Charte d'Utilisation des Ressources des Systèmes d'Information de l'Établissement Public Caisse des Dépôts

Juin 2022

Table des matières

Remarque : A la suite de la consultation des instances, un nouvel arrêté du Directeur général relatif à la charte d'utilisation des ressources des systèmes d'information de la Caisse des dépôts et consignations, sera pris. Il abrogera et remplacera celui du 13 avril 2018 actuellement en vigueur. Cet arrêté sera inséré dans le document porté à la connaissance des personnels.

1. Objet

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

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'Établissement.

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'Établissement et de le responsabiliser ;
- de préciser les principaux droits, les devoirs et les responsabilités des utilisateurs des systèmes d'information de l'Établissement, en conformité avec les législations et réglementations en vigueur, les règles de déontologie, ainsi que les règles et recommandations en vigueur dans l'Établissement, en particulier la Politique 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'Établissement ;
- de prévenir la divulgation de Données Sensibles à des personnes non autorisées, ou encore les intrusions de tiers non autorisés dans tout ou partie du Système d'Information.

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

La Charte a été soumise à l'avis du Comité unique de l'établissement public de la Caisse des dépôts et consignations et du Comité santé, sécurité et conditions de travail (CSSCT), compétents pour l'ensemble des collaborateurs de l'Établissement public. Elle est annexée 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.

La mise en œuvre la Charte est un gage de protection de l'Utilisateur dans son utilisation quotidienne des Systèmes d'information de l'Etablissement et contribue à garantir un environnement sécurisé pour l'Etablissement.

Ce document annule et remplace toutes ses précédentes versions.

2. Application et mesures en cas de non-respect

2.1. Portée

La présente Charte s'adresse à tout Utilisateur qui utilise les Ressources des Systèmes d'Information de l'Établissement, quel que soit son statut (public, privé, intérimaires, stagiaires, etc.), à l'exception des prestataires de services.

Les règles de sécurité des systèmes d'informations applicables aux prestataires de services sont précisées dans le document « Règles de Sécurité des Systèmes d'informations pour les Prestataires de Services (RSSIPS) ».

2.2. Date d'entrée en vigueur

La présente Charte entre en vigueur à compter du *(date fixée postérieurement à la consultation des instances)*

2.3. Information et sensibilisation des Utilisateurs

La Charte est annexée au Règlement intérieur. Elle est également portée à la connaissance de tous les Utilisateurs, par les différents moyens mis en œuvre par l'Établissement. Constituent notamment un moyen adéquat l'un des moyens suivants : diffusion sur la plate-forme de travail collaboratif de l'Établissement (Intranet « next »), 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'Établissement en matière de sécurité des systèmes d'information et à consulter la Charte afin d'appliquer les règles d'utilisation prévues par la présente Charte.

2.4. Mesures en cas de non-respect

Tout Utilisateur des Systèmes d'Information de l'Établissement 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, que ce soit en commettant un fait prohibé, en tentant de commettre un fait prohibé, ou en s'abstenant d'exécuter un acte prescrit, l'Établissement peut notamment restreindre ou révoquer sans préavis les

droits d'accès aux ressources (messagerie, Internet…). L'Utilisateur est alors informé par écrit des constats motivant l'intervention et pourra faire valoir sa position.

L'Établissement 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.

3. Définitions

Administrateur : au sein du Service Informatique ou des directions et services de l'Établissement, 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, clé cryptographique privée 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 courriel, un projet, une application, etc. Cinq niveaux de classification sont mis en œuvre par l'Etablissement : "privé", "C1 - Public", "C2 - Interne", "C3 - Confidentiel", "C4 - Secret".

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 (électronique) : lorsqu'il est électronique, un document est une forme de représentation de l'information consultable à l'aide d'un équipement électronique. Cela comprend notamment les courriels, vidéos, photographies, etc. Il peut être enregistré sous forme de fichiers ou stocké dans des bases de données.

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.

Donnée Sensible :

- les informations dont la Classification est "C4 - Secret" ;

- les Données à caractère personnel suivantes :

    - les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne de manière unique, les données concernant la santé ou la vie sexuelle ou l'orientation sexuelle d'une personne.

    - les données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté ;

    - le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ;

    - les données dont la violation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (ex. : données bancaires susceptibles d'être utilisées pour des paiements frauduleux telles que les numéros de comptes ou de cartes bancaires).

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

Fonction Sécurité des Systèmes d'Information : au sein de l'Établissement, 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'Établissement tels que les correspondants sécurité.

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

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 la Classification d'un Document.

Moyens Personnels : équipements individuels et systèmes d'information et de communication qui sont la propriété d'un Utilisateur ou qu'il détient à titre personnel.

Ressource (du Système d'Information) : tout élément intervenant dans la mise en œuvre et le fonctionnement du 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.).

Règlement général sur la protection des données (RGPD) : règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Service Informatique : ensemble des fonctions de l'Établissement 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.).

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.

Utilisateur : toute personne, à l'exception des prestataires de services, qui accède à, ou utilise, des Systèmes d'Information de l'Établissement, de manière permanente ou occasionnelle. Les Administrateurs sont des Utilisateurs.

4. Législation / Réglementation

4.1. Principes généraux

Dans le cadre de l'usage des Ressources mises à sa disposition par l'Établissement, 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 interdit 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, œuvres audiovisuelles ou musicales, textes, etc. protégées par le droit d'auteur, et d'autre part, pour les marques, dessins et modèles et bases de données protégés par un droit de propriété intellectuelle.
- La réglementation relative à la protection des Données à caractère personnel, qui responsabilise les organismes traitant des Données à caractère personnel et qui renforce les droits des personnes dont les données sont traitées. La loi du 6 janvier

1978 modifiée, dite « Informatique et Liberté » et le Règlement général sur la protection des données (RGPD) du 27 avril 2016 obligent à traiter les données personnelles de manière loyale, transparente et sécurisée dans le respect du droit des personnes. Cette réglementation rappelle les grands principes suivants : une collecte loyale, transparente, adéquate et minimisée des données, une utilisation légitime et proportionnée, la limitation de leur conservation, leur Confidentialité et Intégrité et une protection dès la conception et par défaut. 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. Respect de la propriété intellectuelle

Chaque Utilisateur doit respecter des règles de bon usage et ne pas installer ou copier, sur les Ressources de l'Établissement, de logiciels, même ceux gratuitement disponibles.

Sous réserve des règles internes applicables, en particulier celles relatives à la conformité logicielle et à la sécurité, le téléchargement et l'installation de logiciels sont interdits. En vue d'accorder, le cas échéant, de telles autorisations, le Service Informatique procédera 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'Établissement doivent tous être utilisés et exploités exclusivement dans les conditions des licences souscrites par l'Établissement et sous réserve des autorisations nécessaires, y compris les logiciels à code source ouvert (dit « open source »).

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'Établissement qui est seul habilité à les exercer.

Il est rappelé à l'Utilisateur que les 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 pour porter atteinte aux droits de propriété intellectuelle de l'Établissement 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'Établissement 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 en dehors des possibilités légales ou contractuelles qui lui sont reconnues.

Il est également rappelé que, lors de l'usage de services Internet (réseaux sociaux, webmails, services de partage de fichiers ou de données, etc.), 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'Établissement.

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'Établissement lors de l'utilisation de services Internet tels que les réseaux sociaux.

5. Accès aux Ressources

L'accès aux Ressources de l'Établissement est géré par le Service Informatique, habilité à délivrer les Moyens d'authentification à chaque Utilisateur, selon les procédures 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'Établissement n'est possible que dans le cadre de l'activité professionnelle de l'Utilisateur concerné au sein de l'Établissement, 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'Établissement.

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 et non transmissibles, l'Utilisateur étant responsable de leur sécurité. En conséquence, il lui est interdit :

- d'inscrire les mots de passe 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 perte ou de suspicion de compromission d'un Moyen d'authentification, l'Utilisateur doit alerter le Service Informatique dans les meilleurs délais et demander son changement.

Sauf preuve contraire, les utilisations faites à l'aide d'un Moyen d'authentification propre à chaque Utilisateur sont réputées être le fait du détenteur légitime de ce Moyen d'authentification.

Il est également précisé que l'accès de l'Utilisateur aux Ressources de l'Établissement 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'Établissement (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 écrit et motivé.

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.

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

Les accès sont contrôlés dans le respect de la réglementation relative à la protection des données à caractère personnel. La définition des mots de passe de l'Utilisateur obéit à un certain nombre de règles de Sécurité définies par l'Établissement.

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'Établissement. Cet usage est présumé être professionnel.

L'Utilisateur doit en particulier :

- assurer la protection de ces Ressources en respectant les règles de sécurité applicables à celles-ci ;
- s'assurer de ne pas les mettre à disposition de personnes non autorisées, que ce soit des personnes internes ou externes à l'Établissement ;
- protéger la confidentialité des informations en utilisant des outils adaptés aux exigences de sécurité, cf. plateforme collaborative NEXT (intranet de l'Etablissement) article « Echanger des documents sensibles »[1];
- être vigilant et signaler, dans les meilleurs délais et par écrit, toute anomalie ou tout constat, tentative ou soupçon de violation d'une Ressource de l'Établissement, ou toute situation dont il a un motif raisonnable de penser qu'elle présente un danger grave et immédiat pour la Sécurité 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 Équipement Individuel en cas d'absence même temporaire ;
- restituer son Equipement Individuel en cas de départ.

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 Équipement Individuel au réseau de l'Établissement et à des réseaux et systèmes externes ;
- lire, modifier, copier ou détruire des informations autres que ceux qui lui appartiennent en propre ou pour lesquels il dispose des droits correspondants (lecture, modification ou suppression) ;
- 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 ;

[1] https://next.caissedesdepots.fr/jplatform/jcms/pr1_20880/echanger-des-documents-sensibles

- contourner ou désactiver les dispositifs de sécurité de ses Équipements individuels, notamment les antivirus ;
- exploiter une 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'Établissement ;
- 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/ou par le Service Informatique ;
- déplacer, dupliquer, téléverser ou détruire des informations sur lesquelles sa fonction et ses missions le conduisent à intervenir avant de s'être assuré que cela ne porte aucun préjudice à l'Établissement. 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'Établissement, 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 Équipements 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 Équipements 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 la configuration et les paramètres de ces Ressources, y compris par l'installation de logiciels ;
- désactiver les mécanismes de sécurité mis en œuvre (logiciel antivirus, écran de veille automatique, outils d'authentification, outils de chiffrement de données ou de messages…), ou en changer les paramètres ;
- utiliser des outils de sécurité non-fournis par l'Établissement, notamment en termes de sécurité réseau ou de chiffrement de données ;
- connecter aux Systèmes d'Information de l'Établissement des Ressources non fournies par l'Établissement, notamment : modem, périphérique, disques durs externes, graveurs, carte réseau Wifi / Bluetooth, carte ou puce réseaux mobiles (3G, 4G, 5G, …), logiciel, sauf accord exprès préalable de la Fonction Sécurité des Systèmes d'Information.

6.3. Usage privé des Ressources

Les Ressources ont une finalité professionnelle. L'utilisation résiduelle de certaines Ressources à titre non professionnel est tolérée de manière exceptionnelle, dans les conditions décrites dans la présente Charte.

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 Charte.

Cet usage privé résiduel ne doit notamment pas porter préjudice à l'activité professionnelle et ne doit pas être susceptible d'affecter 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 ou la réputation de l'Établissement.

Seront considérés comme 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 :

- pour les messages émis, soit ils doivent être marqués comme « PRIVÉ » à l'aide de l'outil de classification mis à disposition par l'Établissement, soit l'objet du message doit mentionner l'indication « PRIVÉ » ;
- pour les messages reçus, soit ils doivent être envoyés en réponse à un message marqué comme « PRIVÉ » à l'aide de l'outil de marquage mis à disposition par l'Établissement, soit l'objet du message doit mentionner l'indication « PRIVÉ » ;
- pour les fichiers, soit ils doivent être marqués comme « PRIVÉ » à l'aide de l'outil de classification mis à disposition par l'Établissement, soit les noms des fichiers doivent mentionner l'indication « PRIVÉ », soit ils doivent être conservés dans des répertoires spécifiques dont les noms mentionnent l'indication « PRIVÉ ».

Les différentes graphies du terme « PRIVÉ » sont valables : en majuscules, minuscules, accentuées ou non. La mention « PERSONNEL » est à exclure car pouvant faire référence au personnel de l'Etablissement.

Tout courriel, répertoire, ou fichier ne correspondant pas à ces règles est présumé professionnel.

L'Utilisateur est informé que les dispositifs et procédures de contrôle automatiques mis en place par l'Établissement (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 d'atteinte manifeste à la confidentialité d'une information ou à la sécurité du Système d'Information, l'Utilisateur est également informé que l'Établissement se

réserve le droit d'effacer les données correspondantes sans avoir 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.

L'Établissement ne pourra être tenu responsable de toute perte ou altération de quelques données que ce soit relevant de l'usage privé des Ressources.

En cas de départ définitif de l'Utilisateur, ce dernier prend toutes les dispositions nécessaires pour récupérer et supprimer ses fichiers *privés*. 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'Établissement.

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

6.4. Comportements abusifs

Seront notamment considérés comme abusifs au sens de la Charte les comportements visant à recevoir, consulter, télécharger, conserver, publier, diffuser ou distribuer, en toute connaissance de cause et au moyen des Systèmes d'Information de l'Établissement, tous programmes, logiciels, documents électroniques, messages, informations, données :

- à caractère violent, pédopornographique, pornographique, xénophobe, antisémite, révisionniste, négationniste, raciste, sectaire ou faisant l'apologie du terrorisme 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 ;
- contenant des codes malveillants tels que des virus ;
- manifestement attentatoires à l'image de marque interne ou externe de l'Établissement 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. Gestion des absences et des départs

Chaque Utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation définies par l'Établissement.

En cas d'absence de l'Utilisateur, pour quelque raison et durée que ce soit, l'Établissement se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement à toute Ressource et à tout document à caractère professionnel de l'Utilisateur, ayant recours en tant que de besoin aux codes administrateurs systèmes.

A l'annonce du départ définitif de l'Établissement de l'Utilisateur, et pour des raisons légitimes de protection de ses intérêts, les droits d'accès et les conditions d'utilisation du Système d'Information et des Equipements individuels pourront être modifiés. De même, des règles particulières de Traçabilité pourront être mises en œuvre.

Dans l'hypothèse où l'Utilisateur change de service ou quitte l'Établissement, l'Utilisateur doit :

- ~~remettre en bon état général de fonctionnement, l'ensemble du Système d'Information et des Equipements Individuels qui lui ont été fournis ;~~
- remettre aux services informatiques l'ensemble des Equipements Individuels qui lui ont été fournis ;
- transmettre à son supérieur hiérarchique toute Ressource nécessaire à la continuité du service qu'il détient, par exemple sur ses espaces partagés, sa messagerie ou ses Equipements individuels ;
- restituer tous les Moyens d'authentification qui lui ont été fournis ;
- la veille de son départ, récupérer puis supprimer les fichiers, les répertoires et les messages électroniques nommés « PRIVÉ », ainsi que tous les documents non professionnels.

L'Utilisateur est informé que l'accès à son compte, à ses documents et fichiers, y compris privés, seront gelés pendant un (1) mois à compter de son départ de l'Etablissement ou de son changement de service.

A défaut de destruction de ses fichiers, messages et répertoires privés par l'Utilisateur lors de son départ, ce dernier est informé que ces éléments pourront être détruits, et ce, sans être consulté et sans qu'aucune copie ne soit réalisée. La responsabilité de l'Établissement ne pourra pas être engagée pour ces destructions, pertes ou altérations.

Sauf nécessité liée à la continuité du service, le compte messagerie individuel de l'Utilisateur, ainsi que ses Moyens d'authentification, sont désactivés dès le lendemain de son départ ou de son décès.

Les départs temporaires sont encadrés par une procédure dédiée.

8. Usage de l'Informatique mobile

Les Equipements mobiles mis à la disposition de l'Utilisateur par l'Établissement, le sont à des fins professionnelles. L'Utilisateur n'est autorisé à les utiliser à des fins personnelles qu'à titre résiduel et dans le respect des règles édictées par la présente Charte.

Ces équipements comprennent l'ensemble des matériels et dispositifs informatiques mis à disposition de l'Utilisateur en situation de mobilité : PC portable, téléphone portable, etc.

Outre le respect des règles définies au chapitre 6 « Bon usage général des Ressources », les Équipements Individuels mobiles sont soumis aux procédures de sécurité et de contrôle mises en œuvre au sein de l'Établissement.

Seuls les Équipements individuels fournis par l'Établissement sont autorisés à accéder aux Ressources. L'utilisation d'Équipements mobiles personnels, c'est-à-dire non fournis par l'Établissement, est prohibée pour accéder au Système d'information.

L'Utilisateur d'un Équipement Individuel mobile doit prendre des précautions supplémentaires par rapport à un Équipement 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 Équipement Individuel mobile sont régulièrement sauvegardées, via un mécanisme automatique que l'Utilisateur ne doit en aucune manière chercher à bloquer ou désactiver ;
- lorsque l'Utilisateur laisse son Équipement Individuel mobile dans des locaux sous le contrôle de l'Établissement ou sous son propre contrôle (domicile), il doit assurer la protection de cet équipement, notamment à l'aide des moyens mis à disposition par l'Établissement (par exemple, attaché à un bureau avec un câble de sécurité, conservé dans une armoire ou un tiroir fermé à clé) ;
- en dehors des locaux mentionnés au point précédent, l'Utilisateur doit veiller à ne pas laisser son Équipement Individuel mobile sans surveillance (chambres d'hôtel, voitures, lieux publics, etc.) ;
- lorsque l'Utilisateur ne se sert pas de son Équipement Individuel mobile, même pour une courte durée, il doit en verrouiller l'accès logique.

9. Usage de la messagerie électronique

9.1. Principes généraux

L'usage de la messagerie électronique est par principe professionnel.

La messagerie électronique est un outil d'échange d'informations, mais peut également être le vecteur de propagation de codes malveillants, ce qui peut notamment constituer un vecteur d'infection susceptible d'impacter le Système d'Information de l'Établissement.

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

- Les seuls outils de messagerie électronique autorisés à des fins professionnelles au sein de l'Établissement sont les outils de messagerie gérés et exploités par le Service Informatique (interdiction d'utiliser de messageries privées à des fins professionnelles).
- Sauf communication institutionnelle, la messagerie électronique ne doit pas être utilisée pour des envois en nombre pouvant encombrer le réseau (notamment lors de l'utilisation inappropriée de grandes listes de diffusion).
- L'Utilisateur doit s'assurer du bien-fondé des messages qu'il émet vers ses correspondants et rester vigilant. Il ne doit, par exemple, pas transmettre en connaissance de cause de fausses alertes ou canulars circulant par messagerie.
- En cas de réception à tort d'un message électronique interne destiné à une autre personne, l'Utilisateur doit le renvoyer à son expéditeur en indiquant l'erreur d'adresse et doit le supprimer de sa boîte de réception, de ses éléments envoyés et de sa corbeille. Si le contenu de ce message était confidentiel, l'Utilisateur s'interdit d'en faire état à quiconque, en interne comme en externe.
- 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 Données Sensibles, même à titre de projets. Par sécurisation, on entend des outils supplémentaires, fournis et maîtrisés par l'Établissement. 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 la redirection automatique de ses messages vers une adresse de messagerie externe à l'Établissement, afin d'éviter que des Données Sensibles ne se trouvent envoyés sur Internet à l'insu de l'émetteur. Il est donc interdit de rediriger sa messagerie professionnelle en direction d'une messagerie privée, de même qu'il est interdit de rediriger sa messagerie privée en direction de sa messagerie professionnelle.

- 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 du supérieur hiérarchique et de la Fonction Sécurité des Systèmes d'Information. La mise en œuvre de cette disposition 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 électroniques reçus, notamment de correspondants extérieurs. En effet, l'usurpation de l'identité de l'auteur d'un courriel est facilement réalisable.
- Les boîtes aux lettres font l'objet de sauvegardes centralisées, conservées sur une période maximale de six mois.

De plus, l'Utilisateur sera particulièrement vigilant quant à la stricte nécessité d'envoyer des messages en « masse » (« spamming »), notamment par l'utilisation de la fonction « répondre à tous ». 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, afin notamment de préserver la messagerie de l'Établissement d'attaques pouvant viser les organismes teneurs de ces listes de diffusion.

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, la réputation, la sécurité, d'autrui ou de l'Établissement, ni au bon fonctionnement des Ressources.

L'Utilisateur ne doit jamais écrire dans un courriel ce qu'il s'interdirait d'exprimer par tout autre moyen, à l'oral ou par écrit (propos discriminatoires, racistes, injurieux ou malveillants, etc.). Par ailleurs, il s'engage à ne pas ouvrir les courriels ainsi que les fichiers attachés aux courriels qu'il reçoit et pour lesquels il a des doutes concernant l'émetteur 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 ».

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'Établissement, dans les conditions fixées au chapitre 6.3 « Usage privé des Ressources » (utilisation limitée et raisonnable, Marquage des courriels à caractère privé, etc.).

Cette exception s'applique exclusivement aux échanges entre personnes physiques, l'utilisation de l'adresse professionnelle comme support d'échanges privés avec des entités dotées de la personnalité morale, commerciales ou associatives, est prohibée, afin notamment de préserver la messagerie de l'Établissement d'attaques pouvant viser ces personnes morales.

9.2. Comportements abusifs

Outre les différents points explicités au chapitre 6.4 « Comportements abusifs », seront notamment considérés comme abusifs l'usage privé inapproprié de la messagerie, du fait notamment de la fréquence trop importante des messages reçus ou envoyés, de l'utilisation d'une liste de diffusion interne ou externe, du volume de données échangées (messages et pièces jointes), du transfert de Données Sensibles, ainsi qu'en cas d'utilisation abusive ou malveillante de la mention « PRIVÉ ».

10. Usage des services Internet

10.1. 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.) met en évidence de nouveaux risques auxquels il faut être particulièrement attentif.

Par principe, l'accès Internet est mis à la disposition des Utilisateurs à des fins professionnelles.

L'accès aux services Internet doit se faire dans le respect des règles d'accès et d'usage des Ressources définies aux chapitres 5 « Accès aux Ressources » et 6 « Bon usage général des Ressources » (autorisations d'accès, non-contournement des dispositifs de protection, non-atteinte à la confidentialité des informations, usage limité à titre privé, etc.). 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 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'Établissement 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 NEXT (communauté « Département Cyber Sécurité Groupe (DCSG) » de l'espace collaboratif « Next »).

En outre, la loi et les règlements varient en fonction des États ; 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.

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 dans la mesure où 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 non validés par l'Etablissement sans autorisation explicite préalable de l'Établissement et la mise en œuvre si nécessaire, par le Service Informatique, de mesures de protection adéquates.

L'Utilisateur n'est pas autorisé à utiliser des services d'échanges et de communications d'informations (forums, réseaux sociaux et autres services collaboratifs) à titre professionnel en dehors de la stricte nécessité de ses fonctions au sein de l'Établissement et explicitement autorisés par l'Établissement (par exemple, espace collaboratif interne à l'Établissement). 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 (courriels, forums de discussion, messages déposés sur des réseaux sociaux ou des espaces collaboratifs…).

10.2. Dispositions spécifiques sur l'usage privé des services internet

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, n'affecte pas l'exercice de ses fonctions par l'Utilisateur, n'entrave pas la sécurité ou les performances des réseaux, ne gêne pas la bonne marche de l'Établissement ni ne porte atteinte à son image ou ses intérêts et ce, pendant ou en dehors des heures de travail.

11. Usage des services de téléphonie

Les postes téléphoniques fixes, mobiles ou logiciels (« softphonie ») mis à la disposition des Utilisateurs le sont à des fins professionnelles.

Les Utilisateurs sont informés que les systèmes de téléphonie enregistrent les numéros de téléphones sortants.

En outre, des relevés individuels téléphoniques sont établis tous les mois.

Les téléphones mobiles mis à disposition comportent deux zones étanches : une dite « professionnelle » hébergeant des applications sous le contrôle du Service Informatique et une dite « personnelle » pour laquelle l'Utilisateur bénéficie d'une

tolérance afin d'y installer des applications tierces disponibles dans le magasin d'application de son téléphone.

Dans le cadre de la tolérance mentionnée ci-avant, l'Utilisateur veille à n'installer que les applications tierces nécessaires à son usage quotidien du téléphone pour minimiser le risque d'installation d'une application malveillante.

12. Usage de la plateforme collaborative "NEXT"

Ce service est mis à la disposition des Utilisateurs par l'Etablissement à des fins exclusivement professionnelles. La plateforme collaborative "NEXT" (référencée ci-après simplement NEXT) doit être utilisé de manière responsable.

La plateforme est accessible via l'adresse https://next.caissedesdepots.fr/

NEXT est destiné à promouvoir la communication, à faciliter l'échange d'informations et l'interaction sociale entre les Utilisateurs et à améliorer l'efficacité et la qualité du travail de chacun.

En fonction du poste occupé, de la fonction, du statut, ou encore du rang hiérarchique, un Utilisateur peut être habilité à accéder à certaines informations, applications, fonctionnalités ou contenus spécifiques.

NEXT comprend également un espace collaboratif permettant l'échange et le partage d'informations entre les Utilisateurs.

Afin de préserver la sécurité de l'Établissement et les libertés individuelles de chacun, l'Utilisateur doit respecter, lorsqu'il échange, publie, partage ou consulte des informations ou des documents sur l'Intranet, les règles décrites dans la présente Charte, et notamment celles liées à la propriété intellectuelle, à la confidentialité des informations, à la sécurité du Système d'Information de l'Établissement, au respect de la vie privé des tiers, ou encore celles sur le bon usage général des Ressources.

Tout Utilisateur est responsable de l'usage des services auquel il a accès et reste seul responsable des informations qu'il publie ou échange sur NEXT.

13. Usage des Moyens Personnels de l'utilisateur

L'Utilisateur *ne* peut *pas* utiliser à des fins professionnelles des équipements individuels et systèmes d'information et de communication qui sont sa propriété personnelle ou qu'il détient à titre personnel.

Seuls les Equipements Individuels mis à disposition par l'Etablissement (dont PC et téléphone portable) doivent être utilisés à des fins professionnelles.

14. Télétravail

Les dispositions de la présente Charte et instructions données par l'Établissement pour l'utilisation de Système d'Information et des Equipements Individuels s'appliquent également dans le cadre des différentes modalités de télétravail (régulier, ponctuel, TOD…) pour tout Utilisateur.

Une vigilance particulière doit être effectuée par l'Utilisateur dans ce contexte en veillant à protéger en toute circonstance l'accès au Système d'Information et aux informations. A cette fin, l'Utilisateur veillera à prendre toute disposition utile telle que l'activation de l'écran de verrouillage de son poste.

Les postes de travail sont fournis pour un usage professionnel et ne doivent pas être prêtés à un tiers.

15. Protection de l'Information

La protection de l'Information vise avant tout à assurer sa disponibilité, son Intégrité et sa Confidentialité. En la matière, **la vigilance de chaque Utilisateur est fondamentale, dans la mesure où les seules dispositions organisationnelles et techniques ne sont pas suffisantes.**

L'Établissement met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité du Système d'Information et des informations y étant stockées ou échangées.

15.1. Confidentialité

Les moyens de protection des informations (restrictions des accès, chiffrement, possibilité de blocage, journalisation des actions, etc.) 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'Établissement.

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 moyen 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'Établissement, ses partenaires, ses clients, ses fournisseurs et ses personnels, que ce soit sous forme orale ou écrite (articles de presse, publication sur Internet, forum ou réseaux sociaux, etc.).

Notamment, l'Utilisateur ne doit pas :

- détourner ou utiliser des informations propres à l'Établissement à des fins étrangères à l'activité du service ;
- mettre à disposition d'autrui des Données Sensibles sans y être préalablement autorisé ;
- répondre aux sollicitations externes visant à l'obtention de renseignements liés à l'Établissement et son activité (démarchage téléphonique, courrier électronique, enquêtes, etc.).

L'Utilisateur veille tout particulièrement à préserver la sécurité (Intégrité et Confidentialité notamment) des Données à caractère personnel ainsi que leurs traitements. Il est rappelé que l'Etablissement, en tant que responsable de traitement ou sous-traitant, à l'obligation de prendre toutes précautions utiles afin de préserver la sécurité des Données à caractère personnel qu'il traite et d'empêcher en particulier que ces données ne soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

Chaque Utilisateur doit être vigilant sur le risque de divulgation dans le cadre d'utilisation d'Équipements Individuels mobiles en dehors des locaux de l'Établissement (hôtels, lieux publics, transports, etc.).

15.2. 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, 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 (« C1 - Public », « C2 - Interne », « C3 - Confidentiel », « C4 - Secret », Privé).
- *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'Établissement selon la Confidentialité des informations. L'Utilisateur devra uniquement utiliser les logiciels et outils de chiffrement et d'échange de documents mis à sa disposition par l'Établissement, 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 Leak 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'Établissement.

16. 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 à la règlementation relative à la protection des données à caractère personnel.

L'ensemble des outils de sécurité déployés dans les Systèmes d'Information de l'Établissement (antivirus, 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 susceptibles d'être analysés par les équipes de sécurité du Service Informatique. En cas de nécessité de preuves et de traces numériques plus complètes, l'Établissement peut également mettre en œuvre des outils d'investigations avancées (dits « d'analyse forensique »).

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 dix-huit mois (sauf obligations légales ou règlementaires particulières de conserver ces données sur une durée plus longue) et font l'objet de mesures de protection adaptées contre tout risque de divulgation et d'utilisation abusive. En cas de risque pour le Système d'Information ou d'usage inapproprié des Ressources, des poursuites, notamment disciplinaires, pourront être engagées contre l'Utilisateur concerné, en particulier sur la base de ces données de connexion.

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, etc.).

16.1. Contrôles automatisés

Journaux d'exploitation

Le Système d'Information génère des journaux d'exploitation (dits « logs » ou journaux d'événements) créés automatiquement par les équipements informatiques et de communication électronique. Ils permettent de retracer la vie du Système d'Information de l'Établissement et les actions qui y sont menées. Ils sont stockés sur les postes informatiques et sur le réseau. Ils contribuent à assurer le bon fonctionnement du Système d'Information et la sécurité des informations de l'Établissement, 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 « http**s**://... ») sont systématiquement interrompus par l'Établissement le temps d'opérer ces contrôles de sécurité, puis sont à nouveau chiffrés pour en assurer la protection sur le reste de leur parcours.

Filtrage

Des systèmes de filtrage peuvent être mis en œuvre pour analyser les messages entrants et sortants (contrôle antiviral, 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, accès aux messageries en ligne pour lutter contre la propagation de codes malveillants et la fuite d'information, etc.).

Détection de la fuite d'information

Afin de s'assurer de la mise en œuvre de manière efficace de l'ensemble du processus décrit précédemment, des contrôles systématiques et automatiques sont définis. Ces contrôles s'appuient sur l'évaluation du niveau de sensibilité de l'information, le Marquage des Documents et sur la protection qui en est faite afin de détecter tout échange d'information qui ne serait pas conforme aux dispositions de la Charte.

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.).

16.2. Investigations

L'Utilisateur est informé que des contrôles individualisés pourront être diligentés, suite à un dysfonctionnement des Systèmes d'Information de l'Établissement, à une alerte de sécurité mais également en cas de suspicion d'un usage non conforme des 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 sur la réalisation éventuelle 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'Établissement, le concours de l'Utilisateur pourra être sollicité pour 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 (accès internet depuis le réseau de l'Établissement, partages de fichiers, etc.) pourra être interdit sans préavis ni information.

16.3. Spécificité des Documents privés

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.

Sauf risque ou évènement particulier, conformément à la jurisprudence en vigueur, le contenu des messages et des fichiers portant explicitement la mention « PRIVÉ » ne pourra être consulté qu'en présence de l'Utilisateur ou celui-ci dument appelé.

Enfin, les communications émises ou reçues par la médecine du travail sont également considérées « PRIVÉ » au sens de la présente Charte, même si elles ne sont pas explicitement identifiées comme telles.

16.4. Droit syndical et instances représentatives du personnel

Par ailleurs, les Ressources mises à disposition des représentants du personnel de l'Établissement, quel que soit le statut public ou privé dont ils relèvent, font l'objet de dispositions particulières détaillées dans l'accord relatif au droit syndical et aux moyens syndicaux au sein de l'établissement public CDC en vigueur.

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 « PRIVÉ » 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 16.2 « Investigations »), qu'après accord du dirigeant (ou de l'un des dirigeants) de l'organisation syndicale au sein de l'établissement auquel il appartient. Il s'agit de s'assurer que ces messages 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.

17. 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, 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 ou pour des raisons techniques, les Administrateurs peuvent être amenés à invalider le ou les codes d'accès de l'Utilisateur concerné.

À titre d'exemple, ce type d'intervention 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.

18. Rôle des Administrateurs

18.1. Missions et rôle des Administrateurs

Les missions des Administrateurs portent essentiellement sur la qualité et la sécurité des Systèmes d'Information de l'Établissement. 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'Établissement.

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

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.

18.2. Droits des Administrateurs

Les Utilisateurs sont informés que les Administrateurs peuvent avoir accès à l'ensemble des Systèmes d'Information de l'Établissement, 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'Établissement ;

- la preuve de la date de création ou de la diffusion desdites informations ;
- la protection de l'Intégrité et de la Confidentialité des données ;
- la suspension ou la suppression des Habilitations ;
- la vérification de l'absence d'intrusion dans les Systèmes d'Information ;
- 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 le Service Informatique est autorisé à prendre la main à distance sur les Équipements 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 Équipements individuels jugés suspects. Toutefois, cette prise de main sans autorisation ne sera légitime que dans les cas où ces Équipements individuels présentent un danger pour les Systèmes d'Information de l'Établissement.

En tout état de cause, les Administrateurs sont tenus d'en informer préalablement la Fonction Sécurité des Systèmes d'Information de l'Établissement, puis les Utilisateurs concernés dès lors que le Système d'Information sera à nouveau sécurisé.

18.3. Devoirs des Administrateurs

Les Administrateurs sont tenus à une obligation de confidentialité stricte. 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.

Un Administrateur doit en particulier :

- s'assurer de la protection des accès privilégiés qui lui sont fournis dans le cadre de sa mission et respecter en particulier les règles de gestion des Moyens d'authentification, consultables sur NEXT ;
- limiter strictement l'usage des accès privilégiés dont il bénéficie exclusivement aux tâches qui lui sont confiées et qui en nécessitent strictement l'utilisation ; les activités courantes étant réalisées au moyen d'un profil d'accès à moindre privilège ;
- restreindre les accès aux informations et messages professionnels des Utilisateurs dans la stricte limite des conditions mentionnées de la présente Charte et des instructions de sécurité de l'Établissement ;
- observer le respect strict de la confidentialité des informations afférentes aux Ressources dont il a connaissance et en limiter la communication aux seules

personnes ayant besoin d'en connaître pour assurer leurs activités professionnelles (la diffusion en étant interdite sur les forums Internet, blogs, réseaux sociaux, etc.).

- documenter toute action et intervention en écart avec les procédures internes de l'Établissement, toute action ou trace de suppression de données, et tout évènement impactant le niveau de sécurité du Système d'Information de l'Établissement ;
- informer la Fonction Sécurité des Systèmes d'Information de toute faille ou incident de sécurité qu'il pourrait découvrir ou dont il pourrait avoir connaissance.

L'Administrateur ne doit pas :

- utiliser ses droits d'accès privilégiés pour accéder à des informations non nécessaires à l'exécution de sa mission ;
- prendre connaissance des mots de passe des Utilisateurs, ni donner suite à aucune demande en la matière, quelle qu'en soit l'origine, en dehors de certaines exceptions recensées par le Service Informatique et validées par la Fonction Sécurité des Systèmes d'information ;
- consulter les messages privés des Utilisateurs du SI au mépris de la Charte ;
- porter atteinte à l'Intégrité des fichiers de journalisation ;
- procéder, ou faire procéder par l'intermédiaire d'un prestataire, à des changements de configuration permettant de supprimer les traces informatiques ;
- En cas d'incident de sécurité avéré, tel que tentative d'intrusion, attaque virale, usurpation d'identité, vol de matériel ou d'information, les actions de correction sont pilotées par la Fonction Sécurité des Systèmes d'Information en concertation avec l'Administrateur concerné. Par conséquent, l'Administrateur ne doit engager aucune action qui pourrait avoir pour conséquence de détruire ou corrompre des éléments de preuve sans validation de la Fonction Sécurité des Systèmes d'Information ;
- utiliser les comptes privilégiés pour des activités et besoins autres que ceux directement liés aux tâches d'administration ou d'exploitation dont il a la charge ;
- recevoir et prendre consigne d'une personne non identifiée et, le cas échéant, à transmettre au Service Informatique toute requête lui paraissant inappropriée.

19. Stockage des informations

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

Les serveurs de fichiers (U:) sont les espaces de stockage de référence pour les informations internes. D'autres espaces internes ou externes (« cloud ») sont susceptibles d'être utilisés conformément aux dispositions présentées sur NEXT qui s'appuient notamment sur la sensibilité des informations échangées.

La messagerie professionnelle utilise un service de cloud et l'envoi de courriels sensibles (contenu du message ou pièces-jointes) est encadré par les exigences précitées.

Les espaces de stockage interne 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'Établissement (stockage dans des répertoires dit « PR_ »). 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 en s'assurant au préalable que leur usage est compatible avec la sensibilité des données et Documents susceptibles d'être enregistrés (cf. lien ci-avant concernant l'échange de Données Sensibles).

Chaque Utilisateur doit 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 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 privé ne pourra s'opérer que sur les Équipements individuels de l'Utilisateur à l'exclusion de tout espace partagé. L'Établissement se réserve la possibilité de déplacer ou d'effacer les contenus stockés sur tout espace partagé sans avoir à en avertir préalablement l'Utilisateur. L'Utilisateur devra s'assurer de la parfaite innocuité de ces fichiers pour les Ressources de l'Établissement

L'Utilisateur 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'Établissement.

L'Utilisateur ne devra conserver des Données Sensibles sur un Équipement mobile que si les mesures de protection appropriées et prévues par l'Établissement pour préserver la Confidentialité des informations 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'Établissement 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, etc.).

L'usage de dispositifs de stockage externes fournis par le Service Informatique (graveurs de support magnétique ou optiques, clés USB, disques durs externes…) est

soumis à une demande de dérogation et exclusivement dédié à un usage professionnel. Les autres moyens d'échange mis à disposition de l'Etablissement doivent être privilégiés pour échanger des données compte tenu des risques d'introduction de code malveillant et de fuite d'information.

Tout usage non conforme à la Charte d'un dispositif de stockage externe entrainera la révocation immédiate de la dérogation.

20. Protection des Données à caractère personnel des Utilisateurs

Le Règlement européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que la loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

La réglementation relative à la protection des données à caractère personnel impose notamment aux responsables de traitement une information auprès des personnes concernées sur les traitements qu'ils opèrent, et vise également à préserver la sécurité (Confidentialité et Intégrité) des Données à caractère personnel contenues dans les traitements opérés, lesquels doivent respecter une finalité déterminée, et légitime.

L'Établissement poursuit son intérêt légitime lorsqu'il met en œuvre des traitements de données à caractère personnel en relation avec l'usage des Systèmes d'Information et des Ressources couverts par la présente Charte et pour assurer leur sécurité. L'Établissement s'engage à ce que les données concernant les Utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

Les données collectées sont destinées aux services concernés de la CDC en charge de la sécurisation des systèmes d'information de la CDC ou qui seraient légitimes à recevoir ces données, sur la base d'habilitations strictes et d'un accès restreint, ainsi que, le cas échéant, à ses sous-traitants ou prestataires mandatés aux mêmes fins.

Les données et traces informatiques relatives aux contrôles de l'usage des ressources sont conservées pendant une période maximale de 18 mois à compter de leur enregistrement (sauf obligations légales ou règlementaires particulières de conserver ces données sur une durée plus longue).

A toutes fins utiles, il est rappelé que les données collectées auprès des Utilisateurs sont obligatoires aux fins de bonne gestion, de maintenance, d'organisation et de sécurité des Systèmes d'Information et des Ressources.

Conformément à la règlementation précitée, les Utilisateurs disposent d'un droit d'accès, de rectification ou d'effacement, de limitation du traitement de ses données,

d’un droit d’opposition, ainsi que du droit de définir des directives relatives au sort de ses données après son décès, qui s’exercent par courrier électronique à mesdonneespersonnelles@caissedesdepots.fr ou par courrier postal à l’adresse suivante :

Caisse des Dépôts et consignations – Données Personnelles - Établissement de Bordeaux – 5 rue du Vergne – 33059 BORDEAUX CEDEX

Pour toute information complémentaire ou difficulté relative à l’utilisation de vos données, vous pouvez contacter notre Déléguée à la protection des données (DPO) à l’adresse : dpo@caissedesdepots.fr

En cas de difficulté non résolue, vous pouvez saisir la Commission Nationale de l’Informatique et des Libertés (CNIL), autorité de contrôle en charge du respect des obligations en matière de données à caractère personnel.

Vous pouvez nous contacter aux adresses génériques suivantes :

POURRIEL@caissedesdepots.fr

pour l'envoi des courriels suspects que vous recevez (service également disponible depuis votre logiciel de messagerie via l'icône « Signaler un courriel suspect »)

SECURITE-SI@caissedesdepots.fr

pour tout autre sujet lié à la sécurité des systèmes d'information