliser de touches juxtaposées sur le clavier (telles WXCVBN). Toutefois, certaines combinaisons sur le clavier (comme a2z3e4r5t6a2z3e4r5t6) peuvent donner un mot de passe compliqué tout en étant facile à retenir. Par ailleurs, il est possible de recourir à une combinaison différente mais de modèle identique en cas de changement en remplaçant simplement le caractère de départ « a » par « z ». Cela permet d'obtenir toujours un mot de passe très difficile, totalement inédit et facile à retenir.
5. Recours à une phrase aisément mémorisable et utilisation uniquement de la première lettre de chacun des mots qu'elle contient. Remplacement des sons par des lettres ou des chiffres (« 2 » pour « deux », « K7 » pour « cassette » etc.) Exemple : « Julie aime beaucoup les cassettes » devient « jablk7 ».

4. UTILISATION D'INTERNET

Les Ressources permettant un accès à l'Internet, mises à disposition des Utilisateurs par Manpower France, sont la propriété de l'Entreprise. Ces équipements sont **destinés à un usage professionnel.**

4.1 Navigation sur l'Internet

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

Toutefois, l'**utilisation limitée de l'Internet à des fins personnelles est tolérée à titre ponctuel** pour des impératifs de la vie privée, à condition que cette utilisation :

- soit de courte durée et n'interfère pas avec la capacité de l'Utilisateur à accomplir les tâches attendues,
- 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.

Recommandations

L'Utilisateur ne devra pas oublier que l'usage de l'Internet à des fins privées accroît les risques d'altération du Système d'Information de Manpower France (infection par des virus informatiques ou autres programmes malveillants, volume accru de courriels indésirables, diminution de la performance du Système d'Information (temps de réponse allongés...) et qu'il doit rester **ponctuel**.

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

Par ailleurs, les données concernant l'Utilisateur (sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'Utilisateur, etc.) peuvent être enregistrées par des tiers, analysées pour en déduire ses centres d'intérêt, les préoccupations de Manpower France, et utilisées à des fins notamment commerciales.

Il est recommandé à chaque Utilisateur de **ne pas fournir son adresse e-mail professionnelle** ni aucune coordonnée professionnelle sur l'Internet si ce n'est strictement nécessaire à la conduite de l'activité de l'Entreprise. Il est également recommandé aux Utilisateurs d'effacer régulièrement les cookies et les fichiers de mémoire temporaire.

Comportements prohibés

En toute hypothèse, **il est strictement interdit** d'utiliser les équipements Manpower France d'accès à Internet pour :

- se rendre sur des sites Web pornographiques
- se rendre sur des sites qui approuvent la violence, la discrimination raciale ou religieuse, les dérives sectaires, l'intolérance, l'abus de drogues / d'alcool, les activités criminelles ou tout autre comportement illégal ;
- se rendre sur des sites qui permettent ou approuvent les jeux d'argent en ligne ;

- écouter la radio ou regarder la télévision en ligne ;
- accéder à des plateformes de partage de fichiers en *« peer to peer »*, des sites communautaires (*« Social Networking »*), des solutions en ligne de messagerie (sauf messagerie personnelle) ou de discussions instantanée (*« chats »*) ;
- télécharger tout fichier (programmes, images, photos, musique, film...) étrangères aux fonctions exercées au sein de l'Entreprise par l'Utilisateur.

Par ailleurs, toute publication d'un document interne à l'Entreprise ou d'une information de l'Entreprise sur un site Internet autre que le site officiel de l'Entreprise doit préalablement avoir reçu l'autorisation formelle de la Direction de la communication.

4.2 Filtrage

Manpower France utilise un système de protection spécifique permettant de s'assurer que la connexion Internet de l'Entreprise est utilisée par les Utilisateurs dans le respect des lois en vigueur et des termes de cette Charte.

Ce système **enregistre et stocke l'ensemble des connexions effectuées** (« Logs ») par les Utilisateurs d'Internet et **identifie les sites consultés par Utilisateur**. Le journal des connexions est conservé durant une durée conforme à la loi.

La mise en place de cette protection a pour objectif de :
- protéger les données du Système d'Information de l'Entreprise ;
- sécuriser le serveur et les postes informatiques des virus circulant sur Internet et d'autres programmes dont l'installation ou l'utilisation présente un risque pour Manpower France ;
- 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 infantile.

Le système de protection pourra identifier et bloquer automatiquement toutes les tentatives d'accès à des sites, et les tentatives d'émission ou de réception de messages électroniques dont le contenu relève de :
- la violence et l'apologie ou l'incitation de crimes ou de délits ;
- la pornographie, notamment infantile et adolescente ;
- la diffusion d'images et de vidéos à caractère érotique et/ou sadomasochiste ;
- la haine raciale, la discrimination raciale sous toute forme ;
- la diffusion de contenus clairement contrefaisants;
- services de jeux d'argent et de paris.

Le système de protection pourra identifier et bloquer automatiquement toutes les tentatives d'accès et d'utilisation de certains services en raison de la nature de ces services ou des modalités de fourniture de ces services, et notamment:
- échange de données en peer to peer ;
- sites communautaires, « social networking » ;
- messagerie instantanée, streaming, spamming, chat, applets java... ;
- téléchargement de fichiers exécutables, fichiers mutli-médias, vidéos.

Cette liste n'est pas exhaustive et pourra être modifiée régulièrement par l'Entreprise conformément aux principes énoncés dans cette Charte.

Le système de protection peut adresser sur demande au Système d'Information de l'Entreprise un compte-rendu pour chaque tentative d'accès à une page Web dont l'accès est prohibé. Ce compte-rendu inclut notamment:
- le jour et le moment exact où a eu lieu la tentative d'accès ;

- l'identification du poste à partir duquel a eu lieu la tentative d'accès ;
- l'identification de la page Web dont l'accès n'a pas été permis.

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.

En revanche, il est strictement interdit de **tenter d'une manière répétée** d'accéder à une même page Web prohibée (ou à des pages Web prohibées faisant parties d'un même site Web). Les Utilisateurs doivent être sensibles au fait que de tels agissements saturent le Système d'Information et perturbent inutilement le travail de ceux ayant en charge la surveillance de l'usage des Ressources.

5. UTILISATION DES OUTILS DE COMMUNICATION ELECTRONIQUE

Les règles d'utilisation des outils de communication électronique ci-dessous exposées ont pour but de :

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

5.1 Conditions générales d'utilisation des outils de communications électroniques

Utilisation à titre professionnel et à des fins personnelles

Les équipements et les systèmes de communication électronique (comme le courriel, la messagerie instantanée, etc.) mis à disposition par Manpower France sont réservés à un **usage professionnel.**

Toutefois, l'utilisation limitée de ces Ressources à des fins personnelles est tolérée à **titre exceptionnel** pour tenir compte des impératifs de la vie privée, à condition que cette utilisation :

- présente un caractère ponctuel et de courte durée et n'interfère pas avec la capacité du salarié 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 pour les autres Utilisateurs,
- n'occasionne ni préjudice, ni embarras pour l'Entreprise.

Seuls les équipements de communication électronique fournis par l'Entreprise doivent être employés dans le cadre d'échanges à caractère professionnel.

L'utilisation de compte de messagerie personnel (notamment services de messagerie fournis par des tiers comme Yahoo, Hotmail, etc.) est interdite pour la conduite des affaires pour le compte de l'Entreprise.

Comportements prohibés

En toute hypothèse, **il est strictement interdit** de stocker ou de transmettre, par l'intermédiaire des outils de communication fournis par l'Entreprise :

- des documents sexuellement explicites ou suggestifs ;
- des documents 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, à moins que cela ne fasse partie d'une exigence professionnelle comme définie et approuvée par l'Entreprise, **les outils de communications électroniques ne pourront 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'**envoyer de manière excessive des messages personnels** (que ceux-ci soient expressément identifiés comme tel ou non);
- le fait d'accéder à des données concernant d'autres Utilisateurs sans leur autorisation, sauf lorsque le salarié a définitivement quitté l'entreprise et à l'exception des personnes en charge de la supervision du Système d'Information de l'Entreprise ;
- le fait d'utiliser un autre identifiant/mot de passe que le sien.

Par ailleurs, il est strictement interdit à un Utilisateur disposant d'une boîte à lettre individuelle attribuée par l'Entreprise (@manpower.fr) d'en transférer automatiquement le contenu vers une adresse privée, sans autorisation expresse de la Direction du Système d'Information.

Recommandations diverses

Il est rappelé aux Utilisateurs que le courrier électronique (courriel, email ou mel) ou le message court (« Texto », « SMS ») 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 signatures doivent être respectées.

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.

Protection des données confidentielles :

Les risques d'interception des messages électroniques exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du Système d'Information, aux informations à caractère non confidentiel, non stratégique et non sensible.

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.

5.2 Correspondances à caractère privé

Tout message envoyé ou reçu, par un Utilisateur au moyen d'un outil de messagerie électronique mis à disposition par Manpower France (courriel, sms, télécopie...) est réputé à caractère professionnel, sauf s'il est clairement identifié comme étant « privé ».

Afin de garantir le droit au respect de la vie privée, chaque Utilisateur veillera à indiquer la mention « privé » dans la case « objet » lors de l'envoi d'un message électronique de cette nature. **Le défaut d'une telle mention conférera au message une présomption de message à caractère professionnel.**

L'Utilisateur susceptible de recevoir un message électronique personnel dans le cadre de la tolérance stipulée ci-dessus doit demander à son correspondant d'indiquer le caractère personnel de son message en objet.

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

6. UTILISATION DES RESSOURCES MATERIELLES

6.1 Fourniture et règles générales d'utilisation

Fourniture et configurations des Ressources matérielles

Les Ressources matérielles du Système d'Information appartiennent à l'Entreprise. Elles sont mises à la disposition des Utilisateurs pour les aider dans l'accomplissement des missions qui leurs sont confiées dans le cadre de leurs activités professionnelles. Les matériels 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.

Lorsqu'un Utilisateur éprouve le besoin de disposer d'un nouveau matériel ou d'utiliser un équipement non standard, il doit solliciter la DSI 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 DSI ou des personnels habilités.

Le matériel réseau (routeurs, commutateurs, serveurs, etc.) situé dans les locaux de l'Entreprise ou sur tout réseau informatique de l'Entreprise doit être d'un type et d'une configuration approuvés et mis en œuvre par le personnel autorisé de Manpower France au sein de la DSI

Ce matériel ne peut être installé que par les personnes dûment autorisées au sein de la DSI par Manpower France pour la fourniture de cette prestation de service.

L'Entreprise se réserve le droit de désactiver ou de retirer tout matériel réseau installé en violation de cette règle.

Recommandations générales d'utilisation

Les Utilisateurs doivent, 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.

Les supports amovibles de mémoire (disquettes, clefs usb...) constituent un vecteur très important de transmission des virus et impliquent lors de leur utilisation la vérification de leur contenu.

À l'exception des équipements dédiés à une utilisation nomade, les équipements ne doivent pas être déplacés, sans l'intervention de la DSI.

6.2 Équipements nomades

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

Les outils d'accès à distance au réseau Manpower France qui ne sont pas spécifiquement fournis et mis en œuvre par Manpower France sont interdits.

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 « *PDAs* » ou assistants personnels, ainsi que 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 portables sans surveillance dans les lieux publics.
- Le vol ou la perte d'appareils informatiques doit être immédiatement signalé(e). auprès de son supérieur hiérarchique, à la DSI et à la DRH.

Recommandations et informations supplémentaires

Afin de prévenir les risques de vol,

- ne laissez pas les appareils portables sans surveillance dans votre bureau, ou dans les locaux de clients, prestataires ou de toute autre Entreprise à moins qu'ils ne soient convenablement sécurisés au moyen d'un câble antivol ou d'un autre mécanisme.
- lors de l'utilisation d'un câble antivol, assurez-vous que celui-ci est attaché à un objet fixe qui ne peut être facilement déplacé, soulevé ou volé avec l'ordinateur.

Recommandations en voyage :

- Transportez votre ordinateur portable dans un sac de protection rembourré. Un sac de transport que l'on imagine difficilement pouvoir contenir un ordinateur est conseillé. Tout voleur potentiel ciblera en priorité les sacs contenant de toute évidence un ordinateur. Un bon moyen pour cacher son ordinateur consiste à placer son sac de protection matelassé dans une autre serviette ou dans un sac de sport.
- N'enregistrez pas votre ordinateur portable comme bagage à l'aéroport. Le risque de vol ou d'endommagement l'emporte de loin sur les avantages.
- Soyez particulièrement vigilant lorsque vous faites la queue aux points de contrôle de sécurité dans les aéroports car il s'agit d'un endroit idéal pour qu'un voleur opère une diversion pendant qu'un complice vole votre ordinateur. Surveillez avec attention votre appareil lorsqu'il passe sur le tapis roulant.
- Ne laissez jamais votre ordinateur ou tout autre appareil informatique portable sans surveillance dans un lieu public (comme les restaurants, les halls d'hôtels, les salles d'attente des aéroports, etc.)
- Si vous devez laisser votre ordinateur dans une voiture sans surveillance, veillez à ce que cette dernière soit fermée à clé et que l'ordinateur soit hors de vue, de préférence dans le coffre.
- Utilisez un câble antivol si vous devez laisser votre ordinateur sans surveillance dans une chambre d'hôtel. Assurez-vous qu'il soit attaché à un objet fixe, difficile à déplacer dans la pièce. L'alternative est de ranger l'appareil dans un coffre-fort situé dans la chambre ou bien dans un tiroir pouvant être fermé à clé.

6.3 Protection des systèmes inactifs ou laissés sans surveillance

Tous les Utilisateurs doivent 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.

Par ailleurs, avant de laisser son poste de travail actif sans surveillance, l'Utilisateur doit systématiquement le verrouiller par toute méthode empêchant l'accès à tout utilisateur non autorisé. (Exemple : économiseur d'écran).

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 DSI. Il ne peut en aucun cas être modifié ou annihilé par l'Utilisateur.

Recommandations et informations supplémentaires

Les recommandations standard de fermeture de session prévues pour chaque Ressource doivent être respectées. Ces règles figurent notamment dans le manuel d'utilisation de chaque Ressource. Le contenu du manuel est porté à la connaissance du salarié au travers d'une aide en ligne ou de tout autre moyen approprié.

Certaines Ressources disposent de processus qui terminent automatiquement une session une fois que certains seuils ont été atteints. Ces seuils peuvent être basés sur la durée totale d'inactivité de la session, des heures spécifiques de la journée auxquelles les Utilisateurs doivent quitter le système ou bien d'autres facteurs spécifiques aux systèmes.

7. PROTECTION DES INFORMATIONS

Toutes les informations traitées ou conservées par Manpower France sont classées en quatre catégories, selon leur degré de confidentialité. A chaque catégorie de données ou d'informations correspond un régime particulier de protection. Les Utilisateurs doivent respecter les règles prévues pour chacune des catégories de données qu'ils sont amenés à connaître.

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

Objectif

Cette politique contribue à garantir que les informations appartenant à l'Entreprise sont convenablement protégées durant tout leur cycle de vie. L'Entreprise confie aux Utilisateurs autorisés à accéder à ces informations le soin de les protéger convenablement afin de préserver leur confidentialité, leur intégrité et leur disponibilité.

Le respect de cette politique aidera à protéger les informations de l'Entreprise – et particulièrement les informations confidentielles - contre le vol, ou leur simple perte. Ainsi la vie privée des salariés, partenaires et clients est protégée et il en est de même de la marque Manpower France et de la réputation de l'Entreprise.

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

En cas de doute, la DSI ou tout autre direction désignée par elle peut être consultée afin de déterminer le périmètre des informations qui doivent être protégées dans le cadre de cette politique.

Les définitions ci-dessous données dans le cadre de la protection des données offrent une vue élargie des différences entre les catégories adoptées dans le cadre de cette politique et fournissent une liste d'information pratiques qui doivent être considérées comme étant à protéger dans chacune des 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).

A titre d'exemples, constituent des Informations Confidentielles :

- les données à caractère personnel suivantes des employés 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, salaire, avantages professionnels...
- les informations concernant la sécurité interne tel que le paramétrage des firewalls ou d'autres équipements.

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, organisateur...) doivent être chiffrées ;
- Les Informations Confidentielles ne doivent pas être stockées sur des média amovibles (tels que CD, disquettes, bandes, 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) ;
- 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 dont la diffusion est restreinte »

Les Informations à Diffusion Restreinte incluent celles :
- présentant un caractère confidentiel sans pour autant constituer des Informations Confidentielles définies ci-dessus ; 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 pénale de l'Entreprise (notamment pour violation de la vie privée).

Constituent des Informations à Diffusion Restreinte :
- les données à caractère personnel ne constituant pas, par nature, des Informations Confidentielles des employés ou candidats de Manpower France, telles que les adresses physiques ou e-mail, les numéros de téléphone, formation, compétences, référence professionnelles, l'expérience professionnelle, les préférences relatives au travail, les prétentions salariales, les CV, les évaluations professionnelles ;
- 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.

Le régime de protection minimal à respecter pour cette catégorie de données est le suivant :
- Les documents ou supports (tels que cd-rom, disquettes, bandes, clé USB...) contenant des Informations à Diffusion Restreinte ne doivent pas laissées à la vue et à la vue et / ou à la portée de tous ;
- La divulgation d'informations sensibles en dehors de l'Entreprise n'est autorisée que si elle est strictement nécessaire et doit être en conformité avec les autres procédures applicables, par une autorisation personnelle, une procédure, un guide, ou pour des contrats conclus avec des clients ou des partenaires ;
- Lorsqu'ils ne sont plus utilisés, les supports contenant des informations sensibles 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.

Exemples :

- Lettres d'information de l'Entreprise ou d'une direction.
- Annuaire des lignes téléphoniques directes

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.

Exemples :

- Liste téléphonique des agences et autres bureaux ;
- informations publicitaires.

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

8. PROTECTION CONTRE LES VIRUS INFORMATIQUES

Il est strictement interdit d'introduire sciemment dans le Système d'Information de Manpower France, 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'avertissements concernant des programmes malveillants, auprès d'autres individus, en particulier par l'intermédiaire de la messagerie électronique mis à disposition par Manpower France.

8.1 Logiciel anti-virus

L'ensemble des postes de travail est équipé d'un logiciel antivirus à jour fourni ou approuvé par Manpower. Afin de garantir son efficacité, les Utilisateurs doivent veiller à :

- ce que le logiciel antivirus soit toujours actif.
- l'utiliser pour détecter la présence d'un virus lorsque celle-ci est suspectée.
- signaler immédiatement à la Direction du Système d'Information (DSI) de Manpower France tout problème lié soit à la détection, soit l'éradication des virus (securite.dit@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'un autre logiciel antivirus, non fourni ou non approuvé par Manpower France 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 d'ordinateur.

8.2 Recommandations et informations supplémentaires

Aucun logiciel antivirus ne peut être considéré comme étant infaillible. C'est pourquoi, il est indispensable pour les Utilisateurs de se conformer aux règles préventives suivantes :

- Méfiez-vous de tout courriel ou de toute pièce jointe imprévu(e) même si le courriel provient d'une personne que vous connaissez et en laquelle vous avez confiance. Les courriels et pièces jointes représentent actuellement les moyens de diffusion de virus les plus courants et les courriels infectés sont souvent générés automatiquement sans que l'expéditeur en ait même conscience.
- soyez prudent lors du téléchargement de fichiers provenant d'Internet. La majorité des entreprises jouissant d'une certaine renommée applique des mesures contre les virus sur leur site Internet mais très peu d'entre elles garantissent que les téléchargements provenant de leur site sont « exempts de virus ».
  Il est rappelé aux Utilisateurs que le téléchargement de tout document (images, photos, musique, film...) sans rapport avec les fonctions exercées au sein de l'Entreprise est strictement interdit (cf. « Utilisation d'Internet »).
- Méfiez vous des courriels ou autres annonces que vous pourriez recevoir d'autres personnes que de la DSI, vous avertissant de l'apparition de nouveaux virus et des terribles conséquences que leurs infections provoquent.
  En effet, la majorité de ces avertissements sont des canulars conçus pour propager les craintes et semer la panique.

Ces messages prient avec insistance le destinataire de transférer l'avertissement à toutes les personnes de sa connaissance inondant ainsi les systèmes de messagerie avec de faux avertissements et les surchargeant jusqu'au point de défaillance. Si un tel avertissement est reçu, envoyez-le pour vérification au personnel de sécurité concerné de Manpower France. Ces messages ne doivent en aucun cas être envoyés à d'autres personnes.

9. APPLICATION DES CORRECTIONS DU SYSTEME DE SECURITE

9.1 Généralités

Pour protéger les ordinateurs de manière adéquate contre la propagation de virus, vers et autres programmes malveillants, il est impératif que les patchs de sécurité et les mises à jour d'antivirus soient régulièrement mis en œuvre.

Toutefois, il est tout aussi impératif que ces mises à jour et corrections ne soient pas appliquées tant qu'elles n'ont pas été testées et vérifiées par le personnel d'assistance technique concerné (la DSI, l'un des prestataires de Manpower France ou du Groupe, l'éditeur du programme ayant présenté des failles de sécurité...)

Par conséquent, afin de garantir que les patchs-et mises à jour logicielles seront appliqués de manière opportune :

- le personnel d'assistance technique devra suivre la procédure de mise à jour des logiciels et d'application des corrections du système de sécurité afin que les mises à jour et corrections critiques soient rapidement mises en œuvre.
- Il est interdit aux Utilisateurs de procéder à des mises à jour de logiciel antivirus ou d'appliquer des patchs sur ces logiciels sauf si ceux-ci proviennent directement du personnel d'assistance technique de Manpower France.

9.2 Informations supplémentaires

Des techniciens spécialisés (personnel d'assistance technique) sont chargés de surveiller et de protéger le Système d'Information.

Dès que des mises à jour, des corrections ou d'autres mesures de protection sont disponibles, le personnel d'assistance technique teste leur compatibilité avec les logiciels actuellement déployés et décide en fonction du niveau de risque de chaque menace, du moyen de communiquer le patch ou la correction disponible.

En général, les corrections et patchs qui sont considérés comme étant « critiques » seront déployés aussi rapidement que possible.
Les mises à jour « critiques » pourront être lancées directement et immédiatement sur tout ordinateur dès lors qu'il se connecte au réseau. Les autres mises à jour moins importantes peuvent être simplement incluses dans un cycle de mise à jour de la maintenance générale du logiciel.

Le déploiement réussi de toute mesure de protection dépend des actions de chacun. Plus les mesures de protection sont appliquées rapidement, plus la probabilité qu'un ordinateur particulier soit endommagé, ou corrompu, est réduite.
Les utilisateurs ne doivent en aucun cas télécharger des corrections, ou des mises à jour provenant de toute source autre que le réseau Manpower.

10. SIGNALER LES INCIDENTS DE SECURITE

Tout incident réel ou suspecté relatif à la sécurité des informations doit être signalé sans délais. 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 (cf. ci-dessous).

Les Utilisateurs devront rendre compte de ces incidents auprès de la Direction du Système d'Information (DSI) de Manpower France (securite.dit@manpower.fr) et à leur supérieur hiérarchique immédiat.

Objectif

L'objectif de cette politique est de réduire le risque d'incident de sécurité pour l'Entreprise. Le recueil des rapports d'incidents de sécurité réels ou suspectés peut, en effet, permettre de détecter une activité malveillante. Les retards de signalement peuvent entraîner des pertes supplémentaires pour l'Entreprise.

Règles de prudence et 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 de l'Entreprise) 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.

11. UTILISATION DE MODEMS

Définition : Les modems sont employés pour connecter les ordinateurs et les réseaux distants au moyen de lignes téléphoniques.
Les modems reliés aux ordinateurs connectés aux réseaux de Manpower France doivent être configurés pour un accès sortant uniquement. **Ces modems ne doivent en aucun cas autoriser les appels entrants.**

Seule la Direction du Système d'Information est autorisée à introduire, retirer ou modifier les modems et autres matériels nécessaires au fonctionnement du Système d'Information.

Les ordinateurs reliés aux lignes téléphoniques publiques au moyen de modems sont extrêmement vulnérables aux attaques provenant de l'extérieur. Les techniques, telles que celles usant d'un composeur d'attaque, sont employées pour détecter les ordinateurs connectés de sorte que des actes de piratage puissent être réalisés par la suite à leur encontre. La protection la plus efficace contre ce genre d'attaques est de débrancher complètement la ligne téléphonique des ordinateurs équipés d'un modem. Toutefois, cette solution n'est pas satisfaisante puisque la connexion du modem à la ligne téléphonique est nécessaire pour que le poste de travail puisse se connecter à un ordinateur distant ou au réseau.

Dans ces cas, le modem de l'ordinateur doit être configuré de manière à ce que seuls les appels sortant soient autorisés. En d'autres termes, la propriété « Réponse automatique » doit être désactivée de sorte qu'aucun appel entrant ne soit reconnu.

Ainsi, les attaquants extérieurs ne peuvent se connecter à l'ordinateur ou prendre son contrôle et le risque d'accès, par des personnes non autorisées, à des ordinateurs contenant des informations confidentielles, est réduit. Il en est de même du risque qu'un ordinateur compromis soit employé pour accéder aux réseaux informatiques de Manpower France.

12. UTILISATION DES LOGICIELS

12.1 Logiciels non fournis par Manpower France

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

Il est interdit aux Utilisateurs d'installer tout programme informatique (progiciels logiciels y compris bibliothèques logicielles, applets, API, scripts...), même gratuit qui n'est pas spécifiquement fourni ou approuvé par l'Entreprise. Manpower France fournit tous les programmes informatiques dont les Utilisateurs ont besoin pour réaliser leur travail.

L'installation de tout autre logiciel peut affecter la performance et la fiabilité de ceux qui sont fournis, et par conséquent, **est rigoureusement interdit**.

Sont notamment prohibés, le téléchargement et/ ou l'installation :

- de logiciels de jeux,
- de programmes utilitaires et économiseurs d'écran personnalisés,
- les logiciels de partage de fichiers « peer to peer » (comme Napster, Morpheus, Kazaa, etc.)
- d'équipements de messagerie instantanée non fournis par l'Entreprise
- de tout logiciel gratuit téléchargeable en provenance d'Internet.

Conformément à l'article « Contrôles », le recours à des moyens électroniques pour effectuer un inventaire de tous les programmes informatiques présents sur tout ordinateur connecté au réseau de Manpower France est possible.

12.2 Logiciels fournis par Manpower France

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

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 paramétres de sécurité d'un logiciel installé sur un poste de travail est strictement interdite.

Pour des raisons liées à l'accomplissement des missions qui leurs sont confiées, les collaborateurs de la DSI 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.

Le but de cette politique est d'empêcher que les employés de Manpower France 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 protégé par les lois relatives à la propriété intellectuelle et au copyright sans licence valable pour la version utilisée constituent tous des exemples de violation des lois relatives à la propriété intellectuelle et au copyright.

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

Tous les Utilisateurs sont responsables de l'utilisation des outils conformément aux conditions d'utilisation qui sont portées à leur connaissance.

13. INTRANET

Mise en place et Fonctionnement

L'Intranet fonctionne sous la responsabilité informatique de la DSI et sous la responsabilité éditoriale du Directeur des ressources Humaines.

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 à la Direction des ressources humaines quant au contenu ou fonctionnement de l'Intranet.

14. CONTROLES

Dans le but de protéger son Système d'Information, l'Entreprise procèdera à des contrôles pour s'assurer du respect des dispositions de la Charte par les Utilisateurs. A ce titre, la Direction du Système d'Information pourra, dans le cadre de ses missions de protection du système d'information, exercer un contrôle de l'utilisation d'Internet par les Utilisateurs. Ces contrôles portent sur les durées des connexions, la fréquence de connexion aux sites les plus visités, les volumes téléchargés...

Un historique de l'usage d'Internet par les Utilisateurs de l'Entreprise peut être conservé à des fins d'audit.

Les représentants du personnel ont été informés et consultés sur les moyens de contrôle qui pourront être utilisés, conformément à l'article L.2323-32 du Code du travail.

14.1 Principes

Les Ressources mises à disposition des Utilisateurs font partie du patrimoine de l'Entreprise et/ou demeurent sous sa garde et sa responsabilité. Par conséquent, toute donnée émise, reçue ou stockée sur l'une quelconque de ces Ressources est réputée constituer la propriété de L'Entreprise (à l'exception des messages reçus et émis ayant un caractère personnel et dûment identifiés comme tel).

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.

14.2 Informations objet des contrôles

Au sein de L'Entreprise, toute opération va déclencher l'enregistrement :

- de l'heure de la connexion ;
- de l'identifiant de l'Utilisateur ayant déclenché l'opération ;
- du système auquel il est accédé ;
- du type de transaction réalisée (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.

Cette surveillance permet :

- de bloquer, **a priori**, à l'aide de systèmes à l'entrée ou à la sortie, tout type de fichier ou message non conforme aux présentes dispositions ou dont la provenance permet d'identifier une source interdite ou illicite, dont la nature ou le contenu sort de l'ordinaire par la taille ou le type ;
- d'analyser et de contrôler, a **posteriori**, les traces à fin d'études statistiques et de surveillance du système d'informations faisant ainsi ressortir :
  - la liste des sites les plus visités sur le Web,
  - les temps de connexion et la fréquence des connexions site par site, utilisateur salarié par le nombre de messages émis et reçus classés par volume et par nature des pièces associées,
  - le coût des connexions le cas échéant.

14.3 Réalisation des contrôles (généralités)

La DSI étant habilité à prendre connaissance de tous les dossiers, toute information peut être interceptée et consultée sous réserve des dispositions spécifiques à certains messages électroniques identifiés comme personnels.

Lorsqu'à l'occasion de son activité 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, voire susceptible de causer un préjudice à l'Entreprise ou un tiers, il déclenche une procédure d'alerte.

Informé de la mise en œuvre d'une procédure d'alerte, le directeur des ressources humaines peut décider, à la vue des éléments obtenus de manière a priori soit de se contenter de ces éléments s'il 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 le service informatique et où le ou les Utilisateurs concernés ont été 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 permet pas à l'Utilisateur 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.

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, le service 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.

14.4 Réalisation des contrôles (messagerie électronique)

Tout message électronique présent dans les Ressources de l'Entreprise est présumé être une information professionnelle appartenant à l'Entreprise, sauf pour les quelques messages électroniques clairement identifiés comme privés (cf. Chapitre 5 – Utilisation des outils de communication électronique).

En conséquence, la DSI pourra prendre connaissance et analyser tous les **fichiers de journalisation** attachés aux messages électroniques. En revanche, la DSI ne pourra prendre connaissance du **contenu** que des seuls messages électroniques non-revêtus de la mention de leur caractère personnel, et protégés comme tels par le secret des correspondances.

Les Utilisateurs sont informés que la prise de connaissance par la DSI de courriers électroniques personnels non-revêtus de la mention adéquate aura nécessairement été commise de bonne foi et ne pourra en tant que telle être reprochée à l'Entreprise.

Le personnel du service informatique en charge de ces contrôles est soumis à une obligation stricte de confidentialité en ce qui concerne le contenu des correspondances. En tout état de cause, ce personnel est soumis à une obligation de discrétion sur l'ensemble des éléments qui leur seraient connus du fait de l'exercice de leurs missions. A ce titre, ce personnel ne portera les informations connues du fait de ces contrôles qu'à la connaissance de leurs supérieurs hiérarchiques et/ou aux autorités de police/ judiciaires.

15. DISPOSITIONS FINALES

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

Elle a été soumise à l'avis du Comité Central d'Entreprise le 9 octobre 2008, le 20 novembre 2008, le 18 décembre 2008 et le 12 mars 2009.

Conformément à l'article L.1321-4 du Code du travail, deux exemplaires de la présente Charte, ainsi que l'avis du CCE ont été envoyés à l'Inspecteur du Travail.

Conformément à l'article R.1321-2 du Code du travail, un exemplaire de la présente Charte a été déposé au secrétariat du Greffe du Conseil de Prud'hommes de Paris, le 30 mars 2009.

Les modifications et adjonctions apportées à la présente Charte feront l'objet des mêmes procédures de consultation, de communication, de publicité et de dépôt.

L'entrée en vigueur de la présente Charte est fixée au 1er mai 2009, à l'exception des dispositions prévues aux articles Filtrage (4.2) et Contrôles (14) qui entreront en vigueur le 1er juin 2009.

Fait à Paris, le 30 mars 2009.

Jean- François DENOY
Directeur des Ressources Humaines