

Charte nationale des utilisateurs des systèmes d'information de l'EFS

Date de création : 18/03/2022
Date de mise à jour : 06/01/2025

SOMMAIRE

1. Application de la charte nationale	3
1.1. Préambule	3
1.2. Objet	3
1.3. Définitions	3
2. Principes d'utilisation du système d'information	5
2.1. Loyauté	5
2.2. Utilisation professionnelle des systèmes d'information	5
3. Respect des règles d'utilisation, de sécurité et de bon usage	5
4. Protection des données	7
4.1. Protection des données à caractère personnel et des données professionnelles	7
4.2. Les obligations des utilisateurs et la protection des données à caractère personnel	7
4.2.1. Les obligations des utilisateurs et la protection des données professionnelles	7

4.2.2. Protection des données à caractère confidentiel ou des données à caractère sensible	8
4.3. Préserver l'intégrité des systèmes informatiques et de télécommunications	8
5. Usage des services internet (web, réseaux sociaux, forum...)	8
6. Analyse et contrôle de l'utilisation des ressources	9
7. Modalités d'accès et de conservation	10
7.1. Modalités d'accès	10
7.1.1. Accès aux systèmes d'information tout au long de l'exercice professionnel au sein de l'établissement	10
7.1.2. Accès aux systèmes d'information en cas de suspension ou de cessation d'activité au sein de l'établissement	10
7.2. Archivage des messages professionnels	11
7.3. Archivage des informations dématérialisées	11
8. Respect du droit de la propriété intellectuelle	11
9. Sanctions	11
9.1. Dispositions propres aux utilisateurs membres des personnels de l'établissement	11
9.2. Dispositions propres aux utilisateurs membres d'une entreprise extérieure	12
10. Publicité	12
11. Entrée en vigueur	12

1. Application de la charte nationale

1.1. Préambule

Parce que la préservation du patrimoine (matériel et immatériel) et la réputation de l'Établissement français du sang (EFS) sont essentielles, l'utilisateur s'engage à ce qu'au quotidien, la protection et le respect de la confidentialité, la disponibilité et l'intégrité des données de l'établissement soient toujours conformes aux règles imposées par l'EFS.

La présente Charte nationale d'utilisation des systèmes d'information tient lieu de principe et de règles pour les utilisateurs qui devront en prendre obligatoirement connaissance.

1.2. Objet

L'Établissement français du sang dispose d'un système d'information nécessaire à son activité et auquel les utilisateurs accèdent pour l'exercice de leur mission.

La présente Charte nationale détermine les règles de sécurité et d'usage des systèmes d'information que l'utilisateur s'engage à respecter lorsqu'il les utilise, y a accès ou accède à des données qui y sont stockées. Elle définit les droits et obligations que l'établissement s'engage à respecter vis-à-vis des utilisateurs, notamment les conditions et les limites des éventuels contrôles portant sur l'utilisation du SI.

Elle constitue un des moyens mis en œuvre pour préserver la sécurité des systèmes d'information en application de la Politique Nationale de Sécurité des systèmes d'information (PNSSI) disponible sur l'espace de gestion documentaire de l'EFS, GEDEON :

PNSSI 1 / Enjeux et organisation SSI

PNSSI 2 / Objectifs et règles de sécurité

Elle a pour vocation de concilier la sécurité informatique de l'établissement avec les libertés individuelles et la vie privée des utilisateurs auxquels elle s'adresse.

Elle rappelle l'existence de sanctions professionnelles ou personnelles applicables en cas de non-respect des règles et principes qu'elle établit ou rappelle (cf. [le Chapitre 9 « Sanctions »](#)).

La Charte nationale s'impose aux utilisateurs des systèmes d'information de l'établissement quel que soit leur statut (cf. définition ci-dessous). Les administrateurs du système d'Information sont soumis à la Charte nationale au même titre que les utilisateurs. Une charte spécifique leur est également applicable.

1.3. Définitions

Les termes ci-après mentionnés devront être entendus dans le cadre de la présente Charte nationale, selon les définitions suivantes :

- **Administrateur** : tout individu devient administrateur d'un système d'information dès qu'il reçoit de manière individuelle et formelle des privilèges d'administration sur les systèmes d'information de l'EFS, en particulier sur les services réseaux, les applications, les serveurs, et les équipements. Il dispose de droits d'administration nécessaires à la bonne réalisation d'actions d'administration. Il se distingue ainsi de l'utilisateur standard du SI par les privilèges qui lui sont accordés sur le système d'information.
- **Charte nationale** : désigne le présent document. La Charte nationale s'impose aux utilisateurs au même titre que le règlement intérieur des Établissements de Transfusion Sanguine ainsi que du règlement intérieur des Services Centraux dont la Charte nationale constitue une annexe.

- Chiffrement : le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.
- Délégué à la protection des données ou Data Protection Office ou DPO : désigne la personne chargée de conseiller et accompagner la conformité au Règlement européen sur la protection des données (RGPD) de l'ensemble des traitements mis en œuvre par un organisme.
- Direction des Systèmes d'Information (DSI) : la DSI nationale est la direction responsable du SI de l'EFS. Elle est en charge de définir l'architecture des systèmes d'information ainsi que de concevoir, installer, déployer et exploiter les systèmes d'information nationaux.
- Donnée à caractère personnel : désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.
- Donnée à caractère sensible : les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
- Données classifiées secret : elles répondent aux exigences de l'IGI 1300 du 11 sept 2021. (Anciennement de niveau CONFIDENTIEL DEFENSE). Les données au niveau secret peuvent être uniquement communiquées aux personnes habilitées au SECRET et ayant besoin d'en connaître à l'aide d'outils prévus à cet effet.
- Données couvertes par le secret professionnel : désignent les informations confidentielles en raison de leur nature (couverte par une obligation de discrétion, de confidentialité ou dont le caractère secret protège les intérêts matériels ou moraux des personnes qu'elle concerne).
- Données ou informations à caractère confidentiel : données ou informations dont le caractère sensible est tel que leur divulgation, leur perte ou leur modification peut porter une atteinte grave aux intérêts essentiels de l'EFS : perte de confiance, perte de revenu, perte d'image de marque. Ces données ou informations à caractère confidentiel ne sont communicables qu'aux personnes formellement autorisées.
- Établissement : désigne l'Établissement français du sang (EFS) et ses Établissements de Transfusion Sanguine (ETS) ainsi que le Siège Social.
- Responsable National de la Sécurité des Systèmes d'Information (RNSSI) : il assure le pilotage de la démarche de cybersécurité au sein de l'EFS. Il définit la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il a également une mission de représentation externe en lien avec les organismes institutionnels et les tutelles dans le domaine de la sécurité des systèmes d'information. Il assure par ailleurs la fonction d'officier de sécurité des systèmes d'information.
- Service de cybersécurité (SCS) : le service cyber sécurité est en charge de la gestion opérationnelle de la sécurité du SI. Il est le relais indispensable entre la RNSSI et les correspondants des systèmes d'information des régions.
- Système d'Information (SI) : désigne l'ensemble des outils informatiques mis à la disposition des utilisateurs pour l'exercice de leur mission, que ce soit dans les locaux de l'établissement ou à l'extérieur de ceux-ci. Sont notamment visés les moyens suivants :
 - De production et de traitement (applications métiers, serveurs, automates biomédicaux, ordinateurs fixes et portables, tablettes, smartphones et autres périphériques informatiques) ;
 - De stockage que constituent tous les supports magnétiques fixes ou amovibles (disques durs, clés USB, ...) ;
 - De télécommunication (téléphonie, messagerie, internet, intranet, ...) ;

- De duplication permettant la reproduction d'un document ou d'une information originale (ex : imprimantes multifonctions, scanners, ...) ;
 - Des flux permettant d'échanger les informations.
- Traitement de données à caractère personnel : Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...).
 - Utilisateur : désigne une personne physique quel que soit son statut (personnel, stagiaire, prestataire de service, membre d'association, personnel mis à disposition ou détaché, etc.) qui accède, même de manière temporaire, aux systèmes d'Information de l'EFS.
 - Violation de données à caractère personnel : événement qui entraîne de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

2. Principes d'utilisation du système d'information

2.1. Loyauté

Chaque utilisateur doit adopter un comportement rationnel et loyal dans l'usage des systèmes d'information de l'établissement. Ainsi, cet usage ne doit pas nuire aux intérêts de l'établissement ou de ses personnels, ni au fonctionnement de l'établissement et doit s'inscrire dans le cadre d'une pratique raisonnable.

2.2. Utilisation professionnelle des systèmes d'information

Les ressources des systèmes d'information sont mises à la disposition des utilisateurs à des fins exclusivement professionnelles pour l'exercice des missions qui leur sont confiées par l'établissement.

Néanmoins, une utilisation à des fins personnelles de certaines ressources des systèmes d'information (ex : messagerie électronique, Internet, téléphonie) peut être exceptionnellement tolérée lorsqu'elle est motivée par des nécessités de la vie courante et/ou par l'urgence. Elle doit être alors peu fréquente, de courte durée ou peu volumineuse et identifiée comme « personnel ».

Cette utilisation extra-professionnelle des ressources des systèmes d'information ne peut en aucun cas entraver le bon fonctionnement des systèmes, ni se faire au détriment de l'activité professionnelle incombant à l'utilisateur, ni porter préjudice aux intérêts de l'établissement, des collaborateurs, des donneurs ou des tiers.

3. Respect des règles d'utilisation, de sécurité et de bon usage

Il appartient à chaque utilisateur d'adopter un comportement responsable pour l'utilisation des matériels de l'établissement. L'utilisation de ces ressources doit être réalisée en respectant les règles établies par l'EFS afin d'en éviter la saturation ou leur détournement à des fins personnelles.

L'utilisateur s'engage à :

- Respecter la politique nationale de sécurité des systèmes d'information de l'établissement, le Règlement intérieur, les directives données par le Responsable National de la Sécurité des Systèmes d'Information (RNSSI), par le Délégué Défense et Sécurité (pour les données classifiées SECRET), ou le Délégué à la Protection des Données (ou Data Protection Officer – DPO) ;
- Choisir des mots de passe en fonction de la politique des mots de passe de l'EFS. Ceci afin de garantir l'intégrité des données contenues dans le système d'information de l'EFS. Il est nécessaire de garder

secrets ses mots de passe, et en aucun cas ne les communiquer à des tiers (mot de passe de la session, LMT) ;

- Respecter les règles d'usage des postes de travail : ne pas laisser sans surveillance le matériel, verrouiller son ordinateur dès que l'utilisateur quitte son poste de travail ; ne pas démarrer son poste de travail à partir d'un support amovible qui aurait pour effet de contourner les mesures de sécurité du réseau de l'établissement (ex : clé USB, disque dur externe, CD, DVD) ; ne pas modifier la configuration du poste de travail sans l'intervention du service informatique de l'établissement ;
- Ne pas utiliser les clés USB non fournies par vos Responsables des systèmes d'information. Les clés fournies par ces derniers, sont à utiliser uniquement dans vos PC professionnels. Il est interdit de les brancher sur tout autre outil personnel.
- Ne pas brancher son téléphone mobile personnel ou professionnel pour le recharger à son pc. Les téléphones mobiles ne sont pas sécurisés. Cette interdiction vaut aussi pour le chargement des données ou images ;
- Favoriser l'utilisation de son téléphone mobile professionnel pour partager la connexion réseau au lieu d'utiliser les WIFI publics, lors de vos déplacements
- Ne pas mettre à la disposition d'utilisateurs non autorisés, un accès aux systèmes ou aux réseaux, à travers des matériels dont l'utilisateur a l'usage ;
- Ne pas utiliser ou essayer d'utiliser des comptes autres que celui affecté à chaque utilisateur, ou de masquer sa véritable identité ;
- Respecter l'usage de la messagerie électronique : limiter l'envoi de messages aux seuls destinataires réellement intéressés ou concernés, prévenir le risque de saturation des boîtes aux lettres et des serveurs en évitant de joindre à un même message des documents trop volumineux, s'assurer de l'exactitude de l'adresse électronique du destinataire du message, ne pas tenter d'intercepter ou de prendre connaissance d'un message dont il n'est pas destinataire, ne pas ouvrir les pièces jointes de courriers dont l'origine est inconnue, ne pas répondre aux messages non sollicités et dont l'expéditeur n'est pas identifié (spam...), ne pas transférer de messages professionnels vers sa messagerie personnelle ;
- Préserver la confidentialité et l'intégrité des données contenues sur des supports amovibles (CD, DVD, disques amovibles, clés USB, etc..) en utilisant le matériel et les outils fournis par l'EFS (DSI), et veiller à stocker ces données de manière chiffrée pour éviter tout risque de compromission (ex : perte, vol, dégradation ou accès illégitime) ;
- Ne mener aucune action corrective ou investigation technique de sa propre initiative ;
- Concernant les logiciels : ne pas effectuer de copies de logiciels commerciaux acquis par l'EFS, ne pas installer de logiciels sans l'autorisation de la DSI, ni contourner les restrictions d'utilisation.

En cas de tentative d'accès extérieur aux systèmes d'information de l'EFS, de perte ou de vol du matériel de l'établissement ou d'utilisation d'un support amovible dont la fiabilité est compromise (CD, DVD, disques amovibles, clés USB, etc..), l'utilisateur doit contacter le RNSSI. La procédure pour se connecter à nouveau en toute sécurité sera précisée à l'utilisateur.

Par ailleurs, si l'utilisateur vient à ouvrir une pièce jointe externe ou cliquer sur un lien externe qui lui semble frauduleux, il doit contacter sans délai le Service cybersécurité via l'adresse mail suivante alerte.virus@efs.sante.fr.

4. Protection des données

4.1. Protection des données à caractère personnel et des données professionnelles

La sauvegarde des intérêts de l'établissement passe par le respect par l'utilisateur d'une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations disponibles au moyen des systèmes d'information.

Les systèmes d'Information contiennent des données à caractère personnel et des données couvertes par le secret professionnel, ce qui implique que seules les personnes autorisées peuvent accéder à ces informations, sous réserve qu'elles en aient la nécessité d'accès et d'utilisation dans le cadre de leurs fonctions et pour l'exercice de leur mission.

4.2. Les obligations des utilisateurs et la protection des données à caractère personnel

Le traitement de données à caractère personnel par les utilisateurs doit respecter les principes directeurs suivants :

- Traitement licite, loyal et transparent au regard des personnes concernées ;
- Collecte pour des finalités déterminées, explicites et légitimes ;
- Pertinence et exactitude des données au regard des finalités poursuivies ;
- Respect des durées de conservation.

L'utilisateur ne peut consulter, copier, divulguer ou modifier des données contenues dans le système d'information que dans le strict cadre de l'accomplissement de sa mission. Il doit veiller en outre à la non-diffusion de ces données au-delà des destinataires autorisés. Les destinataires autorisés sont ceux qui ont été explicitement désignés pour en obtenir régulièrement communication.

Plus spécifiquement, lorsque l'utilisateur prend part à un traitement de données à caractère personnel en raison de l'exercice de ses missions professionnelles, ce traitement de données (modification, accès, lecture, extraction, destruction, ...) ne peut être réalisé qu'à des fins purement professionnelles. Toute poursuite d'une finalité autre que celle prévue au traitement est susceptible d'entraîner des sanctions disciplinaires, pénales et civiles.

Les utilisateurs ayant accès à des traitements de données à caractère personnel et doivent les utiliser pour des finalités déterminées, explicites et légitimes compte tenu de leurs missions et/ou de leurs fonctions.

L'utilisation des différentes applications professionnelles (médico techniques, support ou autres) répond aux mêmes principes et doit être légitime et en particulier répondre à une finalité conforme à l'exercice des missions de l'utilisateur et justifié par celui-ci.

L'utilisateur qui est amené à mettre en œuvre des traitements ou constituer des fichiers de données à caractère personnel, devra saisir au préalable son référent protection des données ou les équipes de la mission d'appui au DPO, conformément à la procédure en vigueur.

Tout incident constitutif d'une violation de données à caractère personnel (ex : vol ou perte de fichier contenant des données personnelles) doit être traité conformément à la procédure concernant les incidents affectant le SI et et/ou des données à caractère personnel qui décrit la conduite à tenir pour prendre en compte et qualifier des incidents affectant le système d'information de l'EFS et/ou affectant des Données à caractère personnel, en vue de notifier ou non ces incidents aux autorités compétentes.

4.2.1. Les obligations des utilisateurs et la protection des données professionnelles

Tous les fichiers ou documents stockés sur le matériel fourni par l'EFS sont professionnels à l'exclusion de ceux qui sont explicitement désignés par l'utilisateur comme relevant de sa vie privée.

Ces informations doivent être obligatoirement enregistrées dans le répertoire professionnel à usage individuel mis à disposition par la DSI.

Toutes les informations professionnelles doivent être stockées sur les répertoires partagés du réseau de l'EFS afin de bénéficier d'une sauvegarde, ou sur les supports qualifiés.

4.2.2. Protection des données à caractère confidentiel ou des données à caractère sensible

En cas de transmission par messagerie électronique de données à caractère confidentiel ou à caractère sensible (ex : données de santé) ces dernières doivent obligatoirement être chiffrées au préalable avec un outil de chiffrement mis à la disposition de l'utilisateur.

Les données à caractère confidentiel ou à caractère sensible ne doivent pas être stockées sans protection sur tout support tels que ceux dit « nomades » ou « amovibles » (ex : clés USB, disques externes, non chiffrés). Elles doivent faire l'objet d'une sécurisation renforcée (chiffrement du contenu).

Les données confidentielles et ou sensibles doivent être placées dans les répertoires tel que Sharedoc ou le répertoire sur le réseau informatique partagé de l'entité. Ceci à condition que les répertoires soient accessibles uniquement par les utilisateurs ayant le droit d'en connaître.

4.3. Préserver l'intégrité des systèmes informatiques et de télécommunications

L'établissement prend des dispositions techniques pour protéger son réseau des intrusions ou malveillances externes. L'utilisateur ne doit pas apporter volontairement de perturbations au bon fonctionnement des systèmes d'information et des réseaux et des télécommunications que ce soit par des manipulations inappropriées du matériel, par l'introduction volontaire, la propagation ou l'exécution de tout code malveillant y compris à des fins de tests (exemple : virus, cheval de Troie, bombes logiques).

5. Usage des services internet (web, réseaux sociaux, forum...)

Internet et les réseaux de communication ne sont pas des zones de non droit. L'utilisateur doit respecter les règles propres aux sites consultés ainsi que la législation en vigueur.

L'établissement met en place un dispositif de filtrage visant à interdire l'accès à certains sites considérés comme illicites, dangereux ou contraires aux dispositions de la Charte nationale (ex : sites pornographiques, sites pédopornographiques, sites de piratage informatique, etc.)

Certains blocages peuvent également intervenir en fonction de la menace (risque de cyber attaque).

Le contournement de ce dispositif est strictement interdit (ex : utilisation de relais d'anonymisation).

Face à la multiplication et au succès des réseaux sociaux, des blogs et forums de discussions, il est important de rappeler que ce mode d'expression est susceptible d'engager la responsabilité de l'établissement, mais également celle des utilisateurs.

Une vigilance renforcée des utilisateurs est donc indispensable, afin d'adopter une utilisation responsable et appropriée en distinguant ce qui relève de la sphère privée et ce qui relève de la sphère professionnelle.

L'accès et la contribution à des forums de discussion, blogs, réseaux sociaux pendant le temps de travail et sur le lieu de travail sont rendus possible aux utilisateurs dont les attributions professionnelles le prévoient.

Néanmoins l'utilisation de l'adresse professionnelle dans les sites ou forums à usage personnel n'est pas autorisée.

Les autres utilisateurs doivent disposer des autorisations expresses de la Direction de la Communication afin de s'exprimer au nom de l'établissement et devront préalablement prendre contact avec la Direction de la Communication.

Les espaces des réseaux sociaux peuvent rendre accessibles au plus grand nombre les informations diffusées par les utilisateurs.

L'établissement rappelle aux utilisateurs :

- La nécessité de veiller à la nature des informations qu'ils diffusent et au choix des personnes à qui ils souhaitent y donner accès,
- La nécessité de vérifier, avant toute mise en ligne, la possibilité de supprimer ultérieurement ces données afin de faire valoir leur droit à l'oubli numérique.

L'établissement garantit la liberté d'expression de l'utilisateur dans ses limites légales et contractuelles ainsi que dans le respect du principe de neutralité s'imposant aux collaborateurs de l'EFS en tant que participant à l'exécution d'un service public.

L'utilisateur doit être conscient des risques liés à la diffusion en ligne de contenus illicites ou de publications portant atteinte aux intérêts de l'établissement.

Aussi, s'expose à des sanctions disciplinaires, conformément aux dispositions du Règlement Intérieur de l'établissement l'utilisateur qui procède à :

- la publication de contenus dénigrant systématiquement l'établissement,
- la publication de commentaires diffamatoires, injurieux ou dénigrants à l'encontre de ses collègues, de ses supérieurs hiérarchiques,
- la diffusion d'informations confidentielles,
- la violation des obligations de discrétion et de loyauté inhérentes au contrat de travail.

L'utilisateur garantit qu'il n'usurpera pas l'identité d'une autre personne qu'il n'interceptera pas de communication entre tiers. Les services internet ne peuvent être utilisés pour proposer ou rendre accessible à des tiers des données et informations confidentielles, professionnelles ou contraires à la législation en vigueur.

6. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique ou pour des raisons de sécurité des personnes ou des biens , l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable, par les entités de tutelle (Ministère en charge de la Santé et Agence nationale de la sécurité des systèmes d'information, Agence du numérique en santé, ...) et en interne par toute direction ou service, spécialement et expressément missionné par le Président de l'EFS (Délégué Défense et Sécurité – DDS- , Direction Risques Audit et Qualité - DRAQ, RNSSI, tout prestataire d'Audit missionné ou délégués par les tutelles, ou par le Président de l'EFS).

Les administrateurs ont à leur disposition les fichiers de traces générées par l'ensemble des services utilisés. Ces fichiers ne seront utilisés que pour un usage technique. Toutefois, les administrateurs pourront être autorisés à analyser ces fichiers de traces dans le cas d'un incident de sécurité et sous la demande expresse de la RNSSI ou du Délégué Défense et Sécurité dans le cadre d'une enquête administrative.

Ces fichiers et traces font l'objet d'un traitement de données à caractère personnel par l'EFS, en tant que responsable de traitement et dont le siège se situe 20 avenue du Stade France, 93218 La Plaine Saint-Denis Cedex. Ce traitement est mis en œuvre pour des finalités de sécurité, de contrôle du respect des règles et de détection des abus, de gestion technique ainsi que de production d'indicateurs. Ce traitement est automatique et est fondé sur l'intérêt légitime de l'EFS à pouvoir sécuriser son système d'information.

Ces données sont conservées pendant une durée maximum d'un an et sont destinées aux entités de tutelle ainsi qu'aux personnels de l'EFS ou à ses prestataires habilités à en connaître. En cas d'alerte, ces données peuvent être conservées plus longtemps, dans la limite de trois ans.

L'utilisateur peut accéder et obtenir copie des données le concernant, s'opposer au traitement de ces données en justifiant d'une situation particulière, les faire rectifier ou les faire effacer en cas d'inexactitude. Il dispose également d'un droit à la limitation du traitement de ses données. Pour exercer ses droits ou pour toute question sur le traitement de ses données, il peut contacter la Direction des Ressources Humaines de l'établissement dont il dépend. Enfin, l'utilisateur dispose du droit d'introduire une réclamation auprès de la Commission Nationale Informatique et Libertés (CNIL). L'EFS a désigné un délégué à la protection des données (ou DPO) dont l'adresse de messagerie est efs.dpo@efs.sante.fr.

7. Modalités d'accès et de conservation

7.1. Modalités d'accès

7.1.1. Accès aux systèmes d'information tout au long de l'exercice professionnel au sein de l'établissement

Les droits d'accès de l'utilisateur aux Systèmes d'Information sont strictement personnels.

L'accès et le maintien dans le système d'information sont limités à l'accomplissement des missions de l'utilisateur. Chaque utilisateur est responsable de la protection des informations auxquelles il a accès au moyen du système d'information. L'extraction ou le transfert d'un document couvert par le secret professionnel à des fins personnelles est strictement interdit.

L'établissement peut mettre à disposition d'un utilisateur, si sa mission le nécessite, un accès à distance sur tout ou partie du SI, un ordinateur, un téléphone portable, etc. L'utilisation de ces technologies doit se limiter aux nécessités de l'activité professionnelle.

Sauf autorisation expresse de la direction, l'accès au système d'information/ au réseau de l'établissement avec du matériel n'appartenant pas à l'établissement (PC personnel, assistants personnels, supports amovibles...) ou bien avec un PC portable propriété de l'EFS mais non géré par la DSI, est interdit. **Dans le cas où il a été autorisé, il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé à ses données et à son innocuité.**

7.1.2. Accès aux systèmes d'information en cas de suspension ou de cessation d'activité au sein de l'établissement

L'utilisateur n'est plus autorisé à accéder aux systèmes d'Information à compter de la date de son départ effectif de l'établissement.

En cas de cessation provisoire d'activité (ex : changement temporaire d'affectation, d'absence, arrêt maladie, congés maternité, congés parental, congé sabbatique, congé création d'entreprise, etc.), le droit d'accès pourra être suspendu sur demande du manager et en accord de la Direction des Ressources Humaines compétente.

Si le comportement d'un utilisateur constitue un risque avéré pour la sécurité du système d'information, ses accès peuvent être suspendus à titre conservatoire sur décision conjointe de DDS, DSI et DRH.

Aussi, l'utilisateur s'engage à supprimer les documents, informations et messages identifiés comme lui étant personnels et stockés sur les matériels mis à sa disposition par l'établissement. Cette suppression interviendra au plus tard à la cessation de l'activité professionnelle (à la date de son départ effectif, à compter de la dispense de préavis, etc.). Tout autre document est considéré professionnel et ne doit donc pas être effacé ni transféré sur un support externe personnel.

Dans le cas du départ définitif, d'un cadre dirigeant, son responsable hiérarchique doit demander l'accès au poste de l'utilisateur au Délégué Défense et Sécurité qui exécutera les actions dans les conditions légales et réglementaires.

En outre, l'utilisateur s'engage expressément à restituer les matériels qui lui auront été confiés ainsi que toute copie ou reproduction en sa possession des moyens de stockage, le jour où il cessera effectivement ses fonctions.

L'établissement étant une personne morale de droit public, l'ensemble des données générées par l'utilisateur dans le cadre de son exercice professionnel constitue des archives publiques au sens du Code du patrimoine.

7.2. Archivage des messages professionnels

Comme le contenu enregistré sur le matériel fourni par l'établissement, le contenu de la messagerie mise à disposition de l'utilisateur est présumé être professionnel.

Au départ de l'utilisateur ou lorsque sa mission au sein de l'établissement prend fin, sa messagerie électronique est désactivée à J+1, sauf demande de prolongation exceptionnelle pour des raisons de continuité de service émanant de l'autorité hiérarchique.

Le contenu de la messagerie professionnelle d'un utilisateur peut être archivé. La DRH devra, dans ce cas de figure, prévenir l'utilisateur de veiller à supprimer de sa messagerie les éléments de nature personnelle. La durée de conservation étant définie par procédure interne.

Le responsable hiérarchique peut demander à la DRH d'autoriser l'accès à la messagerie professionnelle et aux répertoires de travail du personnel sous ses ordres, exception faite des cadres dirigeants qui pourront être pris en charge par le Délégué Défense et sécurité.

Des règles spécifiques à la conservation des messageries existent concernant les cadres dirigeants.

7.3. Archivage des informations dématérialisées

Les informations dématérialisées du Président de l'établissement ainsi que les Directeurs d'Établissements de Transfusion Sanguine, des membres du COMEX et plus largement des cadres dirigeants, seront archivées sur un disque dur externe chiffré et entreposé dans le bureau du Délégué Défense et Sécurité.

8. Respect du droit de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies, ou autres créations protégées par le droit de la propriété intellectuelle, sans avoir obtenu préalablement l'autorisation du ou des titulaire(s) de ces droits s'agissant de l'utilisation envisagée.

9. Sanctions

En cas de violation aux dispositions de la Charte nationale, la suppression du droit d'accès de l'utilisateur à tout ou partie des systèmes d'information peut être décidée à titre temporaire ou définitif.

Suivant la gravité des faits, une enquête administrative pourra être diligentée sur ordre du Président de l'EFS.

L'établissement mettra en jeu la responsabilité civile et pénale de l'utilisateur pour toute infraction commise au moyen des systèmes d'information et en dehors de ses missions.

9.1. Dispositions propres aux utilisateurs membres des personnels de l'établissement

Le non-respect de la Charte nationale entraînera de manière appropriée et proportionnée aux manquements commis, l'application des sanctions disciplinaires prévues par le règlement intérieur applicable à l'utilisateur concerné, outre les sanctions civiles et pénales pouvant découler de tels agissements.

9.2. Dispositions propres aux utilisateurs membres d'une entreprise extérieure

Le non-respect de la Charte nationale par l'utilisateur membre d'une entreprise extérieure, lorsqu'il est constaté par l'établissement, entraîne l'application des sanctions prévues par le contrat (ou le marché) conclu entre l'entreprise concernée et l'établissement, outre les sanctions civiles et pénales pouvant découler de tels agissements.

10. Publicité

La présente Charte, est portée à la connaissance de l'ensemble des utilisateurs selon les mêmes modalités que le prévoit le Règlement Intérieur auquel elle est annexée. Elle est aussi mise à disposition au sein de l'intranet nationale.

Pour les salariés de sociétés extérieures qui doivent utiliser les ressources informatiques de l'EFS, cette charte leur est communiquée à l'établissement du contrat de prestation qui les lie à l'EFS.

11. Entrée en vigueur

Cette Charte a été soumise à l'avis consultatif des membres du Comité social et économique central (CSEC) et à celui des membres du comités sociaux et économiques d'établissements régionaux. Elle remplace les chartes existantes ayant le même objet au sein de l'EFS.

Les avis émis par ces institutions et deux exemplaires de la Charte ont été communiqués à l'Inspecteur du travail.

La Charte, déposée au secrétariat du greffe du conseil des prud'hommes compétent et affichée conformément aux dispositions du code du travail entre en vigueur un mois après l'accomplissement des formalités de dépôt et de publicité. La date d'entrée en vigueur est stipulée dans le règlement intérieur de chaque ETS.

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

Cette charte entrera en vigueur un mois après la date d'accomplissement de sa publicité et de dépôt.