



Etablissement Français du Sang

LE LIEN ENTRE LA GÉNÉROSITÉ DES DONNEURS DE SANG ET LES BESOINS DES MALADES

CHARTER D'UTILISATION DU SYSTÈME D'INFORMATION DE L'EFS



Sommaire

1. Statut de la Charte	4
<i>A. Définitions</i>	4
<i>B. Application de la Charte</i>	5
2. Utilisation du système d'information	6
<i>A. Principes généraux</i>	6
<i>B. Sécurité du système d'information</i>	7
<i>C. Protection des données contenues dans le système d'information</i>	10
<i>D. Utilisation responsable des ressources du système d'information</i>	12
<i>E. Information des utilisateurs</i>	17
3. Sanctions	18
4. Information des utilisateurs	18
5. Sensibilisation des personnels	19
6. Entrée en vigueur	19



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 Charte d'utilisation du système d'information de l'EFS a été élaborée dans le cadre de la politique de sécurité du système d'information de l'établissement. Elle a pour vocation de concilier la sûreté des services électroniques de communication et d'information de l'EFS avec les libertés individuelles et la vie privée des utilisateurs auxquels elle s'adresse.

Elle pose les règles d'emploi des ressources du système d'information afin de sensibiliser les utilisateurs et de prévenir des dérives de l'utilisation des technologies de l'information et de la communication.

Elle est guidée par les principes de transparence, de sécurité et de responsabilité des utilisateurs.

Chaque utilisateur doit être conscient qu'il est un acteur de la sécurité du système d'information de l'établissement.

L'EFS s'engage à respecter les cinq grands principes de la loi « Informatique et Libertés » en matière d'exploitation des données à caractère personnel :

- **Principe de finalité**

Les données à caractère personnel des utilisateurs ne seront recueillies et traitées que pour un usage déterminé et légitime.

- **Principe de proportionnalité**

Les données traitées seront cohérentes avec la finalité du traitement et devront être strictement nécessaires à cette finalité.

- **Principe d'une durée adéquate de conservation des données**

La durée de conservation est déterminée en fonction de la finalité de chaque traitement.

- **Principe de sécurité et de confidentialité des données**

L'établissement garantit la sécurité et la confidentialité des données qu'il collecte. L'EFS prend toutes les mesures nécessaires pour garantir la confidentialité des données et éviter qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés (y compris en interne).

- **Principe du respect des droits des personnes**

La Charte a notamment pour fin d'informer clairement les utilisateurs du système d'information des objectifs poursuivis et des modalités d'exercice de leurs droits.



Statut de la Charte

A. Définitions

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

Charte : désigne le présent document. La Charte s'impose aux utilisateurs au même titre que le règlement intérieur des ETS et des services centraux dont elle constitue une annexe.

Etablissement : désigne l'Etablissement Français du Sang (EFS) et ses établissements de transfusion sanguine (ETS) ainsi que les services centraux (SC).

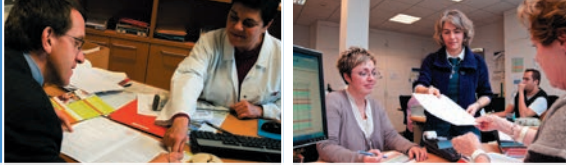
Utilisateur : désigne une personne physique quel que soit son statut (personnel, stagiaire, prestataire de service, membre d'association, personnel mis à disposition ou détaché, etc.) qui accède, même de manière temporaire, au système d'information.

Administrateur : désigne les personnels en charge des opérations de support et d'administration des systèmes de l'établissement.

Système d'information (SI) : désigne l'ensemble des outils mis à la disposition des utilisateurs pour l'exercice de leur mission, que ce soit dans les locaux de l'EFS ou à l'extérieur de ceux-ci.

Sont notamment visés les moyens suivants :

- de production et de traitement (applications métiers, serveurs, automates biomédicaux, postes de travail, smartphones et autres périphériques informatiques),
- de stockage que constituent tous les supports magnétiques fixes ou amovibles (disquettes, CD et DVD ROM, disques durs, clés USB...),
- de télécommunication (téléphonie, messagerie, internet, intranet),
- de duplication permettant la reproduction d'un document ou d'une information originale (ex : photocopieuses, scanners...),
- les flux permettant d'échanger les informations.



Donnée à caractère personnel : désigne une information permettant l'identification d'une personne physique de manière directe ou indirecte.

Donnée couverte par le secret professionnel : désigne une information confidentielle en raison de sa 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).

Correspondant sécurité du système d'information (CSSI) : désigne la personne nommée par le directeur de chaque ETS. Il constitue un relais auprès des utilisateurs du SI au sein de l'établissement et assure un rôle de support dans le respect quotidien des exigences de sécurité applicables.

La liste complète et actualisée des CSSI est consultable sur l'intranet national.

Intranet national : désigne un réseau informatique interne semblable à internet mais propre à l'établissement.

B. Application de la Charte

La Charte contient les règles d'utilisation du système d'information de l'établissement.

Elle définit les droits et obligations que l'établissement s'engage à respecter, notamment les conditions et les limites des éventuels contrôles portant sur l'utilisation du système d'information.

Elle rappelle l'existence de sanctions applicables en cas de contravention aux règles et principes qu'elle établit ou rappelle (cf. Responsabilité des utilisateurs).

La Charte constitue un des moyens mis en œuvre pour préserver la sécurité du système d'information et trouve son complément dans les politiques de sécurité du système d'information disponibles sur l'intranet national.

La Charte s'impose aux utilisateurs du système d'information de l'EFS quel que soit leur statut.

Les administrateurs du système d'information sont soumis à la Charte au même titre que les utilisateurs. Ils sont également soumis à la Charte d'utilisation des systèmes spécifiques aux administrateurs.



Utilisation du système d'information

A. Principes généraux

1. Principe de loyauté

Chaque utilisateur doit adopter un comportement rationnel et loyal dans l'usage du système d'information de l'établissement. Ainsi, cet usage ne doit pas nuire aux intérêts de l'EFS ou de ses personnels, ni au fonctionnement de l'établissement et s'inscrit dans le cadre d'une pratique raisonnable afin d'éviter toute dérive.

L'utilisateur n'est plus autorisé à accéder au système d'information à compter de la date de son départ effectif de l'établissement.

Aussi, les documents et informations personnels stockés par l'utilisateur dans les matériels de l'établissement devront être supprimés par lui-même à cette date.

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.

2. Utilisation professionnelle du système d'information

Les ressources du système 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 du système d'information (messagerie électronique, internet, téléphone) peut être exceptionnellement admise 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 » lorsque cela est possible.

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



B. Sécurité du système d'information

1. Droits d'accès de l'utilisateur

Les droits d'accès au système d'information de l'utilisateur sont strictement personnels.

L'accès et le maintien dans le système sont limités à l'accomplissement des missions de l'utilisateur. Tout accès ou maintien dans le système en dehors de ses missions par l'utilisateur est considéré comme non autorisé et pourra être qualifié de frauduleux.

Chaque utilisateur se réfère aux procédures définies par l'établissement concernant l'accès aux ressources (application, partage réseau, matériel, etc.).

Chaque utilisateur est responsable de la protection des informations auxquelles il a accès au moyen du système d'information. Il applique les recommandations de sécurité de l'établissement.

L'EFS peut mettre à disposition d'un utilisateur, si sa mission le nécessite, un accès à distance à tout ou partie du SI, un ordinateur, un téléphone portable ; ces technologies ne présument pas de contraintes professionnelles hors du temps de travail. L'utilisation de ces technologies doit par conséquent se limiter aux nécessités de l'activité professionnelle.

2. Authentification de l'utilisateur

Les moyens d'accès au système d'information de l'utilisateur ne peuvent en aucun cas être cédés.

L'utilisateur est responsable de la protection des moyens d'authentification qui lui sont confiés (mot de passe, carte à puce et code pin, carte professionnelle de santé ou autres dispositifs), et qui l'identifient lors de ses accès au système d'information.

En cas de perte des moyens d'authentification ou de difficulté de connexion, la direction des systèmes d'information donne à l'utilisateur la marche à suivre pour qu'il puisse à nouveau se connecter en toute sécurité.



3. Gestion des identifiants de l'utilisateur

Lorsque l'accès à certains éléments du système d'information (la messagerie électronique ou téléphonique, les sessions sur les postes de travail, etc.) est protégé par des paramètres de connexion (identifiant et mot de passe) permettant l'authentification de l'utilisateur, ces paramètres doivent respecter les consignes de sécurité élaborées par la direction des systèmes d'information.

Le mot de passe doit être difficile à deviner et facile à retenir (il est possible de prendre par exemple les premières lettres d'un texte, d'une chanson que l'on connaît : ainsi, « Au clair de la lune, mon ami Pierrot » devient « Ac2llmaP »).

Le mot de passe ne doit pas être un mot du dictionnaire ou un mot en rapport avec la vie courante (prénom du conjoint ou des enfants, date de naissance, de mariage, etc., sont à proscrire).

Le mot de passe devra être régulièrement changé.

En outre, un mot de passe ne doit pas être inscrit sur un support accessible à des tiers.

Les modalités pratiques de constitution d'un mot de passe sont consultables dans la rubrique « sécurité des systèmes d'information » de l'intranet national.

4. Intégrité du système d'information

L'EFS prend des dispositions techniques pour protéger son réseau des intrusions ou de malveillances externes. L'utilisateur est tenu de ne pas mettre en péril ces dispositifs par l'introduction de matériels de communication sans un accord préalable express de la direction des systèmes d'information. En particulier, la connexion de modems ou de dispositifs de réseau sans fil (Wifi, Bluetooth) permettant un accès externe est formellement interdite.

Il est interdit d'apporter, volontairement ou non, des perturbations au bon fonctionnement du SI, que ce soit par des manipulations anormales du matériel, par l'introduction de logiciels non autorisés ou le contournement de règles de sécurité (ex : arrêt de l'antivirus ou des mises à jour de sécurité).

L'introduction volontaire (développement, décompilation, copie, téléchargement, etc.), la propagation ou l'exécution de tout code malveillant (virus, etc.) au sein du système d'information de l'EFS sont strictement interdits, même pour procéder à des tests.

La connexion d'ordinateurs personnels ou d'intervenants externes est strictement interdite sauf autorisation exceptionnelle accordée par le Correspondant sécurité du système d'information (CSSI).



5. Incidents de sécurité

Tout événement remettant potentiellement en cause la sécurité du système d'information (ex : la perte ou le vol d'équipements informatiques, tentative d'accès non autorisé, etc.) de l'EFS doit être signalé sans délai par l'utilisateur auprès du CSSI (la propagation de certaines attaques informatiques est rapide et les conséquences peuvent être importantes).

L'utilisateur ne doit mener aucune action corrective ou d'investigation technique de sa propre initiative.

6. Déconnexion du système d'information

Afin d'éviter l'accès au système d'information par des personnes non autorisées, l'utilisateur veille à se déconnecter des applications ou, a minima, à verrouiller sa session de travail lorsqu'il quitte son poste de travail même momentanément.

7. Droit d'accès de l'établissement

L'établissement peut accéder librement au poste de travail des utilisateurs, notamment en cas d'absence, si cet accès est utile à la poursuite des activités.

Une demande d'accès au poste de l'utilisateur doit être adressée à la direction des ressources humaines.

L'utilisateur est informé, préalablement, de la nécessité d'accéder à son poste informatique.

L'EFS s'engage à ce que les messages et dossiers de l'utilisateur identifiés comme « personnels » ne soient pas consultés.



C. Protection des données contenues dans le système d'information

1. Respect de l'intégrité et de la confidentialité des données

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 du système d'information.

L'utilisateur ne peut consulter, copier, divulguer ou modifier des données 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.

Toutes les données à caractère personnel, ainsi que toutes les données relatives à l'EFS et notamment à son fonctionnement, sont couvertes par l'obligation de discrétion prévue par la convention collective, et éventuellement par une clause contractuelle de confidentialité.

2. Protection des données à caractère personnel

Les fichiers contenant des données à caractère personnel doivent faire l'objet d'une attention particulière dans la mesure où ces fichiers concernent la vie privée des personnes et peuvent porter atteinte à leurs libertés.

Les utilisateurs ayant accès à ces fichiers doivent les utiliser pour des finalités déterminées, explicites et légitimes compte tenu de leurs missions ou de leurs fonctions.

Le système d'information contient 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.

Les destinataires autorisés sont ceux qui ont été explicitement désignés pour en obtenir régulièrement communication.

Si, dans l'exercice de ses missions, l'utilisateur est amené à mettre en œuvre des traitements, ou constituer des fichiers, de données à caractère personnel, il devra en informer la direction des affaires juridiques de l'établissement et se conformer aux recommandations en matière de protection des données qui lui seront transmises.



3. Transmission de données couvertes par le secret professionnel

En cas de transmission de données couvertes par le secret professionnel par messagerie électronique, le chiffrement (ou cryptage) de ces données est obligatoire.

Un outil de cryptage mis à disposition par le service informatique permet à l'utilisateur, qui en fait la demande, de crypter des données.

L'utilisateur peut demander l'assistance du service informatique pour réaliser le cryptage de l'information.

L'utilisateur ne doit pas utiliser sans protection des supports dits « nomades » ou amovibles tels que des ordinateurs portables, clés USB, disques externes, smartphones, etc., pour la transmission de données couvertes par le secret professionnel.

4. Données contenues sur les supports amovibles

Les supports amovibles (disquettes, CD, DVD, disques amovibles, clés USB, ...) sont sous la responsabilité de l'utilisateur.

Pour préserver la confidentialité des données qu'ils contiennent, chacun veille à les stocker de manière à les préserver contre tout risque de perte ou de vol.

En cas de vol ou de perte, il conviendra pour l'utilisateur de se référer à la procédure d'incident (cf. 5. Incidents de sécurité page 9)

5. Stockage d'informations personnelles

Toutes les informations sont professionnelles à l'exclusion de celles qui sont explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans des répertoires explicitement prévus à cet effet et intitulés « personnel ».



D. Utilisation responsable des ressources du système d'information

1. Principes généraux

Il appartient à chaque utilisateur d'adopter un comportement responsable pour l'utilisation du matériel de l'établissement.

L'utilisateur ne peut prétendre à aucun droit de propriété sur le matériel mis à disposition par l'EFS.

Le matériel et les ressources restent, quel qu'en soit leur usage, la propriété de l'établissement.

Chaque utilisateur prend toutes les dispositions utiles pour éviter le vol, la perte et la dégradation des matériels de l'établissement notamment :

- ne pas laisser sans surveillance le matériel dans un lieu public,
- ne pas démarrer un poste de travail à partir d'un support amovible (disquette, clé USB, disque dur externe, CD, DVD),
- ne pas modifier la configuration de son poste de travail sans l'intervention du service informatique de l'établissement.

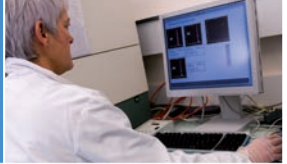
2. Utilisation des logiciels

Seuls les logiciels bénéficiant d'une licence en cours de validité et ayant été approuvés par la direction des systèmes d'information peuvent être installés sur les matériels de l'EFS.

L'installation d'un logiciel dont la provenance est externe à l'établissement sur les serveurs et postes de travail doit être réalisée par le service informatique.

3. Utilisation de la messagerie électronique

La messagerie électronique est un outil de communication électronique permettant à l'utilisateur d'envoyer et de recevoir des messages électroniques à l'intérieur et à l'extérieur de l'EFS.



Son utilisation est présumée professionnelle.

L'utilisateur qui souhaite utiliser, à titre exceptionnel, la messagerie à des fins privées, est tenu d'indiquer clairement dans l'objet du message la mention «Personnel». Les messages personnels reçus doivent être également classés, dès réception, dans un dossier lui-même nommé «Personnel».

Tout message reçu ou destiné à une institution représentative du personnel doit être signalé et classé de la même manière que les messages personnels.

L'utilisateur est susceptible d'engager sa responsabilité pour tout usage abusif de cette mention.

Il s'engage à ne pas effectuer, de manière volontaire, des opérations pouvant nuire au fonctionnement de la messagerie.

Il s'engage notamment à :

- limiter l'envoi de messages aux seuls destinataires réellement intéressés ou concernés, pour éviter la saturation du réseau et des serveurs et ne pas obliger les destinataires à lire des messages sans intérêt pour eux,
- ne pas procéder à des envois massifs de courriers,
- prévenir le risque de saturation des boîtes aux lettres et des serveurs en évitant de joindre à un même message des documents trop volumineux,
- ne pas interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés,
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources,
- ne pas introduire volontairement des virus via la messagerie.

Il s'engage à ne pas effectuer, de manière volontaire, des opérations pouvant nuire à la confidentialité des données qu'il transmet.

A ce titre, l'utilisateur :

- doit s'assurer de l'exactitude de l'adresse électronique du destinataire du message,
- ne doit pas tenter d'intercepter ou de prendre connaissance d'un message dont il n'est pas destinataire,



- ne doit pas envoyer et/ou répondre à des chaînes de message,
- ne doit pas ouvrir les pièces jointes de courriers dont l'origine lui est inconnue,
- ne doit pas répondre aux messages non sollicités et dont l'expéditeur n'est pas identifié (spam...).

Enfin, dans la mesure du possible, l'utilisateur s'engage à ne pas communiquer son adresse de messagerie sur des serveurs internet qui le demanderaient pour éviter de l'exposer à la réception de nombreux messages publicitaires.

4. Utilisation de l'internet

L'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.

> Contenus illégaux

Aussi, 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.

A ce titre, il est rappelé que sont interdits et pénalement sanctionnés :

- l'atteinte à la vie privée d'autrui,
- la diffamation et l'injure,
- la provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur,
- l'incitation à la consommation de substances interdites,
- la provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination, à la haine notamment raciale, ou à la violence,
- l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité,
- la négation de crimes contre l'humanité,
- la contrefaçon de marques,



- la reproduction, représentation ou diffusion d'une œuvre de l'esprit (ex : musique, photo, etc.),
- les copies de logiciels hormis la copie de sauvegarde dans les conditions prévues par le Code de la propriété intellectuelle.

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 (ex : sites pornographiques, sites pédopornographiques, sites de piratage informatique, etc.)

> Services de communication en ligne

Face à la multiplication et au succès des réseaux sociaux, des blogs et forums de discussion, il est important de rappeler que ce mode d'expression est susceptible d'engager la responsabilité de l'EFS, 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.

Les autres utilisateurs doivent disposer des autorisations expresses de la direction de l'EFS 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'EFS 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.



> Liberté d'expression individuelle

L'établissement garantit la liberté d'expression de l'utilisateur dans ses limites légales et contractuelles.

Aussi, s'expose à des sanctions disciplinaires, l'utilisateur qui procède :

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

5. Utilisation de la téléphonie

Des téléphones peuvent être mis à disposition des utilisateurs. Leur utilisation est réservée à des fins professionnelles.

Leur utilisation à des fins personnelles est tolérée, lorsqu'elle est motivée par des nécessités de la vie courante et/ou par l'urgence et respecte les principes généraux d'utilisation du système d'information.

L'EFS est en mesure de contrôler, par la mise en place d'autocommutateurs, le nombre des appels, les numéros appelés, la durée et le coût des communications téléphoniques de façon globale, par service ou par utilisateur.

Ces informations sont conservées sous forme de listes. Ces listes occultent les quatre derniers chiffres des numéros d'appel.

Elles sont archivées pendant six mois.



E. Information des utilisateurs

1. Opération de support sur le matériel de l'utilisateur

L'utilisateur dont le poste fait l'objet d'une action de support individuel par le service informatique (y compris à distance) doit préalablement en être informé et donner son accord.

Les administrateurs sont soumis à une obligation de discrétion.

La divulgation des données couvertes par le secret professionnel ou relevant de la vie privée de l'utilisateur qu'ils sont amenés à connaître est strictement interdite.

Le non respect de la confidentialité des informations dont les administrateurs auraient eu connaissance au cours des opérations de support pourra donner lieu à des sanctions de nature disciplinaire.

2. Traçabilité

L'utilisation des équipements informatiques à des fins non appropriées peut engager la responsabilité de l'EFS et celle de l'utilisateur.

Les événements, les actions ou les tentatives affectant une ressource sont susceptibles de laisser une trace dans les journaux d'événements tenus par chaque système et chaque application. Il s'agit des données de connexion de l'utilisateur.

Pour des nécessités de gestion technique, de contrôle du respect des règles énoncées dans la Charte ainsi qu'à des fins statistiques, d'optimisation, de sécurité, de détection des abus, l'EFS met en place, dans le respect de la législation en matière de protection de la vie privée des utilisateurs, des dispositifs de traçabilité et de contrôle.

Toutes les données relatives à l'activité de navigation sur internet ainsi que les accès autorisés ou interdits sont conservés pendant une durée d'un an.

La mise en œuvre de ces mesures a été soumise à l'avis consultatif du comité central d'entreprise le 16/02/2012.

Concernant le traitement de données les concernant, les utilisateurs disposent, conformément aux dispositions de la loi "Informatique et Libertés" du 6 janvier 1978, d'un droit d'accès, de rectification, de suppression à ces informations, et en cas, de motif légitime, d'opposition. Ils exercent ces droits auprès de la direction des ressources humaines.

03



Sanctions

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

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

> Dispositions propres aux utilisateurs membres des personnels de l'EFS

Le non respect de la Charte entraînera de manière appropriée et proportionnée aux manquements commis, l'application des sanctions disciplinaires prévues par le règlement intérieur applicable à l'utilisateur concerné.

> Dispositions propres aux utilisateurs membres d'une entreprise extérieure

Le non respect de la Charte par l'utilisateur n'appartenant pas au personnel EFS, lorsqu'il est constaté par l'établissement, entraîne l'application des sanctions prévues par le contrat (ou le marché) conclu entre l'entreprise et l'établissement.

04



Information des utilisateurs

La Charte est portée à la connaissance des utilisateurs par voie d'affichage et annexée au règlement conformément aux dispositions du code du travail.

Elle est communiquée individuellement à l'utilisateur lors de son arrivée dans l'établissement.

La direction des systèmes d'information est à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation du système d'information.

La Charte, ainsi que les procédures auxquelles elle se réfère expressément, sont disponibles sur l'intranet national de l'EFS.



05



Sensibilisation des personnels

Les personnels seront informés des règles d'utilisation prévues par la Charte au moyen de campagnes annuelles de sensibilisation organisées par l'EFS.

06



Entrée en vigueur

Cette Charte a été soumise à l'avis consultatif des membres du comité central d'entreprise et à celui des membres des CHSCT et des comités d'établissements des ETS. Elle remplace les chartes existantes au sein des ETS.

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.

Cette Charte sera révisée, tous les quatre ans, afin de tenir compte, si nécessaire, des évolutions technologiques.

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

Etablissement Français du Sang

20, avenue du Stade de France - 93218 La Plaine Saint-Denis Cedex

Tél. : 01 55 93 95 00 - Fax : 01 55 93 95 03 - www.etablissement-francais-du-sang.fr