

Charte nationale de sécurité de l'utilisateur du système d'information



- ☒ public
- ☐ interne
- ☐ diffusion restreinte
- ☐ confidentiel

REVISIONS

Date	Objet
Juin 2017	Version initiale

Table des matières

PREAMBULE	5
1. CHAMP D'APPLICATION	5
1.1 LA CHARTE S'APPLIQUE A TOUS	5
1.2 DISPOSITION PARTICULIERE CONCERNANT LES IRP ET SYNDICATS.....	5
<hr/>	
2. APPLICATION DE LA CHARTE	6
3. REGLES D'UTILISATION DU SYSTEME D'INFORMATION	6
3.1 LES CONDITIONS D'UTILISATION DES RESSOURCES	6
3.2 LA PROTECTION DES RESSOURCES.....	6
3.3 LES EQUIPEMENTS NOMADES	7
3.4 LES SUPPORTS AMOVIBLES	7
3.5 LA PROTECTION DES DROITS D'ACCES AU SYSTEME D'INFORMATION.....	8
3.6 LA PROTECTION DES DONNEES ET DOCUMENTS ELECTRONIQUES	8
3.7 UTILISATION RESIDUELLE A TITRE PRIVE	9
3.8 PROTECTION DES DONNEES PRIVEES DE L'UTILISATEUR.....	9
3.9 LA GESTION DES ABSENCES ET DES DEPARTS	11
3.10 LE DEVOIR DE SIGNALEMENT ET LE RESPECT DES CONSIGNES.....	11
<hr/>	
4. REGLES D'UTILISATION DES COMMUNICATIONS ELECTRONIQUES	12
4.1 LA MESSAGERIE ELECTRONIQUE.....	12
4.2 L'INTERNET ET L'INTRANET	12
<hr/>	
5. UTILISATEURS A DROITS SPECIFIQUES	14
5.1 ROLE ET RESPONSABILITE DU GESTIONNAIRE D'APPLICATION	14
5.2 ROLE ET RESPONSABILITE DU GESTIONNAIRE DES HABILITATIONS	15
<hr/>	
6. ROLE ET RESPONSABILITE DE L'ADMINISTRATEUR DU SI	15
7. TRAÇABILITE	15
7.1 INTERNET	16
7.2 MESSAGERIE ELECTRONIQUE.....	16
7.3 APPLICATIONS ET RESEAUX INTERNES.....	16
7.4 TELEPHONIE	17
<hr/>	

8.	RESPECT DES REGLEMENTATIONS	17
8.1	LE RESPECT DE LA LOI	17
8.2	LE RESPECT DE LA PROPRIETE INTELLECTUELLE	17
8.3	LE RESPECT DE LA LOI INFORMATIQUE ET LIBERTES.....	18
<hr/>		
9.	CONTROLE DE L'APPLICATION DE LA CHARTE ET SANCTIONS.....	18
9.1	LE CONTROLE DE L'APPLICATION DE LA CHARTE.	18
9.2	LIMITATION DES USAGES ET SANCTIONS.....	18
<hr/>		

PREAMBULE

Implanté au cœur du réseau de la branche famille, chaque organisme¹ en partage le système d'information. Les composants de ce système sont dépendants les uns des autres, une défaillance de l'un d'eux a des conséquences qui peuvent dépasser largement le composant lui-même et est susceptible d'impacter l'ensemble du système.

Par conséquent, le bon fonctionnement et la sécurité du système d'information de la branche Famille suppose le respect, par tous, des dispositions législatives, réglementaires, bonnes pratiques relevant de normes et règles d'usage visant à assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité.

La présente charte, dont la CNIL en soutient l'initiative, définit les règles d'usages et de sécurité que l'organisme et l'utilisateur s'engagent à respecter, permettant ainsi de garantir un juste équilibre entre, d'une part, les objectifs de sécurité de l'organisme et, d'autre part, le respect de la vie privée et des libertés individuelles des utilisateurs.

Elle n'a pas pour objectif de couvrir de façon exhaustive tous les cas de figure pouvant se présenter dans le cadre de l'utilisation des moyens informatiques et de communication électronique mis à la disposition par l'organisme. C'est dans l'esprit des règles présentées dans ce document que chacun devra se conformer dans des situations non envisagées.

La présente charte est susceptible d'évoluer en fonction du contexte légal, réglementaire ou technologique et pourra être complétée notamment de nouvelles publications nationales telle que la charte nationale de sécurité l'administrateur du système d'information.

1. CHAMP D'APPLICATION

1.1 LA CHARTE S'APPLIQUE A TOUS

La charte nationale de sécurité du système d'information s'applique à toutes les personnes intervenant à titre professionnel dans les organismes ou accédant au Système d'Information de la branche Famille quel que soit le lieu depuis lequel cet accès s'opère: salariés, personnels temporaires, stagiaires, fonctionnaires détachés, administrateurs du conseil d'administration, etc.

Toute personne habilitée à accéder au Système d'Information est désignée « utilisateur » quel que soit son statut.

La charte nationale de sécurité de l'utilisateur du système d'information de la branche Famille n'a pas vocation à s'appliquer aux prestataires extérieurs et à leurs sous-traitants éventuels. Les obligations à la charge de ces derniers seront déclinées dans un document dédié, à la charge de chaque organisme.

1.2 DISPOSITION PARTICULIERE CONCERNANT LES IRP ET SYNDICATS.

La présente charte ne prend pas en compte les dispositions de la loi n° 2004-391 du 4 mai 2004 relative au dialogue social et de l'article 11 du protocole d'accord du 1er février 2008 sur l'exercice du droit syndical. Ces dispositions définissent le cadre d'accès et d'utilisation des nouvelles

¹ L'organisme se définit comme toute entité composant la branche Famille quelle que soit sa forme juridique et est représenté par le directeur ou ses délégataires.

technologies de l'information et de la communication aux organisations syndicales représentatives dans l'organisme et sont précisées dans un protocole local.

Le protocole est rédigé dans le respect des règles énoncées dans la charte nationale de sécurité du système d'information et du protocole type fourni par l'UCANSS.

A défaut de protocole ou pour les points non traités par ce dernier, la charte nationale de l'utilisateur de sécurité du système d'information s'applique.

2. APPLICATION DE LA CHARTE

La charte nationale de sécurité de l'utilisateur du système d'information est portée à la connaissance de l'ensemble des utilisateurs. Elle est annexée au règlement intérieur des organismes et s'applique à tous les agents. En revanche, elle requiert l'acceptation individuelle de chaque utilisateur non soumis au règlement intérieur, ou bien de tous en l'absence de règlement intérieur.

Les règles contenues dans la charte nationale de sécurité du système d'information constituent le référentiel qui doit être respecté par chacun.

Il appartient donc à chaque utilisateur du système d'information de prendre connaissance et d'appliquer l'ensemble des dispositions de la présente charte.

3. REGLES D'UTILISATION DU SYSTEME D'INFORMATION

3.1 LES CONDITIONS D'UTILISATION DES RESSOURCES

L'organisme est responsable des ressources informatiques qu'il met à la disposition de l'utilisateur pour l'exercice de son activité, les ressources sont donc réservées à un usage professionnel.

Les ressources englobent : les stations de travail, les périphériques, les serveurs, les logiciels, les services, les moyens de communication (messagerie, intranet, Internet, téléphonie fixe et mobile).

L'utilisateur est un acteur de la sécurité du système d'information de la branche Famille, à ce titre il est donc responsable :

- ✓ de l'utilisation des ressources informatiques qui lui sont confiées et celles auxquelles il accède dans son emploi, sa mission, son contrat ou toute forme juridique le liant à l'organisme. Il veillera notamment à respecter les conditions normales d'utilisation afin d'en empêcher toute dégradation ;
- ✓ du bon usage de celles-ci pour garantir la confidentialité, l'intégrité et la disponibilité des données qu'il manipule.

L'utilisation des ressources informatiques est dédiée à l'accomplissement des missions de service public de la branche Famille et doit être licite, rationnelle et loyale.

3.2 LA PROTECTION DES RESSOURCES

La CNAF propose et met en œuvre un ensemble de mesures techniques et organisationnelles propres à garantir la disponibilité, la confidentialité et l'intégrité du système d'information.

L'organisme prend toutes les dispositions nécessaires afin de maîtriser et contrôler de manière fiable l'accès aux bâtiments, l'accès au système d'information et protéger les locaux sensibles contre les risques liés à l'environnement (protection contre le vol par exemple).

A son niveau, chaque utilisateur prend toutes les précautions nécessaires afin de limiter les risques de vol ou d'utilisation frauduleuse des ressources mises à sa disposition.

Par mesure de précaution, les configurations standard de l'architecture technique nationale sont verrouillées et seuls les équipes informatiques et les utilisateurs dûment habilités sont autorisés à introduire dans le système d'information de nouveaux logiciels.

Seuls les équipements conformes à l'architecture technique nationale sont autorisés à se connecter au système d'information de la branche Famille, tout autre matériel doit faire l'objet d'une autorisation de connexion spécifique donnée par écrit (courrier ou courriel).

De ce fait, l'utilisateur s'engage à ne pas effectuer les opérations suivantes :

- ✓ connecter du matériel personnel au système d'information sans disposer des autorisations nécessaires et en aucun cas directement au réseau informatique ;
- ✓ connecter du matériel dont l'origine n'est pas absolument connue et contrôlée ;
- ✓ interrompre le fonctionnement normal des équipements du système d'information ;
- ✓ contourner, modifier ou désactiver les dispositifs techniques de sécurité, en particulier de protection contre les virus, les pare-feux, les traces,...

En cas de besoin d'un nouveau matériel ou logiciel, l'utilisateur effectue une demande selon la procédure définie au sein de l'organisme. Dans tous les cas, il en respecte les consignes d'utilisation.

Dans le cadre de l'application du référentiel national, les organismes sont amenés à contrôler la conformité des logiciels et applications installés sur ses stations et divers supports informatiques, par l'utilisation d'outils de collecte automatisée.

3.3 LES EQUIPEMENTS NOMADES

L'affectation et l'usage des équipements nomades sont soumis à l'autorisation préalable de l'organisme et au respect par l'utilisateur de règles complémentaires relatives au nomadisme contenues dans la procédure de mise à disposition et d'utilisation des matériels nomades et de toute autre directive propre à l'équipement concerné.

Lors de la connexion à distance de ces équipements au système d'information, l'utilisateur s'engage à n'utiliser que les solutions de l'architecture nationale mises à sa disposition par la CNAF et à en respecter les préconisations définies.

Les connexions depuis des réseaux non sécurisés ou non maîtrisés, wifi notamment, ou dans des environnements inconnus sont interdits.

Les risques spécifiques liés à ces équipements, notamment leur utilisation en dehors de l'organisme imposent dans tous les cas à leur utilisateur une vigilance accrue.

3.4 LES SUPPORTS AMOVIBLES

Les supports amovibles (clé usb par exemple) représentent l'un des vecteurs de contamination virale les plus courants. Aussi, la connexion au système d'information d'un support amovible personnel ou d'origine inconnue est interdite.

Néanmoins, l'usage d'un support amovible professionnel pouvant s'avérer nécessaire, certaines dispositions prises au sein de l'organisme sont susceptibles d'autoriser ce type de connexion, sous réserve du respect par l'utilisateur de règles et procédures spécifiques.

L'utilisateur est informé qu'un support amovible connecté au système d'information de la branche Famille est présumé être utilisé à des fins professionnelles, l'organisme est donc légitimement autorisé à accéder aux données qu'il contient dans les limites énoncées au chapitre 3.8.

L'utilisateur veille également à ce qu'aucune information présentant un caractère confidentiel ou contenant des données à caractère personnel ne puisse transiter sans protection sur ce média.

3.5 LA PROTECTION DES DROITS D'ACCES AU SYSTEME D'INFORMATION

Afin de se prémunir d'un usage frauduleux du système d'information, chaque utilisateur possède des identifiants et des mots de passe qui lui sont propres.

Ces codes lui permettent d'accéder de façon individualisée et sécurisée à un ensemble de ressources auxquelles il a été préalablement habilité par l'organisme et qui constituent ses droits d'accès.

Le mot de passe est confidentiel, l'utilisateur en est responsable. En conséquence, les règles suivantes s'imposent :

- ✓ choisir un mot de passe robuste conformément aux consignes de complexité et de renouvellement en vigueur qui lui auront été transmises ou qui lui sont imposées par le système d'information ;
- ✓ ne le communiquer à personne, pas même à son responsable hiérarchique sauf cas évoqué au chapitre 3.9 ;
- ✓ ne pas en conserver d'enregistrement non sécurisé ;
- ✓ ne pas répondre à la sollicitation de mémorisation du mot de passe lorsqu'elle est proposée par une application ;
- ✓ le changer en cas de soupçon sur sa compromission.

Ces codes accès identifient chaque utilisateur individuellement. En conséquence toute opération réalisée au sein du système d'information à partir de son identifiant est présumée avoir été réalisée par l'utilisateur qui le possède.

Aussi, et afin de se protéger contre tout usage malveillant de son poste de travail, celui-ci veillera à verrouiller la session de son poste de travail pour une absence même de courte durée.

De plus, l'utilisateur s'engage :

- ✓ à ne pas utiliser des codes d'accès autres que les siens ;
- ✓ à ne pas accéder, ni tenter d'accéder à des ressources auxquelles il n'a pas été habilité, pour lesquelles il ne dispose pas des droits d'accès.

3.6 LA PROTECTION DES DONNEES ET DOCUMENTS ELECTRONIQUES

Afin d'assurer la confidentialité de l'information de la branche Famille et des données dont il se trouve dépositaire, l'utilisateur s'engage à appliquer les recommandations de sécurité suivantes :

- ✓ conserver en lieu sûr les supports de stockage amovibles ;
- ✓ ne pas laisser de documents confidentiels sur les télécopieurs, imprimantes ou photocopieurs ;
- ✓ ne pas stocker des données confidentielles ou des données à caractère personnel de manière non sécurisée sur les équipements mobiles et les supports de stockage amovibles ;
- ✓ ne pas déposer des données confidentielles de manière non sécurisée sur un service extérieur de stockage ou de partage sans autorisation expresse préalable ;
- ✓ ne pas communiquer d'informations confidentielles susceptibles d'être entendues par une tierce personne non habilitée notamment au téléphone ou dans un lieu public ;
- ✓ ne pas révéler d'informations confidentielles sans s'assurer de la légitimité de l'interlocuteur à disposer de l'information (droit à connaître) ;
- ✓ ne pas laisser de messages comportant des informations confidentielles sur les messageries vocales ;

De plus l'utilisateur s'expose notamment à des poursuites pénales en cas d'utilisation de tout ou partie des informations et des données détenues par la branche Famille, à des fins personnelles ou commerciales.

Chiffrement des données.

L'utilisateur s'engage à n'utiliser, pour la protection des données confidentielles, que les seuls moyens de chiffrement mis à sa disposition et avec l'accord du responsable hiérarchique.

Le respect des règles de la Politique de Sécurité du Système d'Information implique notamment que :

- ✓ le recours au chiffrement ne doit pas perturber la continuité d'activité d'un service. Il appartient à l'utilisateur de garantir, en toute circonstance, l'accès aux données chiffrées aux seuls utilisateurs habilités ;
- ✓ dans le cadre d'échange avec l'extérieur, l'utilisateur veille à chiffrer également au moyen de la clé fournie par l'organisme ou d'un mot de passe respectant les règles de complexité en vigueur.

Sauvegarde.

L'utilisateur doit stocker ses fichiers et ses données dans des espaces définis par l'organisme afin de notamment pouvoir bénéficier d'une sauvegarde régulière s'appuyant sur l'infrastructure nationale.

La sauvegarde des données privées ne relève pas de la responsabilité de l'organisme.

3.7 UTILISATION RESIDUELLE A TITRE PRIVE

Le système d'information est destiné à un usage professionnel dans le cadre des missions de la branche Famille.

Néanmoins les utilisateurs disposent d'un droit résiduel à la vie privée. Ils peuvent, ainsi, utiliser de façon modérée les moyens de communications (téléphonie, messagerie) dans le cadre des nécessités de la vie courante et familiale.

De la même manière, une utilisation résiduelle à titre privé des ressources bureautiques et d'internet est tolérée.

Dans tous les cas, cette utilisation est conditionnée par le respect intégral de la présente charte, de façon à n'affecter ni la sécurité, ni le fonctionnement normal du système d'information, ni la réalisation des missions de l'utilisateur.

Au titre de l'utilisation résiduelle à titre privé, l'utilisateur veille à supprimer, dans la mesure du possible, toute référence (logo, titre,...) identifiant l'organisme et d'une façon générale la branche Famille.

3.8 PROTECTION DES DONNEES PRIVEES DE L'UTILISATEUR

D'une manière générale, toutes les données présentes sur le système d'information sont présumées professionnelles et sont accessibles à tout moment et de quelque façon que ce soit par l'organisme, même hors la présence de l'utilisateur.

Cependant la loi garantit à chacun le respect de sa vie privée à travers l'article 9 du code civil et le secret des correspondances privées. Ainsi les fichiers ou messages dont le caractère privé est explicitement exprimé sont considérés comme relevant de la sphère privée et ne peuvent pas, en conséquence, être consultés librement par l'organisme, sauf en cas de risque particulier (immédiat et important) pour l'organisme.

Dans la mesure où toute correspondance ou donnée est présumée professionnelle, l'utilisateur veille à permettre une identification explicite et précise du caractère privé de celles-ci par l'usage des termes « privé » ou « prive » au début du nom du répertoire de stockage, du nom du fichier, de l'objet du message ou du nom du dossier de stockage du message. La perspective d'une réponse impose d'informer le tiers destinataire du message de cet usage. Ces messages peuvent être archivés dans un dossier spécifique de la boîte de réception de l'utilisateur.

Tout courrier électronique envoyé ou reçu à partir de l'adresse électronique professionnelle ne portant pas la mention « privé » ou « prive » dans la zone « objet du message », ou enregistré ailleurs que dans le dossier « privé » ou « prive » est considéré comme professionnel.

Lorsque le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, ...), le message à caractère personnel doit débuter par le terme « privé » ou « prive ».

Les documents ainsi que le répertoire informatique utilisé pour stocker des documents non-professionnels doivent être identifiés par le terme « privé » ou « prive ».

A l'inverse les exemples suivants ne confèrent pas un caractère privé aux données qu'ils contiennent :

- ✓ les initiales de l'utilisateur ou bien son prénom ou son nom ;
- ✓ le répertoire nommé « Mes documents » ;
- ✓ le label « données privées » d'un disque ne permet pas à un salarié d'utiliser celui-ci à des fins purement privées et d'interdire ainsi l'accès à l'intégralité des fichiers et dossiers qu'il contient à l'organisme ;
- ✓ la dénomination « Espace individuel » ou utilisant le nom de l'utilisateur d'une ressource réseau, mise à disposition par l'organisme ;
- ✓ la dénomination « Mes favoris » ou « Marques-pages » du navigateur internet.

Le caractère privé du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que :

- ✓ l'organisme puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'organisme en termes notamment de sécurité, de continuité de service ou un risque grave de voir sa responsabilité engagée ;
- ✓ en cas de détection ou de suspicion de la présence d'un code malveillant, à la mise en quarantaine ou le cas échéant la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;
- ✓ un administrateur ou toute personne habilitée, accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des moyens informatiques et de communication de l'organisme, ce notamment dans le cadre d'opération de maintenance ;
- ✓ l'organisme, puisse dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisé par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Commission nationale de l'informatique et des libertés, Cour des comptes, etc.).

Dans les cas listés ci-dessus, l'utilisateur concerné est informé préalablement à tout accès aux données ou contenus identifiés comme privés. Si cette information préalable est impossible, elle

est remplacée par une information a posteriori. Les personnes habilitées à ces opérations veillent à respecter la confidentialité de ces informations.

Par ailleurs, le caractère privé du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que ces éléments fassent l'objet de conservation technique dans le cadre des procédures de sauvegarde ou de plans de continuité de reprise d'activité mises en œuvre au sein de l'organisme.

S'il appartient à l'utilisateur d'identifier les fichiers et messages qui sont privés, il est précisé que l'utilisateur ne peut pas identifier ou requalifier comme privés des fichiers et des messages à caractère professionnel.

3.9 LA GESTION DES ABSENCES ET DES DEPARTS

En cas d'absence de longue durée.

Au-delà d'un délai déterminé par l'organisme, les droits d'accès de l'utilisateur sont susceptibles d'être suspendus afin de le protéger d'une utilisation malveillante de ceux-ci.

En cas de nécessité, particulièrement dans le cadre de la continuité d'activité, l'organisme peut accéder aux données de l'utilisateur pendant son absence, conformément aux dispositions du chapitre précédent, et procéder à toute adaptation nécessaire de ses paramètres techniques (par exemple notifier l'absence de l'utilisateur dans sa messagerie).

En cas de départ de l'organisme (retraite, démission,...).

Avant son départ de l'organisme, l'utilisateur procède à la suppression de l'ensemble de ses données privées et uniquement celles-ci et veille à ce que toutes les données professionnelles, liées à son activité, demeurent accessibles par l'organisme.

A son départ de l'organisme, l'utilisateur restitue l'ensemble des ressources qui lui ont été attribuées, il perd ses droits d'accès au système d'information. Les données encore identifiées comme privées seront alors supprimées.

3.10 LE DEVOIR DE SIGNALEMENT ET LE RESPECT DES CONSIGNES

Le respect des règles de sécurité et de déontologie exposées dans la présente charte concourt à la prévention contre la malveillance et la fraude dans le cadre de l'utilisation du système d'information.

De ce fait, tout soupçon ou constat d'acte malveillant ou tout autre événement susceptible de présenter un risque pour la sécurité du système d'information (vol, accès non autorisé, usurpation d'identité, corruption de données, ...) doit être immédiatement signalé à son responsable hiérarchique, au MSSSI ou au service informatique.

De la même manière, l'utilisateur s'engage à appliquer toutes les consignes qui lui sont transmises par le directeur ou ses délégataires, le service informatique, les services de support dûment habilités ou le MSSI à la suite d'un incident de sécurité. Par exemple, il pourra être demandé à l'utilisateur de déconnecter son poste du réseau en cas d'infection virale.

4. REGLES D'UTILISATION DES COMMUNICATIONS ELECTRONIQUES

4.1 LA MESSAGERIE ELECTRONIQUE

L'organisme met à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des courriels. L'aspect nominatif de l'adresse électronique ne retire en rien le caractère professionnel de la messagerie.

Par conséquent tout message est réputé professionnel sauf s'il comporte dans son objet une mention explicite indiquant son caractère privé ou bien s'il est stocké dans un espace identifié comme privé (Cf chapitre 3.8).

Cependant conformément au chapitre 3.7 l'utilisateur dispose du droit résiduel à la vie privée, aussi l'utilisation de la boîte à lettres professionnelle nominative à titre privé est autorisée à condition qu'elle n'affecte pas le trafic normal des messages professionnels.

D'une façon générale, tout courriel peut engager la responsabilité de son émetteur et est susceptible de constituer une preuve en cas de contentieux. Aussi, l'utilisateur portera une attention particulière à la nature et aux contenus des courriels qu'il transmet. En aucun cas, il n'engagera l'organisme s'il n'est pas habilité à le faire.

Les utilisateurs veilleront par ailleurs à respecter les principes d'usage suivants :

- ✓ le transfert systématique des messages professionnels vers une boîte aux lettres personnelle extérieure (par exemple xxxxx@hotmail.com) est interdit ;
- ✓ le transfert de données confidentielles vers un système de messagerie externe doit être effectué de façon sécurisée ;
- ✓ les messages doivent respecter la correction normalement attendue dans tout type d'échange et notamment le respect de la dignité de la personne humaine. Ainsi la diffusion ou rediffusion, tant en interne que vers l'extérieur, de messages et/ou images à caractère sexuel, raciste ou discriminatoire est interdit ;
- ✓ les dispositifs internes de sécurité ne permettent pas toujours de filtrer les messages non sollicités qu'ils soient de type publicitaires, canulars, chaînes, hameçonnage... Ces messages ne doivent pas être propagés mais impérativement supprimés dès leur réception.
- ✓ les messages revêtant un caractère malveillant ou frauduleux doivent par ailleurs faire l'objet d'un signalement immédiat tel que mentionné au chapitre 3.10 ;
- ✓ les pièces jointes et les liens internet, contenus dans les messages, doivent faire l'objet de toutes les précautions et ne pas être ouverts dès lors que l'émetteur, l'objet ou le contenu sont inconnus, suspects ou sans rapport avec l'activité ;
- ✓ les adresses de messagerie doivent être communiquées avec une grande prudence afin d'empêcher de recevoir davantage de courriels non désirés et malicieux.

Les règles énoncées dans ce chapitre s'appliquent aussi aux boîtes à lettres fonctionnelles.

4.2 L'INTERNET ET L'INTRANET

L'internet.

L'accès à internet est soumis à autorisation pour l'ensemble des utilisateurs.

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle. Toutefois une utilisation résiduelle à titre privé est tolérée, conformément au chapitre 3.7, à condition qu'elle n'affecte pas le trafic normal des flux internet professionnels. Cette tolérance n'empêche pas l'organisme de considérer comme abusifs, notamment :

- ✓ l'accès à des sites de jeux, d'enchères et de paris ;
- ✓ la fréquentation excessive de sites communautaires, de forums de discussion et blogs sans rapport avec l'activité professionnelle ;
- ✓ la création ou la gestion d'un site Internet sans rapport avec l'activité professionnelle ;
- ✓ la promotion ou la vente de tout bien ou service dans un but commercial.

L'utilisateur ne doit en aucune circonstance charger, stocker, publier, diffuser ou distribuer, ni inciter des tiers à lui adresser, des documents, informations, images, vidéos, pages Web, messages, etc. :

- ✓ faisant l'apologie de crimes contre l'humanité, incitant à la violence ou à la commission d'actes de terrorisme ou à leur apologie, incitant à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap, à caractère pédopornographique ;
- ✓ à caractère injurieux, diffamatoire, dénigrant, attentatoire à la vie privée, raciste, xénophobe, révisionniste et terroriste ;
- ✓ susceptibles de porter atteinte au respect de la dignité de la personne humaine ;
- ✓ susceptibles de porter atteinte à la protection des mineurs ;
- ✓ portant atteinte au respect des droits d'auteur et des droits de propriété intellectuelle ;
- ✓ portant atteinte au secret professionnel ;
- ✓ portant atteinte à l'intégrité, à la conservation des données et à l'image de marque interne et externe de l'organisme ou de la branche Famille.

L'accès à internet fait l'objet de contrôles et de filtrages systématiques. Ainsi les tentatives d'accès à des sites présentant un niveau de confiance faible, suspects ou réputés dangereux sont bloquées. Dans certains cas, un message d'alerte avertit l'utilisateur de l'éventuelle dangerosité d'un site, la poursuite de la navigation engage alors sa responsabilité. L'utilisateur quittera immédiatement un site non classifié auquel il pourrait avoir librement accès si il présente en tout état de cause un caractère suspect.

La CNAF se réserve le droit de limiter le téléchargement de fichiers volumineux ou présentant un risque pour la sécurité du système d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information, codes malveillants, programmes espions, etc...).

Afin de contrôler l'application de ces règles, d'assurer la protection du patrimoine informationnel et la détection de flux sortants anormaux, la CNAF met en place un dispositif d'analyse automatique des flux internet, chiffrés ou non, y compris en utilisant le déchiffrement pour les flux https.

Un usage abusif, non conforme ou illicite, détecté par l'employeur, expose l'utilisateur à des poursuites disciplinaires, pénales ou civiles.

La publication sur les sites internet et intranet.

Toute publication de pages d'information sur les sites internet ou intranet de l'organisme, de la branche Famille, doit être validée par le directeur de publication du site.

Aucune publication de pages d'information à caractère privé n'est autorisée.

Les médias sociaux publics.

Les contributions des utilisateurs que ce soit à titre professionnel ou à titre privé sur les médias sociaux constituent un mode d'échange et de partage généralisé. Néanmoins, le caractère communautaire de ces médias et leur absence de confidentialité conduisent à faire preuve de la plus grande vigilance.

Chacun a la liberté d'évoquer son appartenance à la branche Famille, de s'exprimer sur l'organisation et les conditions d'exercice de son travail dans le respect de ses obligations de loyauté, de réserve, de discrétion et de correction vis-vis de l'organisme.

Mais, dès lors que ces contributions sont en lien avec les activités de la branche Famille, son image, ses allocataires ou ses représentants, elles sont considérées relever de la sphère professionnelle et impliquent pour l'utilisateur de :

- ✓ respecter le secret professionnel et la confidentialité des données particulièrement en ce qui concerne les données à caractère personnel ;
- ✓ respecter la dignité de la personne humaine en proscrivant les insultes, le dénigrement, la diffamation même dans un mode « privé » ;
- ✓ respecter l'ensemble des règles énoncées dans cette charte ainsi que les conditions d'utilisation du média social (CGU);
- ✓ ne parler au nom de l'organisme ou n'en utiliser le logo qu'à moins d'y être dûment habilité.

Dans la mesure où Il est difficile d'identifier la limite entre vie personnelle et vie professionnelle sur les médias sociaux, il existe en effet un risque que les propos tenus à titre privé par un utilisateur soient associés à l'organisme ou la branche Famille, l'utilisateur devra également veiller à :

- ✓ ne pas utiliser son adresse professionnelle à titre privé sur les médias sociaux ;
- ✓ indiquer clairement que les propos sont tenus en nom propre et qu'ils ne reflètent pas la position de l'organisme.

Les médias sociaux internes

L'utilisation des médias sociaux internes est soumise aux mêmes règles d'usage et de déontologie que celles décrites dans la présente charte, et en particulier la confidentialité des informations et le respect du secret professionnel.

5. UTILISATEURS A DROITS SPECIFIQUES

Les règles d'utilisation de la présente charte s'appliquent à tous. Cependant, du fait de l'exercice de leurs missions et de leurs responsabilités, certains utilisateurs ont des droits spécifiques quant à la gestion d'applications ou la gestion des habilitations. Ils sont soumis à des règles particulières et complémentaires.

5.1 ROLE ET RESPONSABILITE DU GESTIONNAIRE D'APPLICATION

Le gestionnaire d'application a pour rôle d'assurer le bon fonctionnement d'une ou de plusieurs applications métiers et dispose pour cela de droits spécifiques.

Ces droits et son statut lui permettent de saisir son supérieur hiérarchique afin de l'alerter sur des manquements résultant du mauvais usage de(s) application(s) dont il a la charge ;

En revanche il doit respecter les règles suivantes :

- ✓ ne pas entraver ou détourner, par un paramétrage malveillant, le fonctionnement normal de(s) application(s), l'action des utilisateurs ainsi que le service rendu aux allocataires et aux clients internes ;
- ✓ appliquer les règles de constitution des mots de passe afin de concevoir des mots de passe robustes ;
- ✓ porter une attention particulière aux identifiants et mots de passe des comptes dont il dispose.

Le gestionnaire d'habilitation a pour rôle d'assurer la gestion des droits d'accès d'une ou de plusieurs applications métiers et dispose pour cela de droits spécifiques.

Ces droits et son statut lui permettent :

- ✓ d'interdire temporairement ou définitivement l'accès aux applications à un utilisateur qui ne respecte pas la présente charte, les directives d'utilisation nationales ou les conventions applicables le cas échéant ;
- ✓ de saisir son supérieur hiérarchique afin de l'alerter sur des manquements résultant de l'utilisation abusive de l'application.

En revanche il doit respecter les règles suivantes :

- ✓ appliquer les règles de constitution des mots de passe afin de concevoir des mots de passe robustes ;
- ✓ porter une attention particulière aux identifiants et mots de passe des comptes dont il dispose ;
- ✓ gérer les droits d'accès dans le respect des procédures d'attribution, de vérification et de communication en vigueur et le respect des conventions régissant la mise à disposition et l'utilisation des applications.

6. RÔLE ET RESPONSABILITÉ DE L'ADMINISTRATEUR DU SI

L'administrateur a pour rôle d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Il est conduit par sa fonction à accéder à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à Internet, fichiers de journalisation, etc.), y compris toutes celles qui sont enregistrées sur le disque dur du poste de travail.

Dans le cadre de ces missions et uniquement celles-ci, il peut être amené à :

- ✓ prendre le contrôle du poste de travail d'un utilisateur (même à distance) en ayant pris soin de demander l'accord exprès à ce dernier, sauf en cas de risque potentiel sur la sécurité du SI ;
- ✓ mettre en place des outils de surveillance, de mesure ou d'administration ;
- ✓ exploiter l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à Internet, fichiers de traces ou journaux,...) y compris celles enregistrées sur le poste de travail.

L'administrateur est susceptible d'accéder à des informations, dont le contenu privé ou confidentiel, est couvert par le secret des correspondances privées ou relève de la vie privée.

De ce fait, il est tenu au secret professionnel et aux obligations de confidentialité et de discrétion.

Les droits et devoirs de l'administrateur sont encadrés par la « charte de l'administrateur ».

7. TRAÇABILITÉ

Aujourd'hui tout accès et utilisation du système d'information génère automatiquement des traces collectées dans des journaux. Les finalités couvertes par cette collecte visent notamment à garantir le bon fonctionnement et l'utilisation normale des ressources du système d'information ainsi que le contrôle du bon usage du SI par les utilisateurs.

L'utilisateur est informé que toute connexion au système d'information de la branche Famille l'identifie et qu'elle est une acceptation de l'enregistrement automatique des traces de son activité.

Même si les technologies ou les configurations le permettent, l'utilisateur se garde strictement d'effacer toute trace liée à son activité.

Les données collectées sont susceptibles de présenter un caractère privé, aussi la mise en œuvre de tout dispositif, automatique ou non, traitant de ces données, doit respecter les formalités décrites au chapitre 8.3.

Il convient également que les dispositifs mis en œuvre soient proportionnels aux objectifs poursuivis et que les utilisateurs soient informés de leur mise en place.

7.1 INTERNET

La sécurisation des accès internet est assurée par un système de filtrage qui bloque, alerte et fournit des traces et des statistiques concernant les flux internet des utilisateurs.

Ce dispositif génère des traces par poste utilisateur, les données telles que : Date et heure de connexion, l'adresse IP, identification des sites visités, catégorie des sites visités,... sont enregistrées.

Ce dispositif est utilisé, notamment, pour fournir des statistiques collectives par organisme et pour identifier des cas d'utilisation inappropriée de la ressource internet. Dans ce dernier cas il est nécessaire d'aller au-delà et de disposer d'informations identifiantes qui soient le reflet de l'usage d'internet pour chaque utilisateur de la branche Famille.

En outre, certaines traces des connexions de navigation utilisateurs sont enregistrées automatiquement par les navigateurs sur le poste de travail. Le cas échéant, l'organisme se réserve le droit d'investiguer ces données sous réserve du respect des principes décrits à la section 3.8 du présent document.

7.2 MESSAGERIE ELECTRONIQUE

Les traces liés aux échanges à travers la messagerie électronique nationale sont conservées et sont utilisées, notamment, à des fins de maintien en condition opérationnelle : optimisation des performances, encombrement du réseau, mais aussi de sécurité.

Les données telles que, notamment, les date, heure et taille, désignation de l'expéditeur et du destinataire et objet du message sont enregistrées.

L'accès, par l'organisme, au contenu des messages d'un utilisateur à des fins de contrôle et d'investigation est exceptionnel et doit être effectué dans le respect des principes décrits à la section 3.8 du présent document.

7.3 APPLICATIONS ET RESEAUX INTERNES

Les journaux d'évènements permettent d'identifier et d'enregistrer les connexions, les tentatives de connexion infructueuses et les actions effectuées sur différentes applications, bases de données et domaines du réseau de la branche Famille. Les données telles que : date et heure de connexion, identifiant, échec de connexion, action effectuée, tentative de violation de droit d'accès,...sont enregistrées.

Ces fichiers de journalisation sont conservés selon les besoins et permettent notamment de détecter des comportements anormaux ou des cas de fraude.

Les journaux du système national de téléphonie permettent d'enregistrer des données telles que : numéro de l'appelant et une partie du numéro de l'appelé, durée de communication...sont enregistrées.

Le même type de données est enregistré dans le cadre du contrôle de la téléphonie mobile professionnelle. Le format correspond aux informations classiques d'une facture détaillée opérateur.

Le contrôle de ces données permet, notamment, la maîtrise et le suivi des coûts d'exploitation.

8. RESPECT DES REGLEMENTATIONS

8.1 LE RESPECT DE LA LOI

Chaque utilisateur se garde strictement de faire toute utilisation des ressources (informations ou ressources informatiques) mises à sa disposition qui violerait les législations et les réglementations en vigueur.

De plus chaque utilisateur se garde de commettre des infractions de nature à engager sa responsabilité et/ou celle de l'organisme, notamment en portant atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, par exemple par l'intermédiaire de messages, textes ou images provocants.

8.2 LE RESPECT DE LA PROPRIETE INTELLECTUELLE

L'utilisation des systèmes d'information implique le respect des droits de propriété intellectuelle de l'organisme, de ses partenaires et, de tout tiers titulaire de tels droits.

L'accès internet ne doit pas être utilisé par l'utilisateur à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans autorisation préalable et écrite de sa hiérarchie.

Sans que cette liste soit exhaustive, chaque utilisateur autorisé s'engage à :

- ✓ utiliser les logiciels et applications dans les conditions de licence souscrite par l'organisme ;
- ✓ ne pas effectuer de copie illicite de logiciel ou d'applications et, a fortiori, de tenter d'installer des logiciels ou applications pour lesquels l'organisme ne posséderait pas un droit d'usage ;
- ✓ ne pas reproduire, copier, utiliser, remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'organisme ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ✓ ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles.

L'utilisateur est informé que la contrefaçon est un délit passible de sanctions civiles et pénales. A cet effet, l'organisme pourra mettre en œuvre les mesures de contrôle appropriées au respect de cette obligation.

8.3 LE RESPECT DE LA LOI INFORMATIQUE ET LIBERTES

En fonction de la législation en vigueur, le responsable de traitement (c'est-à-dire la personne qui détermine les finalités, les risques et les moyens à mettre en œuvre) procède au formalisme Informatique et Libertés préalable à la mise en œuvre de tout traitement comportant des données à caractère personnel (c'est-à-dire des informations qui permettent l'identification, directe ou indirecte ou par recoupement, des personnes).

Le responsable de traitement a la charge et l'obligation d'informer les personnes :

- ✓ de la nature des données traitées,
- ✓ de la finalité et de la durée du traitement,
- ✓ ainsi que de leur droit d'accès et des modalités d'exercice de ce droit. Sous réserve des restrictions légales, l'utilisateur possède aussi un droit de rectification et de suppression des données à caractère personnel le concernant.

Dans le cadre de traitements nationaux et afin de simplifier les procédures internes ou externes notamment vis-à-vis de la CNIL (Commission Nationale de l'Informatique et des Libertés), la CNAF a nommé un Correspondant informatique et libertés (Cil).

9. CONTROLE DE L'APPLICATION DE LA CHARTE ET SANCTIONS

9.1 LE CONTROLE DE L'APPLICATION DE LA CHARTE.

Pour des nécessités de sécurité, les organismes constituant la branche Famille doivent procéder périodiquement, par les moyens les plus appropriés, à des contrôles de la bonne application de la présente charte, dans le respect de la législation et de la réglementation applicables, notamment au regard du droit du travail et de la loi Informatique et Libertés. Ces contrôles portent sur tout ou partie de la présente charte.

Ces contrôles automatisés ou non peuvent utiliser les traces mentionnées au chapitre 7.

9.2 LIMITATION DES USAGES ET SANCTIONS

En cas de non-respect des règles définies dans la présente charte, le directeur de l'organisme pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des utilisateurs, limiter les usages par des mesures conservatoires.

Le non-respect de cette charte engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les faits lui sont personnellement imputables. L'utilisateur s'expose, le cas échéant, aux sanctions prévues par la convention collective, le règlement intérieur, le code du travail ainsi qu'à des poursuites civiles ou pénales.