

Charte d'utilisation des Ressources des Systèmes d'Information de l'Etablissement public

1- Objet

Le présent document constitue la charte d'utilisation des ressources des systèmes d'information (ci-après la « Charte ») de l'Etablissement Public de la Caisse des Dépôts (ci-après l' « Etablissement »).

La Charte décrit les règles qui doivent être respectées afin d'assurer les conditions d'un usage sécurisé et en conformité avec la législation et la réglementation en vigueur, des ressources des systèmes d'information de l'Etablissement.

Elle a ainsi pour objet :

- de faire prendre conscience à chaque utilisateur de l'importance de la sécurité des systèmes d'information au sein de l'Etablissement et de le responsabiliser,
- de préciser les principaux droits, les devoirs et les responsabilités des utilisateurs des systèmes d'information de l'Etablissement, en conformité avec les législations et réglementations en vigueur, les règles de déontologie, ainsi que les règles et recommandations en vigueur dans l'Etablissement, en particulier la Politique générale de sécurité de l'information et le Code de déontologie,
- de conduire chaque utilisateur à adopter les comportements de sécurité qui sont nécessaires au bon fonctionnement et à la sécurité des systèmes d'information de l'Etablissement.

Les principes énoncés ne sont pas exclusifs notamment de l'application des lois et de l'ensemble des règles internes à l'Etablissement, des règles de courtoisie et de respect d'autrui.

Ce document annule et remplace toutes ses précédentes versions.

La Charte a été soumise à l'avis du comité technique de la Caisse des dépôts et consignations et du comité d'hygiène, de sécurité et des conditions de travail (CHSCT), compétents pour l'ensemble des collaborateurs de l'établissement public. Elle a été annexée par avenant au règlement intérieur des agents contractuels sous le régime des conventions collectives et a été rendue applicable aux personnels de droit public et sous statut CANSSM par arrêté du directeur général.

2- Engagement et application

La présente charte s'adresse à toute personne qui utilise les ressources des systèmes d'information, c'est à dire : (i) l'ensemble des collaborateurs de l'Etablissement, permanents ou non, quel que soit leur statut (public/privé) et (ii) les collaborateurs occasionnels externes à l'établissement (prestataires de services, intérimaires, stagiaires...).

Tout Utilisateur des systèmes d'information de l'Etablissement est tenu de respecter cette Charte ainsi que la législation et la réglementation en vigueur, notamment en matière de protection des droits de propriété intellectuelle et de protection des données à caractère personnel.

En cas de non-respect avéré de cette Charte, l'Etablissement peut notamment restreindre ou révoquer sans préavis les droits d'accès aux ressources (messagerie, Internet...). Le collaborateur est alors informé par écrit des constats motivant l'intervention et pourra faire valoir sa position.

L'Etablissement peut également décider de prendre des sanctions disciplinaires, dans le respect des procédures applicables, et ceci sans préjuger des éventuelles poursuites judiciaires qui pourraient être initiées.

2.1 – Information et sensibilisation des Utilisateurs

La Charte est portée à la connaissance des utilisateurs par tous les moyens jugés adéquats par l'Etablissement.

Constituent notamment un moyen adéquat l'un des moyens suivants : diffusion sur l'Intranet « Sécurité des SI » et celui des Ressources humaines de l'Etablissement, annexe signée aux conventions de stage pour les stagiaires externes (universités...), notification individuelle notamment auprès des nouveaux entrants, et annexes aux accords-cadres et marchés conclus avec les prestataires et les entreprises de travail temporaires. Lors de son entrée en vigueur, ce document fera l'objet d'une notification individuelle.

Les utilisateurs sont invités à suivre la formation organisée par l'Etablissement en matière de sécurité des systèmes d'information et à consulter la Charte sur le site Intranet de l'Etablissement afin d'appliquer les règles d'utilisation prévues par la présente Charte.

3- Définitions

Administrateur : au sein du Service Informatique ou des directions et services de l'Etablissement, les administrateurs sont des utilisateurs disposant d'accès privilégiés aux systèmes d'information, leur permettant d'en gérer et contrôler le fonctionnement.

Authentifiant / Moyen d'authentification : élément ou ensemble d'éléments permettant à un utilisateur ou à une ressource d'un système d'information de prouver son identité afin, par

exemple, de se voir attribuer des droits d'accès à un système d'information ou à des informations (mot de passe, carte à puce et code d'activation correspondant, bi-clé cryptographique et certificat électronique associé, etc.).

Classification : opération qui consiste à définir le niveau de criticité d'une information selon un ou plusieurs critères de sécurité. La classification s'applique à une donnée, un document, un fichier, un programme, une application, etc.

Comportement / usage abusif : comportement / usage contraire à la Charte et/ou illicite.

Confidentialité : un des critères de sécurité permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder.

Document : lorsqu'il est numérique, un document est une forme de représentation de l'information consultable à l'écran d'un Equipement. Cela comprend notamment les courriels, fichiers, vidéos, photographies, etc.

Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Equipement individuel : tout équipement, mis à disposition par l'Etablissement à titre professionnel, fixe ou mobile, permettant à un utilisateur d'accéder à des systèmes d'information de l'Etablissement et/ou de traiter localement sur l'équipement des informations de l'Etablissement (ordinateurs fixes, ordinateurs portables, téléphones mobiles, téléphones mobiles intelligents (dits « smartphones »), tablettes tactiles, etc.).

Filtrage : action consistant à appliquer sur des flux d'information un ensemble de règles autorisant ou interdisant certains traitements informatiques.

Fonction Sécurité des Systèmes d'Information : au sein de l'Etablissement, fonction chargée de définir et de contrôler la bonne application des règles permettant d'assurer la sécurité des informations et des systèmes d'information. La fonction est incarnée par le Responsable de la Sécurité des Systèmes d'Information, son équipe, ainsi que les différents relais au sein des directions de l'Etablissement (responsables locaux de la sécurité des systèmes d'information, correspondants sécurité).

Habilitation : attribution à un utilisateur de droits d'accès à des Ressources par une entité autorisée.

Information : élément de connaissance (donnée, son, image fixe ou animée...) susceptible d'être conservé, traité ou transmis suivant un mode de codification défini et à l'aide d'un support matériel (papier) ou électronique (information dématérialisée).

Intégrité : un des critères de sécurité, garantie de l'exactitude, de la fiabilité et de l'exhaustivité des informations et des méthodes de traitement.

Marquage : opération consistant à apposer de manière visuelle ou non le niveau de classification d'une information sur un support.

Ressource (d'un système d'information) : tout élément intervenant dans la mise en œuvre et le fonctionnement d'un système d'information (informations sous toutes leurs formes, équipements individuels, imprimante, logiciel, serveur de fichiers, base de données, applications métiers, équipement réseau, service réseau interne / souscrit sur Internet, espace disque, messagerie électronique, etc.).

Sensible : toute donnée, fichier ou document classifié aux niveaux « confidentiel » ou « secret ».

Service Informatique : ensemble des fonctions de l'Etablissement en charge du développement, de la mise en œuvre et du maintien en conditions opérationnelles des systèmes d'information.

Système d'Information : ensemble organisé de ressources (données, procédures, matériel, logiciel, personnel, etc.) permettant d'acquérir, traiter, stocker, diffuser ou détruire les informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des informations (numérique, papier, oral, etc.).

Tiers : entités ou organismes externes en relation contractuelle avec l'Etablissement. Sont ainsi considérés comme des tiers : les prestataires, les intérimaires, les partenaires...

Traçabilité : un des critères de sécurité, traduisant la garantie que les événements et les accès aux Ressources sont enregistrés à travers des traces accessibles et, en cas de besoin, opposables.

Traitement de l'information : élaboration, modification, stockage, échange, diffusion, présentation ou destruction de l'Information, quelle que soit la forme sous laquelle est exploitée cette Information (électronique, imprimée, manuscrite, vocale, image...).

Utilisateur (d'un système d'information) : toute personne, qu'elle soit interne ou externe à l'Etablissement, qui accède à, ou utilise, des Systèmes d'Information et des Informations de l'Etablissement, de manière permanente ou occasionnelle. Désigne également les Administrateurs, les exploitants et les prestataires externes intervenant sur le SI.

4- Législation/Réglementation

4.1 - Principes généraux

Dans le cadre de l'usage des Ressources mises à sa disposition par l'Etablissement, l'Utilisateur s'engage au respect de la Charte, mais également au respect des dispositions législatives et réglementaires en vigueur.

L'Utilisateur doit notamment respecter :

- La réglementation relative aux libertés individuelles et les règles d'ordre public.
- La réglementation relative aux droits de propriété intellectuelle, qui interdisent notamment de reproduire et de diffuser les logiciels sans autorisation, pour quelque usage que ce soit. Il en est de même, d'une part, pour toutes œuvres telles que photographies, images, bases de données, œuvres audiovisuelles ou musicales, textes, etc. protégées par le droit d'auteur, et d'autre part, pour les marques, dessins et modèles, noms de domaine et autres signes distinctifs protégés.
- La réglementation relative à la protection des données à caractère personnel, qui interdit notamment toute collecte et traitement de données à l'insu des personnes concernées et encadre la notification des violations de données à caractère personnel telle que prévue par la loi du 6 janvier 1978 modifiée, dite « Informatique et Liberté » et par le Règlement européen de protection des données du 27 avril 2016.

- La réglementation relative aux atteintes aux systèmes d'information (articles 323-1 à 323-7 du code pénal) qu'il s'agisse notamment de manière frauduleuse de l'accès, du maintien, de l'entrave d'un système de traitement automatisé de données, de l'extraction, de la reproduction, de la transmission de données ou de l'altération des éléments qu'il contient, étant précisé que ces actes sont passibles de sanctions pénales.

4.2 - Propriété intellectuelle

Chaque Utilisateur doit respecter des règles de bon usage et ne pas installer ou copier, sur les Ressources de l'Etablissement, de logiciels, même ceux appartenant au domaine public.

Sauf autorisation expresse de la Fonction Sécurité des Systèmes d'Information et du Service Informatique, le téléchargement et l'installation de logiciels sont interdits. En vue d'accorder, le cas échéant, de telles autorisations, ils procéderont à des vérifications en termes de sécurité informatique et de licence d'utilisation pour les logiciels concernés.

Les logiciels mis en œuvre ou autorisés par l'Etablissement doivent tous être utilisés et exploités exclusivement dans les conditions des licences souscrites par l'Etablissement ou le Service Informatique et sous réserve des autorisations nécessaires. Dans le cas d'une utilisation d'un logiciel à code ouvert (dit « open source »), l'Utilisateur s'engage ainsi à respecter scrupuleusement les termes de la licence correspondante.

Conformément à la loi, il est rappelé que sauf dispositions statutaires ou stipulations contraires, les droits patrimoniaux sur les logiciels et sur leur documentation, créés par un ou plusieurs Utilisateurs dans l'exercice de leurs fonctions ou d'après les instructions de leur responsable hiérarchique, sont dévolus à l'Etablissement qui est seul habilité à les exercer.

Il est rappelé à l'Utilisateur que les œuvres de l'esprit telles que photographies, images, bases de données, œuvres audiovisuelles et musicales, textes, marques, etc. sont protégées par le droit de la propriété intellectuelle. L'Utilisateur ne doit donc pas utiliser les Ressources (Intranet, extranet, réseau...) en portant atteinte aux droits de la propriété intellectuelle de l'Etablissement ou de tiers (téléchargement illicite notamment depuis Internet, mise en partage non autorisée d'œuvres protégées par le droit d'auteur, etc.). Ainsi, l'Utilisateur n'utilisera en aucune manière les Ressources de l'Etablissement pour lire, copier, stocker, ou transmettre, sans licence et à des fins privées ou commerciales, des contenus ou des logiciels protégés par le droit de la propriété intellectuelle. L'Utilisateur s'interdit aussi toute reproduction et utilisation de fichiers, données ou bases de données de tiers protégés par le droit de la propriété intellectuelle ou un droit privatif en dehors des possibilités légales ou contractuelles qui lui sont reconnues.

Il est également rappelé que, lors de l'usage de services Internet ou de réseaux sociaux, l'Utilisateur est soumis aux conditions générales d'utilisation des fournisseurs de ces services. Ces conditions générales d'utilisation peuvent notamment prévoir des dispositions qui accordent des droits de propriété intellectuelle à ces fournisseurs sur les contenus et données de l'Utilisateur ou de l'Etablissement.

Il est de la responsabilité de l'Utilisateur de prendre connaissance des conditions générales d'utilisation des services de fournisseurs tiers et de s'assurer notamment du respect des droits de propriété intellectuelle de l'Etablissement lors de l'utilisation de services Internet et réseaux sociaux.

5- Accès aux Ressources

L'accès aux Ressources de l'Etablissement est géré par le Service Informatique, habilité à délivrer les Moyens d'authentification à chaque Utilisateur, selon les procédures d'autorisation en vigueur.

La mise à disposition d'une Ressource à un Utilisateur se fait sous la responsabilité du Service Informatique, selon les procédures et les modalités en vigueur.

L'accès par un Utilisateur à des Ressources de l'Etablissement n'est possible que dans le cadre de l'activité professionnelle de l'Utilisateur concerné au sein de l'Etablissement, défini par sa fonction, dans les limites des Habilitations qui lui sont accordées.

L'accès à ces Ressources est soumis à l'usage d'un ou plusieurs Authentifiants strictement personnels.

Toute Habilitation liée à une Ressource peut être modifiée ou supprimée, notamment en fonction des nécessités de service. L'Utilisateur doit respecter les règles de délivrance et de mise à jour de ses Authentifiants en vigueur au sein de l'Etablissement.

De plus, toute connexion faite à partir des Moyens d'authentification mis à disposition de l'Utilisateur à des fins professionnelles est présumée être une connexion effectuée à titre professionnel.

De manière générale, les Moyens d'authentification sont personnels, confidentiels et non transmissibles, l'Utilisateur étant responsable de leur confidentialité et de leur sécurité. En conséquence, il lui est interdit :

- de les inscrire sur support papier ou électronique à proximité des Ressources mises à disposition ou sur celles-ci, ainsi que de les stocker en clair dans un registre, un fichier ou un support non prévu à cet effet ;
- d'utiliser ou d'essayer d'utiliser les Moyens d'authentification autres que les siens et/ou de masquer sa véritable identité ;
- de les utiliser en contradiction avec la Charte.

En cas de suspicion de compromission d'un Moyen d'authentification, l'Utilisateur doit alerter le Service Informatique dans les meilleurs délais, puis par écrit, et demander son changement. A défaut de quoi il reste responsable des actions réalisées sous son identité, sauf à ce que sa bonne foi puisse être démontrée.

À ce titre, les utilisations faites à l'aide d'un Moyen d'authentification propre à chaque Utilisateur sont réputées être le fait du détenteur de ce Moyen d'authentification, sauf à ce que sa bonne foi puisse être démontrée.

Il est également précisé que l'accès de l'Utilisateur aux Ressources de l'Etablissement pourra être suspendu, limité ou réexaminé, pour des raisons de sécurité, notamment :

- lors de la cessation de son activité professionnelle au sein de son service ou de l'Etablissement (changement de service, mutation, etc.) ;
- dans certains cas de suspension temporaire de l'activité professionnelle (maladie, congé de maternité, etc.) ;
- dès lors qu'un usage abusif (manquements à la Charte, manquements aux lois et réglementations en vigueur, etc.) sera révélé.

La mise en œuvre de ces dispositions fait l'objet d'une information écrite et motivée à l'Utilisateur qui dispose d'un droit de réponse écrite et motivée.

De façon générale, l'Utilisateur ne doit pas tenter de contourner les dispositifs de sécurité d'accès en place, de s'introduire de façon illicite dans un système ou d'accéder, ou tenter d'accéder, à des Ressources pour lesquelles il n'est pas habilité. Les accès sont contrôlés dans le respect de la réglementation relative à la protection des données à caractère personnel.

6- Bon usage général des Ressources

6.1 - Principes généraux

De manière générale, tout Utilisateur est responsable de l'usage qu'il fait des Ressources qui sont mises à sa disposition dans le cadre de son activité professionnelle au sein de l'Etablissement.

L'Utilisateur doit en particulier :

- assurer la protection de ces Ressources en respectant les règles de sécurité applicables à celles-ci et en s'assurant de ne pas les mettre à disposition de personnes non autorisées, que ce soit des personnes internes ou externes à l'Etablissement ;
- être vigilant et signaler, dans les meilleurs délais puis par écrit, toute anomalie ou tout constat, tentative ou soupçon de violation d'une Ressource de l'Etablissement à sa hiérarchie ou à la Fonction Sécurité des Systèmes d'Information ;
- veiller, en toutes circonstances, à mettre en sécurité le matériel, notamment portable, mis à sa disposition ;
- verrouiller ou déconnecter son Equipement Individuel en cas d'absence même temporaire.

6.2 - Interdictions particulières

L'Utilisateur ne doit pas :

- introduire des failles de sécurité dans les architectures des Systèmes d'Information, par exemple par la connexion simultanée de son Equipement Individuel au réseau de l'Etablissement et à des réseaux et systèmes externes ;
- tenter de lire, modifier, copier ou détruire des données ou Documents autres que ceux qui lui appartiennent en propre ou pour lesquels il dispose des droits correspondants (lecture, modification ou suppression) ;

- risquer d'engorger les réseaux et les Systèmes d'Information, en évitant – sauf impératif de service – d'échanger via la messagerie électronique, ou de télécharger, via Internet, des volumes de données trop importants ;
- contourner ou désactiver les dispositifs de sécurité de ses Equipements individuels, notamment les antivirus, par exemple en installant sur les serveurs de ressources partagées des logiciels susceptibles de contourner, d'affaiblir ou de perturber la sécurité ou les performances du Système d'Information ;
- exploiter ou tenter d'exploiter une éventuelle faille de sécurité d'un Système d'Information ou en faire la publicité ;
- apporter des perturbations au bon fonctionnement des Systèmes d'Information, que ce soit par des manipulations anormales des Ressources matérielles et/ou logicielles ou par l'introduction volontaire de programmes malveillants (tels que des virus) ;
- contourner les restrictions d'utilisation des Ressources mises à sa disposition par l'Etablissement ;
- traiter des Informations professionnelles au travers d'outils ou de services qui n'aient pas été préalablement validés par la Fonction Sécurité des Systèmes d'Information et le Service Informatique.

L'Utilisateur ne doit pas déplacer, dupliquer ou détruire les fichiers ou les Documents sur lesquels sa fonction et ses missions le conduisent à intervenir avant de s'être assuré que cela ne porte aucun préjudice à l'Etablissement. Il respectera les règles et modalités d'archivage dans la mesure où elles sont définies.

L'Utilisateur doit, en outre, enregistrer régulièrement les données qu'il exploite, qu'il crée ou qu'il transforme pour la continuité du service aux endroits adéquats. Toutefois, lorsque les données sont Sensibles, l'Utilisateur s'engage à ne pas les sauvegarder sur un espace de stockage partagé avec des personnes non habilitées à en connaître.

Dans l'hypothèse où l'Utilisateur change de service ou quitte l'Etablissement, il devra suivre la procédure applicable à la transmission des Informations professionnelles qu'il détient par exemple sur ses espaces partagés, sa messagerie ou ses Equipements individuels. En particulier, toute opération d'effacement d'Information devra recevoir de manière générale ou spécifique, l'autorisation de son responsable hiérarchique.

Les Ressources mises à disposition d'un Utilisateur, en particulier les Equipements individuels, sont configurés par le Service Informatique de manière à assurer un niveau de sécurité et de fiabilité optimal. Aussi, l'Utilisateur ne doit jamais de lui-même :

- modifier ou tenter de modifier la configuration et les paramètres de ces Ressources, y compris par l'installation de logiciels ;
- désactiver ou tenter de désactiver les mécanismes de sécurité mis en œuvre (logiciel anti-virus, écran de veille automatique, outils d'authentification, outils de chiffrement de données ou de messages...), ou en changer les paramètres ;
- utiliser ou tenter d'utiliser des outils de sécurité non-fournis par l'Etablissement, notamment en termes de sécurité réseau ou de chiffrement de données ;
- connecter ou tenter de connecter aux Systèmes d'Information de l'Etablissement des Ressources non fournies par l'Etablissement, notamment : modem, périphérique, disques durs externes, graveurs, carte réseau Wifi, logiciel, sauf accord exprès préalable de la Fonction Sécurité des Systèmes d'Information.

6.3 - Usage privé des Ressources

Un usage personnel ponctuel et raisonnable des Ressources (téléphones fixe et portable, messagerie électronique, accès Internet, stockage et échange de fichiers), dans le cadre des nécessités de la vie courante et familiale, est toléré à condition que cet usage soit strictement conforme aux législations et réglementations applicables et respecte la Charte¹, notamment qu'il ne porte pas préjudice à l'activité professionnelle et qu'il ne soit susceptible d'affecter en rien le bon fonctionnement du service et des Ressources (perturbation ou limitation des capacités techniques mises à disposition de l'Utilisateur) ou de mettre en cause l'intérêt et / ou la réputation de l'Etablissement.

Ainsi, seront présumés privés les fichiers et messages qui, lors de leur création, de leur traitement ou de leur conservation auront été clairement identifiés par l'Utilisateur au moyen de la mention suivante et à l'exclusion de toute autre mention telle que « personnel » :

- pour les messages, aussi bien les messages émis que reçus, l'objet du message doit mentionner l'indication « PRIVÉ »²,
- pour les fichiers, les noms des fichiers doivent mentionner l'indication « PRIVÉ » et ils doivent être conservés dans des répertoires spécifiques dont les noms mentionnent l'indication « PRIVÉ ».

Les différentes graphies du terme « PRIVÉ » sont considérées comme valides : en majuscules, minuscules, accentuées ou non...

Tout message ou fichier ne correspondant pas à ces règles est considéré comme professionnel³.

L'Utilisateur est informé que les dispositifs et procédures de contrôle automatiques mis en place par l'Etablissement (ex : antivirus, détection de code malveillant...) s'appliquent à tous les messages et fichiers émis et reçus, sans distinction de la présence ou de l'absence de la mention « PRIVÉ ». En cas de non-respect avéré de l'une de ces dispositions, l'Utilisateur est également informé que l'Etablissement se réserve le droit d'effacer les données correspondantes sans avoir nécessairement à l'en avertir au préalable. L'Utilisateur sera en tout état de cause informé postérieurement par écrit de la mise en œuvre de ces modalités et de leurs motivations, et pourra faire valoir un droit de réponse motivé, les données correspondantes étant sauvegardées pendant les durées prévues pour chaque système.

A ce titre, l'Utilisateur concerné décharge l'Etablissement de toute responsabilité quant à toute conséquence préjudiciable liée aux contrôles réalisés par l'Etablissement (effacement de données, dysfonctionnement, etc.).

Plus généralement, l'Etablissement ne pourra être tenu responsable de toute perte ou altération de quelques données que ce soit relevant de l'usage privé des Ressources.

¹ Cf. ci-dessous les comportements considérés comme abusifs.

² L'Utilisateur devra informer ses correspondants de l'existence de cette règle lors de la communication de son adresse de messagerie à titre privé, et s'assurer du respect de ladite règle dans le cadre de ses communications privées via son adresse de messagerie professionnelle.

³ Par exemple, la fonctionnalité « Critères de diffusion » présente dans le logiciel Outlook de Microsoft Office et permettant à l'Utilisateur de choisir entre les valeurs « normal », « personnel », « privé » ou « confidentiel » n'est pas, pour des raisons techniques, considérée dans la présente Charte comme permettant clairement une identification privée.

En cas de départ définitif de l'Utilisateur, ce dernier prend toutes les dispositions nécessaires pour récupérer ses fichiers privés, étant noté qu'il lui appartient de prendre toutes mesures adéquates pour les protéger des accès de Tiers non autorisés. Il doit notamment identifier les fichiers privés conformément à la règle définie ci-dessus. Il est également rappelé que le chiffrement éventuel des données ne peut être mis en œuvre qu'à l'aide d'outils maîtrisés par l'Etablissement.

L'Utilisateur est informé que l'accès à ses fichiers privés et son compte seront gelés pendant un mois. Au-delà de cette durée, son compte et ses éventuels répertoires privés seront détruits.

6.4 - Comportements abusifs

Par rapport aux règles de bon usage des Ressources, seront notamment considérés comme abusifs au sens de la Charte les comportements visant à organiser la réception, consulter ou tenter de consulter, télécharger, conserver, publier, diffuser ou distribuer, en toute connaissance de cause au moyen des Systèmes d'Information de l'Etablissement, tous programmes, logiciels, documents électroniques, messages, Informations, données :

- à caractère violent, pédopornographique, xénophobe, négationniste, raciste et, plus généralement, contraire à la réglementation en vigueur ;
- susceptibles de porter atteinte au respect de la personne humaine, de sa dignité ou de sa vie privée ;
- à caractère diffamatoire ;
- ayant pour objet le harcèlement, la menace ou l'injure ;
- contenant des éléments protégés par les lois sur la propriété intellectuelle et le droit à l'image, sauf à posséder les autorisations nécessaires ;
- incitant à la commission d'un délit ou d'un crime et, de manière générale, d'actions illicites ou contraires à l'ordre public ;
- contraires aux bonnes mœurs.

Les éléments ci-dessus constituent un rappel de la législation française, plus large que le cadre de cette Charte et qui vont par nature au-delà du contrôle de l'Etablissement. Les tribunaux pourront donc également, le cas échéant, prononcer des sanctions relatives aux comportements abusifs en question.

Par ailleurs, en raison des risques spécifiques encourus par l'Etablissement, seront également considérés comme abusifs au sens de la Charte les comportements visant à organiser la réception, consulter ou tenter de consulter, télécharger, conserver, publier, diffuser ou distribuer, en toute connaissance de cause au moyen des Systèmes d'Information de l'Etablissement, tous programmes, logiciels, Documents électroniques, messages, Informations, données :

- contenant des virus ou des données contaminées ;
- portant sur des Informations internes à l'Etablissement ou confidentielles, au mépris des dispositions internes relatives à la confidentialité des échanges, de l'obligation de loyauté et de discrétion professionnelle, et du secret professionnel ;
- manifestement attentatoires à l'image de marque interne ou externe de l'Etablissement ou à sa réputation.

Seront également considérés comme abusifs : l'utilisation des services Internet à des fins commerciales, ludiques ou illicites, ainsi qu'un usage privé inapproprié des services Internet, du fait notamment de la durée et du volume de connexion.

7- Informatique mobile

Outre le respect des règles définies au chapitre 6, les Equipements individuels mobiles sont soumis aux procédures de sécurité et de contrôle mises en œuvre au sein de l'Etablissement.

Il est rappelé que seuls les Equipements individuels fournis par l'Etablissement et ceux entrant dans le cadre des accords de télétravail sont autorisés à accéder aux Ressources.

L'Utilisateur d'un Equipement individuel mobile doit prendre des précautions supplémentaires par rapport à un Equipement individuel fixe, notamment pour éviter le vol de cet équipement et la perte des données qui y sont stockées :

- la plupart des données professionnelles stockées sur un Equipement individuel mobile sont régulièrement sauvegardées, via un mécanisme de synchronisation, dans l'espace de travail alloué à l'Utilisateur sur le serveur de fichiers correspondant à son service (cf. chapitre 14), via un mécanisme automatique que l'Utilisateur ne doit en aucune manière chercher à bloquer ou désactiver ;
- lorsque l'Utilisateur laisse son Equipement individuel mobile dans des locaux sous le contrôle de l'Etablissement ou sous son propre contrôle (domicile), il doit assurer la protection de cet équipement, à l'aide des moyens mis à disposition par l'Etablissement (par exemple, attaché à un bureau avec un câble de sécurité, conservé dans une armoire ou un tiroir fermés à clé...) ;
- en dehors des locaux mentionnés au point précédent, l'Utilisateur doit veiller à ne pas laisser son Equipement individuel mobile sans surveillance (chambres d'hôtel, voitures, lieux publics...) ;
- lorsque l'Utilisateur ne se sert pas de son Equipement individuel mobile, il doit en verrouiller l'accès logique.

8- Messagerie électronique

8.1 - Principes généraux

La messagerie électronique est un outil d'échange d'Informations, mais peut également être le vecteur de propagation de virus ou d'informations inutiles voire fausses (ex : canulars), ce qui peut notamment se traduire par des pertes de temps et de productivité pour les Utilisateurs.

Afin de s'assurer que cet outil joue correctement et uniquement son rôle d'échange d'informations efficaces, outre le respect des règles définies au chapitre 6, certaines règles spécifiques sont à respecter, notamment :

- Les seuls outils de messagerie électronique autorisés à des fins professionnelles au sein de l'Etablissement sont les outils de messagerie gérés et exploités par le Service Informatique (interdiction d'utilisation de messageries privées à des fins professionnelles).
- La taille des boîtes aux lettres est limitée. Des dépassements de seuil peuvent être autorisés de manière dérogatoire.
- La messagerie électronique ne doit pas être utilisée pour des envois en nombre pouvant encombrer le réseau (notamment lors de l'utilisation inappropriée de listes de diffusion). La hiérarchie seule peut décider de ce type d'envoi, dans le cadre des procédures en vigueur dans chaque entité.
- L'Utilisateur doit s'assurer du bien-fondé des messages qu'il émet vers ses correspondants et rester vigilant, et ainsi ne pas transmettre en connaissance de cause de fausses alertes ou canulars circulant par messagerie.
- L'Utilisateur doit veiller à la protection des Informations diffusées par messagerie. Il est rappelé que la confidentialité des échanges n'est pas techniquement assurée par la messagerie électronique en elle-même. En conséquence, celle-ci ne doit pas être utilisée sans sécurisation appropriée pour les échanges d'Informations ou de Documents à caractère confidentiel ou Sensible, même à titre de projets. Par sécurisation, on entend des outils supplémentaires, fournis et maîtrisés par l'Etablissement. Chaque Utilisateur qui diffuse ou transfère des messages par courrier électronique est entièrement responsable du respect de la confidentialité qui y est attachée.
- L'Utilisateur ne doit, en aucun cas, organiser le reroutage automatique de ses messages vers une adresse de messagerie externe à l'Etablissement, afin d'éviter que des messages sensibles ne se trouvent envoyés sur Internet à l'insu de l'émetteur.
- En cas d'absence d'un Utilisateur et pour des raisons de continuité de service, la mise en place d'un message d'absence dans la messagerie de cet Utilisateur à la demande d'une autre personne que l'Utilisateur concerné, nécessite une autorisation explicite et préalable de la Fonction Sécurité des Systèmes d'Information, et fera l'objet d'une information ultérieure de l'Utilisateur concerné.
- L'Utilisateur doit faire preuve de vigilance vis-à-vis de l'identité des auteurs des messages reçus, notamment de correspondants extérieurs. En effet, l'usurpation de l'identité de l'auteur d'un message est facilement réalisable sur Internet.
- Les boîtes aux lettres font l'objet de sauvegardes centralisées, conservées sur une période maximale de six mois.

De plus, l'Utilisateur s'interdit d'envoyer des messages en « masse » (« spamming ») et de répondre à des « chaînes » de messages. Si l'Utilisateur reçoit des messages qui lui demandent de les transmettre à toutes les personnes qu'il connaît, il ne doit pas les diffuser mais les supprimer immédiatement de sa boîte aux lettres.

L'inscription sur des listes de diffusion externes est réservée à un usage strictement professionnel. En outre, l'Utilisateur doit systématiquement vérifier, lors de l'inscription, qu'il existe une procédure de désabonnement et se désabonner lorsque la liste de diffusion n'est plus utilisée ou en cas de départ de l'Etablissement.

D'une manière générale, l'utilisation de la messagerie doit être conforme à la réglementation applicable et aux prescriptions de la Charte et, notamment, ne doit pas porter atteinte à l'image, à la réputation, à la sécurité d'autrui ou de l'Etablissement ni au bon fonctionnement des Ressources.

L'Utilisateur ne doit jamais écrire dans un message électronique ce qu'il s'interdirait d'exprimer par tout autre moyen, notamment par oral, courrier papier ou téléphonie (propos discriminatoires, racistes, injurieux ou malveillants, etc.). Par ailleurs, il s'engage à ne pas ouvrir les messages ainsi que les fichiers attachés aux messages qu'il reçoit et pour lesquels il a des doutes concernant l'émetteur et/ou le contenu. Il doit les signaler dans un bref délai au Service Informatique ou à la Fonction Sécurité des Systèmes d'Information, notamment à l'aide de la boîte POURRIEL@caissedesdepots.fr.

L'Utilisateur doit être conscient du fait qu'un message électronique peut constituer un élément de preuve susceptible de l'engager et/ou l'Etablissement.

Par exception au principe d'utilisation à des fins professionnelles, il est toléré un usage à titre privé de la messagerie mise à disposition par l'Etablissement, dans les conditions fixées au chapitre 6.3 (utilisation limitée et raisonnable, Marquage des messages à caractère privé...). Cette exception s'applique préférentiellement aux échanges entre individus, l'utilisation de l'adresse professionnelle comme support d'échanges privés avec des entités commerciales, associatives... étant fortement déconseillée. L'inscription, pour des besoins privés, sur des sites Internet, des réseaux sociaux, des lettres d'information doit donc privilégier les adresses électroniques privées des individus afin de préserver la messagerie de l'Etablissement d'attaques pouvant les viser dans leurs activités privées.

8.2 - Comportements abusifs

Outre les différents points explicités au chapitre 6.4, seront notamment considérés comme abusifs :

- La copie partielle ou totale ou la réutilisation de tout ou partie des listes de diffusion internes ou externes (listes créées par l'Etablissement exclusivement à des fins professionnelles ou de gestion interne). Afin d'éviter de perturber le bon fonctionnement du réseau, l'Utilisateur ne pourra utiliser une de ces listes qu'avec l'autorisation des gestionnaires de ces listes.
- Un usage privé inapproprié de la messagerie, du fait notamment de la fréquence trop importante des messages reçus ou envoyés, du volume de données échangées (messages et pièces jointes), du transfert de messages professionnels Sensibles, ainsi qu'en cas d'utilisation abusive ou malveillante de la mention « PRIVÉ ».

9- Usage des services Internet

9.1 - Principes généraux

La dépendance croissante des Systèmes d'Information à l'égard des services offerts par Internet (sites Internet, forums d'échanges et de discussions, réseaux sociaux, stockage et échange de fichiers, applications en ligne, etc.⁴) met en évidence de nouveaux risques auxquels il faut être particulièrement attentif.

L'accès aux services Internet doit se faire dans le respect des règles d'accès et d'usage des Ressources définies aux chapitres 5 et 6 (autorisations d'accès, non-contournement des dispositifs de protection, non-atteinte à la confidentialité des Informations, usage limité à titre privé...). De plus, l'utilisation de ces services Internet doit se faire dans le cadre strict des droits accordés et des accès autorisés, et dans le respect des principes et règles propres aux divers services concernés. L'Utilisateur ne doit pas se

⁴ Le service de messagerie électronique par Internet est traité au chapitre 8.

connecter ou essayer de se connecter à un service Internet autrement que par les dispositions prévues ou sans y être dûment autorisé.

De manière préventive, l'Etablissement met en œuvre un certain nombre de dispositifs de Filtrage de sites, notamment ceux dont le contenu peut être contraire à l'ordre public ou aux bonnes mœurs.

Ces dispositifs sont décrits dans la politique d'accès à Internet disponible sur l'Intranet de l'Etablissement.

En outre, la loi et les règlements varient en fonction des Etats ; chaque Utilisateur doit rester attentif au respect des réglementations applicables aux services Internet qu'il utilise.

L'Utilisateur s'engage à utiliser les services Internet à des fins professionnelles. Notamment, l'Utilisateur ne doit pas créer ou mettre à jour, au moyen de l'accès à Internet qui est fourni par l'Etablissement, tout site Internet (notamment, page personnelle, journal personnel en ligne, site Internet collaboratif, etc.) en dehors du cadre strictement professionnel et dûment autorisé. L'utilisation de services Internet à des fins privées est une simple tolérance, ayant un caractère nécessairement exceptionnel, sous réserve du respect des règles de la Charte et du fait que la durée et le volume de connexion restent raisonnables.

L'Utilisateur ne doit pas stocker, échanger ou faire traiter des Informations professionnelles par des services Internet sans autorisation explicite préalable de l'Etablissement et la mise en œuvre si nécessaire, par le Service Informatique, de mesures de protection adéquates.

L'Utilisateur est informé des risques liés à l'utilisation des services d'échanges et de communications d'Information (forums, réseaux sociaux et autres services collaboratifs) :

- d'une part, au regard des risques d'encombrement, d'engorgement et de ralentissement des connexions ;
- d'autre part, au regard de la responsabilité de l'Utilisateur, vis-à-vis de l'Etablissement et des Tiers, sur les propos émis et les informations échangées et communiquées.

Il en résulte que l'Utilisateur n'est pas autorisé à utiliser ces services collaboratifs à titre professionnel en dehors de la stricte nécessité de ses fonctions au sein de l'Etablissement et explicitement autorisés par l'Etablissement (par exemple, réseau social interne à l'Etablissement). Dans le cadre de ce type de participation, l'Utilisateur est notamment tenu de :

- Respecter l'ensemble des règles de la Charte.
- Faire preuve de politesse et de la plus grande correction à l'égard de ses interlocuteurs lors d'échanges électroniques (courrier, forums de discussion...).

10- Protection de l'Information

La protection de l'Information vise avant tout à assurer sa disponibilité, son intégrité et sa confidentialité (communication de l'Information aux seules personnes « habilitées à en connaître »). En la matière, la vigilance de chaque Utilisateur est fondamentale, dans la mesure où les seules dispositions organisationnelles et techniques ne sont pas suffisantes.

10.1 Confidentialité

Les moyens de protection des informations (restrictions des accès, chiffrement, possibilité de blocage, journalisation des actions...) sont définis en cohérence avec les niveaux de confidentialité retenus et en fonction du cycle de vie de l'Information.

En tout état de cause, les obligations inhérentes au devoir de réserve, à l'obligation de loyauté et au respect du secret professionnel s'appliquent à l'utilisation des Ressources mises à disposition des Utilisateurs par l'Etablissement.

Chaque Utilisateur doit être vigilant quant au risque de divulgation ou de publication des Informations qu'il utilise dans l'exercice de ses fonctions particulièrement lorsque sont utilisés des moyens de communications électroniques. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont applicables quel que soit le support de communication utilisé.

Chaque Utilisateur est ainsi tenu à une obligation générale de confidentialité, de discrétion et de probité en toutes circonstances et doit, en particulier, éviter en dehors de sa propre activité professionnelle, tout usage ou toute communication d'Information, données et Documents concernant ou en provenance de l'Etablissement, ses partenaires, ses clients, ses fournisseurs et ses personnels, que ce soit sous forme orale ou écrite (articles de presses, publication sur Internet de type forum ou réseaux sociaux...).

Notamment, l'Utilisateur ne doit pas :

- Détourner ou utiliser des Informations propres à l'Etablissement à des fins notamment de concurrence déloyale, émettre de fausses déclarations visant à falsifier les données de l'Etablissement, supprimer ou modifier des données au préjudice de l'Etablissement.
- Mettre à disposition d'autrui des Informations Sensibles sans y être préalablement autorisé.
- Répondre aux sollicitations externes visant à l'obtention de renseignements liés à l'Etablissement et son activité (démarchage téléphonique, courrier électronique, enquêtes, etc.).

Chaque Utilisateur doit être vigilant sur le risque de divulgation dans le cadre d'utilisation d'Equipe-ments individuels mobiles en dehors des locaux de l'Etablissement (hôtels, lieux publics, transports...).

10.2 - Politique de lutte contre la fuite d'Information

L'Utilisateur veillera en particulier à respecter la Politique de lutte contre la fuite de l'information disponible sur l'Intranet Sécurité des Systèmes d'Information, laquelle se déroule en différentes étapes : classification, marquage, protection et contrôle de l'Information.

- Classification et Marquage des Documents : chaque Utilisateur doit s'assurer que les Documents qu'il traite sont classifiés en évaluant l'incidence (financière, organisationnelle, juridique, sociale et d'image) d'une divulgation (en interne ou externe) de ces Informations en suivant la matrice d'impact présentée dans la Politique de lutte contre la fuite d'information. Un marquage visuel correspondant à la classification sera automatiquement apposé sur les documents (« public », « interne », « confidentiel », « secret »).

- Protection des Documents : l'Utilisateur doit veiller à protéger les documents qu'il manipule avec les outils mis à sa disposition et à adapter le niveau de protection qui leur est appliqué en fonction du contexte d'utilisation (restriction des accès, diffusion, chiffrement, destruction). Les Utilisateurs doivent utiliser les logiciels et les outils de protection attribués par l'Etablissement selon la Confidentialité des Informations.
L'Utilisateur devra uniquement utiliser les logiciels et outils de chiffrement mis à sa disposition par l'Etablissement, à l'exclusion de tout autre qui n'a pas été agréé.
- Contrôles : la mise en place de mesures de contrôle spécifiques permet de lutter contre la fuite d'Information. Ainsi des outils de détection (ex : le DLP – *Data Leaks Prevention*) associés aux mécanismes de supervision des incidents doivent permettre de s'assurer que les Informations Sensibles ne sont pas manipulées de manière inappropriée (notamment la diffusion), que ce soit en externe ou en interne de l'Etablissement.

11- Contrôle de l'usage des Ressources

Des mesures de contrôle et de suivi sont mises en œuvre dans le strict respect des principes de transparence et de proportionnalité des moyens de collecte, ceci à des fins de sécurité et de vérification du bon accès et usage des Ressources. Ces traitements de données automatisés font l'objet des formalités conformément aux dispositions relatives à la protection des données à caractère personnel.

L'ensemble des outils de sécurité déployés dans les Systèmes d'Information de l'Etablissement (anti-virus, filtrage des flux, lutte contre la fuite d'information...) participent à ce contrôle. Outre leur fonction première qui est de mettre un terme aux menaces qu'ils détectent, ces outils génèrent des événements de sécurité qui sont agrégés dans un environnement technique dédié, permettant leur corrélation et analyse par les personnes habilitées du centre opérationnel de sécurité. En cas de nécessité de preuves et de traces numériques plus complètes, l'Etablissement peut également mettre en œuvre des outils d'investigations avancées (dits « *forensic* »).

Les données et traces informatiques enregistrées dans le cadre de ces mesures portent sur l'identification du compte de l'Utilisateur, la date et heure de l'action considérée, la nature et les résultats de l'action.

Ces données et traces informatiques sont conservées pendant une période maximale de un an (sauf obligations légales ou réglementaires particulières de conserver ces données sur une durée plus longue ; ex : délais de prescription) et font l'objet de mesures de protection adaptées contre tout risque avéré de divulgation et d'utilisation abusive.

Par la présente Charte, l'Utilisateur est donc informé de la mise en place de dispositifs de sécurité visant à collecter des informations concernant son usage des Ressources mises à sa disposition conformément à la réglementation en vigueur, avec comme objectifs :

- de garantir le bon fonctionnement de ces Ressources,
- de lutter contre la fuite d'Informations Sensibles ou la violation de la confidentialité des données à caractère personnel,
- de pouvoir identifier et, le cas échéant, sanctionner des usages contraires à la présente Charte, aux législations et réglementations applicables,
- de traiter les procédures juridictionnelles (judiciaires et administratives), et notamment de pouvoir répondre aux requêtes des autorités compétentes (services de police, autorités judiciaires...).

11.1 Contrôles automatisés

Journal d'exploitation

Le Système d'Information génère des journaux d'événements (dits « logs ») créés automatiquement par les équipements informatiques et de communication électronique. Ils permettent de retracer la vie du Système d'Information de l'Etablissement et les actions qui y sont menées, et sont stockés sur les postes informatiques et le réseau. Ils contribuent à assurer le bon fonctionnement du système et la sécurité des Informations de l'Etablissement, à travers la détection des erreurs matérielles ou logicielles, et le contrôle des actions des Utilisateurs et des Tiers accédant au Système d'Information.

Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des Ressources, pour contrôler l'accès, les modifications et suppressions de données ;
- aux connexions entrantes et sortantes au réseau interne, aux applications, à la messagerie et à Internet, afin de détecter les anomalies liées à l'utilisation des Ressources et prévenir les activités malveillantes.

Navigation sur Internet

Outre le blocage des sites non autorisés, chaque connexion ou tentative de connexion pour la navigation sur Internet fait l'objet d'un contrôle : sites visités, durées de connexion, éléments téléchargés ainsi que leur type.

Interruption de flux chiffrés

Afin de permettre la recherche de logiciels malveillants et de lutter contre la fuite d'Information, les flux chiffrés (repérables par une URL commençant par « <https://...> ») sont systématiquement interrompus par l'Etablissement le temps d'opérer ces contrôles de sécurité, puis sont à nouveau chiffrés pour en assurer la protection sur le reste de leur parcours.

Les deux contrôles précédents sont décrits de manière opérationnelle dans la « Politique d'accès à Internet », consultable sur l'Intranet Sécurité des SI à l'adresse <http://cdcmedia.serv.cdc.fr/securite-si/>, section « Documents de référence ».

Filtrage

Des systèmes de filtrage peuvent être mis en œuvre pour analyser les messages entrants et sortants (contrôle antivirus, contrôle anti-spam, contrôle de la taille, liste des destinataires, etc.) et également pour bloquer, notamment sur la base de listes de mots-clefs, des actions non autorisées (envois de messages électroniques, copies de fichiers, impressions de documents...).

Statistiques

Les données et traces informatiques font l'objet de traitements automatisés à des fins statistiques (nombre de messages émis vers ou reçus d'Internet, volumes occupés par l'ensemble des boîtes aux lettres, sites Internet les plus visités, taille des espaces sur les serveurs de fichiers, durées totales des connexions distantes, etc.).

11.2 Investigations

L'Utilisateur est informé que des contrôles individualisés pourront être diligentés, suite à un dysfonctionnement des Systèmes d'Information de l'Etablissement, à une alerte de sécurité et également en cas de suspicion d'un usage non conforme de ces Systèmes d'Information, sous réserve du respect des dispositions légales applicables.

Dans ce cadre, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront l'incident sur l'éventuelle réalisation d'un fait constitutif d'une faute et sur l'identification de ses auteurs.

Lors de ces investigations, menées par la Fonction Sécurité des Systèmes d'Information de l'Etablissement, le concours de l'Utilisateur pourra être sollicité afin d'accélérer l'analyse de la situation et ainsi préserver le fonctionnement du Système d'Information.

Au besoin, et en fonction du résultat des contrôles opérés, l'accès à certaines Ressources (sites visités depuis le réseau de l'Etablissement, partages de fichiers, etc.) pourra être interdit sans préavis ni information.

11.3 – Spécificité des Informations « privées »

En cas d'alerte de sécurité, de dysfonctionnement ou d'anomalie, il peut être procédé à un contrôle manuel et à une vérification de toutes opérations effectuées par un ou plusieurs Utilisateurs.

Tout message et tout fichier qui n'est pas explicitement identifié comme « PRIVÉ » étant considéré comme professionnel, l'Etablissement peut y accéder pour les besoins exceptionnels rappelés ci-dessus, via des personnels habilités, dans le strict respect de la réglementation applicable ainsi que des règles de sécurité supplémentaires que s'impose l'Etablissement. Après que l'intéressé ait été dûment convoqué, ces règles prévoient notamment que sa présence et/ou celle d'un représentant du personnel est nécessaire à la mise en œuvre de ces opérations exceptionnelles.

Conformément à la législation en vigueur relative à la protection des correspondances privées, le contenu des messages et des fichiers portant explicitement la mention « PRIVÉ » ne pourra dès lors être consulté que par les autorités judiciaires ou policières compétentes, ou sur accord exprès de l'Utilisateur.

11.4– Droit syndical et instances représentatives du personnel

11.4.1 Principes généraux

Par ailleurs, les Ressources mises à disposition des représentants du personnel de l'Etablissement, quel que soit le statut public ou privé dont ils relèvent, font l'objet de dispositions particulières détaillées dans le document relatif aux règles d'utilisation des moyens de communication électronique par les organisations syndicales. De ce fait, les messages à caractère syndical, émanant ou à destination d'une boîte fonctionnelle syndicale ou de la boîte d'un permanent syndical, sont considérés comme « PRIVE » au sens de la présente Charte, même s'ils ne sont pas explicitement identifiés comme tels. Les messages émanant ou à destination de la boîte d'un agent non permanent syndical, titulaire d'un ou plusieurs mandats de représentant du personnel, élu ou désigné, ne peuvent être consultés, dans le cadre de la procédure exceptionnelle prévue par la Charte (cf. article 11.2), qu'après accord du dirigeant (ou de l'un des dirigeants) de l'organisation syndicale au sein de l'établissement auquel il appartient, afin de s'assurer qu'ils ne relèvent pas de son activité syndicale ou de représentation du personnel. S'ils relèvent de son activité syndicale ou de représentation du personnel, les messages sont considérés comme « PRIVÉ » au sens de la Charte.

11.4.2 Autres situations

Enfin, les communications émises ou reçues dans le cadre d'une activité protégée par des dispositions légales (ex : secret médical) sont également considérées « PRIVE » au sens de la présente Charte, même si elles ne sont pas explicitement identifiées comme telles.

12- Continuité de service

Afin d'assurer une continuité de service, il est rappelé le principe de stocker les fichiers sur les espaces partagés afin de faciliter l'accès aux fichiers professionnels par les personnes habilitées.

Toutefois, à titre exceptionnel et sur demande expresse du responsable hiérarchique auprès de la Fonction Sécurité des Systèmes d'Information et suite à l'approbation de cette dernière, les Administrateurs peuvent être amenés à prendre les mesures nécessaires afin d'accéder aux Ressources mises à disposition de l'Utilisateur absent.

Pour les besoins de leur intervention et/ou pour des raisons techniques, les Administrateurs peuvent être amenés à invalider le ou les codes d'accès confidentiels de l'Utilisateur concerné. À titre d'exemple, ce type d'intervention qui doit rester exceptionnel, peut avoir pour finalité de mettre en place le message d'absence de bureau de l'Utilisateur concerné, ou encore de donner accès à un autre Utilisateur aux dossiers et fichiers professionnels détenus par l'Utilisateur concerné.

L'Utilisateur à qui est donné l'accès à ces Ressources est informé qu'il doit respecter le secret de la correspondance privée et qu'il lui est interdit de prendre connaissance d'éventuels contenus marqués « PRIVÉ » sous peine de voir sa responsabilité engagée.

L'Utilisateur absent est informé à son retour de la nature et des motifs de l'intervention. À cette occasion, il est également invité à renouveler ses Authentifiants et à les garder secrets.

13- Rôle des Administrateurs

13.1 - Missions et rôle des Administrateurs

Les missions des Administrateurs portent essentiellement sur la qualité et la sécurité des Systèmes d'Information de l'Etablissement. Les Administrateurs sont garants du bon fonctionnement et de la sécurité des Ressources ainsi que de la disponibilité des données et des applications informatiques de l'Etablissement.

Dans l'exercice de ces missions, les Administrateurs veillent à faire respecter les droits et devoirs des Utilisateurs qui sont définis par la Charte et en application des dispositions légales et réglementaires.

En conséquence, par leurs fonctions mêmes et dans le cadre de leurs missions, les Administrateurs ont la capacité technique d'accéder à l'ensemble des informations présentes sur les Systèmes d'Information. Ils ne doivent pas accéder aux messages et fichiers marqués « PRIVÉ », en dehors de la procédure mentionnée aux présentes.

Seuls les Administrateurs sont autorisés à introduire dans les Systèmes d'Information de nouveaux matériels ou logiciels.

13.2 - Droits des Administrateurs

Les Utilisateurs sont informés que les Administrateurs peuvent avoir accès à l'ensemble des Systèmes d'Information de l'Etablissement, à n'importe quel moment et ce afin d'effectuer tout acte de protection, ce qui peut notamment comprendre :

- la sauvegarde, la conservation et la diffusion des Informations collectées et traitées dans le cadre des activités de l'Etablissement ;

- la preuve de la date de création ou de la diffusion desdites Informations ;
- la protection de l'intégrité et de la confidentialité des données et du fonctionnement des Systèmes d'Information ;
- la suspension ou la suppression des Habilitations ;
- la vérification de l'absence d'intrusion dans les Systèmes d'Information, en violation des dispositions légales et réglementaires en vigueur ;
- la mise à jour, la maintenance, la correction et la réparation des matériels et logiciels nécessaires à l'utilisation des Systèmes d'Information.

L'Administrateur se réserve le droit, à tout moment et sans préavis, de supprimer, le cas échéant, tout élément ou information apporté ou installé par l'Utilisateur qui serait susceptible de porter atteinte au bon fonctionnement des Systèmes d'Information.

Seuls les Administrateurs du Service Informatique sont autorisés à prendre la main à distance sur les Equipements individuels des Utilisateurs afin de résoudre les problèmes signalés auprès du Service Informatique.

Durant les heures ouvrées, la prise de main à distance devra être réalisée avec l'accord préalable de l'Utilisateur. Par exception, en cas de situation grave, et notamment en cas d'attaque virale, la prise de main pourra être réalisée sur tous les Equipements individuels jugés suspects. Toutefois, cette prise de main sans autorisation ne sera légitime que dans les cas où ces Equipements individuels présentent un danger pour les Systèmes d'Information de l'Etablissement. En tout état de cause, les Administrateurs sont tenus d'en informer préalablement la Fonction Sécurité des Systèmes d'Information de l'Etablissement, ainsi que les Utilisateurs concernés dès lors que le Système d'Information sera à nouveau sécurisé.

13.3 - Devoirs des Administrateurs

Les Administrateurs sont tenus à une obligation de confidentialité stricte. Sauf dans les cas où sa responsabilité pénale est susceptible d'être engagée et également dans les cas où la sécurité ou le bon fonctionnement des Systèmes d'Information sont menacés ainsi que l'intérêt de l'Etablissement, un Administrateur ne doit pas utiliser ou divulguer les informations couvertes par le secret professionnel ou le secret des correspondances privées, et, de façon plus générale, toutes les Informations relatives à la vie privée des Utilisateurs.

14- Stockage des Informations

Les informations appartenant à l'Etablissement ne doivent être stockées que sur les emplacements prévus à cet effet.

14.1 - Stockage sur le réseau

Outre les éventuels dispositifs de stockage externes disponibles avec les ordinateurs attribués par le Service Informatique (graveurs de support magnétique ou optiques, clés USB, disques durs externes...), d'autres espaces de stockage sont accessibles, tels que les serveurs de fichiers. Ces derniers permettent le partage de Documents professionnels au sein d'une même entité ou d'un même service, ou

encore pour certains d'entre eux, le stockage de documents professionnels Sensibles de l'Etablissement (stockage dans un espace individuel sur ces serveurs de fichiers). Pour ces raisons, ces espaces sont sauvegardés automatiquement et régulièrement par le Service Informatique. Les services externalisés d'informatique en nuage (*Cloud*) expressément autorisés peuvent également être utilisés à ces fins.

Chaque Utilisateur doit ainsi veiller à ce que les Informations utiles à son service d'appartenance soient stockées dans ces espaces, pour lesquels des dispositions de sauvegarde sont assurées.

Les Utilisateurs ne doivent en aucun cas utiliser ces espaces et les serveurs partagés de façon générale pour stocker et/ou partager tout fichier, multimédia (musiques, photos, vidéos) ou autre qui ne serait pas strictement professionnel.

En tout état de cause, tout stockage de fichier extraprofessionnel ne pourra s'opérer que sur les Equipements individuels de l'Utilisateur à l'exclusion de tout espace partagé. Celui-ci devra s'assurer de la parfaite innocuité de ces fichiers pour les Ressources de l'Etablissement. Il ne devra pas perturber ou limiter les capacités techniques mises à sa disposition à une fin professionnelle et devra respecter l'ensemble des dispositions réglementaires applicables aux contenus stockés ou utilisés (droit d'auteur, droit à l'image, etc.) Ces fichiers ne doivent en aucun cas être susceptibles de porter atteinte à l'image de l'Etablissement.

L'Utilisateur ne devra conserver des Documents Sensibles sur un Equipement mobile que si les mesures de protection appropriées et prévues par l'Etablissement pour préserver la confidentialité des Informations temporairement stockées ont bien été mises en œuvre.

L'Utilisateur veillera particulièrement à respecter les règles internes sur la confidentialité lors de son utilisation des moyens de communication électronique mis à sa disposition et à ne pas disséminer en dehors de l'Etablissement des Documents auxquels il a eu accès dans le cadre professionnel, notamment par voie de stockage sur des supports ou services acquis à titre privé (ex : transferts de fichiers, messageries privées...).

En cas de suspicion de non-respect de l'une quelconque des dispositions de la Charte concernant les fichiers extraprofessionnels, l'Etablissement se réserve notamment la possibilité de retirer et/ou d'effacer les contenus stockés sans avoir à en avertir préalablement l'Utilisateur.