Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DES SOLIDARITES ET DE LA SANTE

MINISTERE DU TRAVAIL

MINISTERE DE L'EDUCATION NATIONALE

MINISTERE DES SPORTS

Charte relative à la protection de l'information et à la sécurité numérique des ministères chargés des affaires sociales

Version novembre 2017

La charte relative à la protection de l'information et à la sécurité numérique rappelle les droits et les devoirs des utilisateurs, prestataires, administrateurs et exploitants de systèmes d'information numériques des ministères chargés des affaires sociales (MCAS), tels qu'ils ressortent des textes et principes applicables, et précise les modalités de mise en œuvre de ces textes et principes dans le champ des MCAS, responsabilité qui incombe au chef de service. Elle vise en particulier à assurer la protection du secret professionnel, du secret des correspondances et des informations traitées dans le cadre de l'activité gouvernementale, ainsi que la protection de la vie privée et des données personnelles.

La charte permet d'assurer l'équilibre entre les impératifs des MCAS et ceux des utilisateurs de leurs systèmes d'information. D'un côté, les utilisateurs s'engagent à faire un usage responsable des ressources mises à leur disposition. De l'autre, les MCAS garantissent la protection des informations et la sécurité de ses systèmes numériques, ses applications et ses réseaux et s'engagent à respecter la vie privée des utilisateurs.

Cette charte a été présentée aux instances consultatives des MCAS. Elle s'applique dès sa publication à **tout utilisateur des systèmes numériques des MCAS** :

- sans distinction de statut, de grade, de fonction ni de rôle ;
- quelle que soit :
    - son entité de rattachement et le statut de cette dernière, sa localisation géographique ;
    - sa situation de travail : dans les locaux des MCAS, en déplacement ou en télétravail.
- Les prestataires des MCAS doivent respecter la présente charte, et cette exigence doit être expressément prévue dans leurs contrats.

Elle est disponible sur l'intranet (PACO) des ministères sociaux.

Cette charte pourra évoluer en fonction du contexte législatif et réglementaire, ainsi que des modifications apportées à la politique de sécurité des systèmes d'information de l'Etat et à la politique de sécurité des systèmes d'information des MCAS.

Le secrétaire général des ministères sociaux
Haut fonctionnaire de défense et de sécurité

Le Secrétaire général

Pierre Ricordeau

SOMMAIRE

1 POURQUOI UNE CHARTE DE PROTECTION DE L'INFORMATION ET A LA SECURITE NUMERIQUE ? 4

2 PROTECTION DE L'INFORMATION 5

3 SECURITE DES SYSTEMES D'INFORMATION 7

5 CONTROLES 14

6 GLOSSAIRE 15

7 TEXTES DE REFERENCES 16

1 POURQUOI UNE CHARTE DE PROTECTION DE L'INFORMATION ET A LA SECURITE NUMERIQUE ?

Les informations et l'ensemble des systèmes numériques qui les supportent constituent une ressource stratégique indispensable à la conduite des activités des MCAS dans le cadre de l'action gouvernementale. Il est donc dans l'intérêt de chacun de protéger notre patrimoine informationnel.
En conséquence, chaque utilisateur s'engage à respecter les procédures décrites dans le présent document et à se conformer à ses exigences.

La charte précise les droits et les devoirs des utilisateurs :

- leurs **droits,** particulièrement le respect de la vie privée (art. 9 du code civil), qui trouve son expression notamment lors de l'usage du matériel mis à disposition par les MCAS et de l'accès à leurs réseaux ;
- leurs **devoirs**, notamment leur responsabilité en matière de protection de l'information et leur devoir d'alerte lors de la détection d'un problème de sécurité.

La charte relative à la protection de l'information et à la sécurité numérique définit **les règles que tout utilisateur doit respecter** afin de garantir :

- la confidentialité, l'intégrité et la disponibilité de l'information et des systèmes d'information ;
- la préservation de l'image des MCAS ;
- la protection de la vie privée et du secret professionnel.

Elle doit également permettre une utilisation fiable et responsable des systèmes d'information partagés par l'ensemble des utilisateurs.

La connaissance et la mise en œuvre par tous les utilisateurs des MCAS **des principes fondamentaux de bon usage et de sécurité** des systèmes d'information permettent d'en assurer le fonctionnement et la performance en tous temps et pour tous, de maintenir un niveau de sécurité homogène au sein de l'organisation et d'éviter la plupart des situations qui pourraient mener à des incidents dans ce domaine.

La présente charte s'applique à tous les composants des systèmes d'information mis à la disposition des utilisateurs par les MCAS (supports papier, matériels fixes ou mobiles, logiciels, systèmes de communication tels que la messagerie, le téléphone ou Internet), ainsi qu'aux informations stockées ou véhiculées par ces composants (documents papier et numériques, messages électroniques, enregistrements audio, échanges verbaux etc.).

2 PROTECTION DE L'INFORMATION

La protection de l'information ne se limite pas aux systèmes informatiques, ni à l'information sous sa forme numérique, ou électronique mais s'applique à l'information sous toutes ses formes, qu'il s'agisse d'une communication orale, d'un document papier, ou encore d'une donnée numérique. L'objectif poursuivi en toutes circonstances est le respect du besoin d'en connaitre (nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise). Le détenteur d'une information ne doit la communiquer que si cela fait sens pour accomplir les tâches qui lui sont confiées. Au sein de chaque service, l'autorité hiérarchique responsable définit les règles de catégorisation des informations. Il appartient à l'émetteur d'information de la catégoriser.

Principes

L'utilisateur assure la protection des informations qu'il manipule selon leur niveau de sensibilité :

Les informations courantes, traitées dans le cadre professionnel, internes à l'administration, sont sujettes aux principes élémentaires de discrétion professionnelle qui permettent d'en assurer la protection.

Les informations considérées comme sensibles, dont la divulgation ou l'altération peuvent avoir des conséquences dommageables, importantes ou inacceptables pour l'administration, les agents, les citoyens ou les organisations. Elles sont protégées par des dispositions telles que le secret professionnel et, le cas échéant, différents textes, obligations réglementaires ou contractuelles (ex : protection des données personnelles).

Les informations classifiées relevant du secret de la défense nationale[1], qui doivent être traitées selon les modalités définies par l'instruction générale interministérielle n° 1300.

Ces informations ne sont diffusées qu'aux seuls agents "habilités", dans le cadre du secret de la défense nationale. Elles ne peuvent être manipulées et communiquées que sur des systèmes d'information spécifiques. Les documents ou supports font l'objet d'un marquage spécifique.

Modalités de traitement des informations considérées comme sensibles

Marquage des documents

Les documents contenant des informations sensibles doivent comporter une mention précisant leur niveau de diffusion, en considération de la **gravité des conséquences de leur divulgation** :

- **« Interne »**, pour les documents à la seule destination des agents des MCAS ou d'une entité particulière ;
- **« Limité »**, pour les documents à destination de personnes clairement identifiées.

Ce marquage peut être complété par une **mention de confidentialité** telle que :
« sensible », «confidentiel», voire « diffusion restreinte »
sur les documents ainsi que dans les courriers ou courriels qui les accompagnent.

La **Diffusion restreinte**[2] est une mention de protection impliquant un traitement particulier :

- Les informations sont nécessairement **stockées et transmises de manière chiffrée**[3] lorsqu'elles quittent le périmètre des MCAS (support de stockage amovible, ordinateur portable, smartphone ; etc.) ;
- les impressions sont réalisées sous surveillance.

[1] Pour toute question relative aux informations classifiées de défense, prendre attache auprès du service du haut fonctionnaire de défense et de sécurité (hfds@sg.social.gouv.fr), ou consulter l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale.

[2] Données « Diffusion restreinte » au sens de l'IGI 1300 (Cette mention de protection est traitée à l'identique au niveau interministériel).

[3] Un dispositif de chiffrement spécifique pour les données « diffusion restreinte » est mis à disposition par la DSI ou les services informatiques (offre de service sur PACO).

Transmission des documents	**Les documents** sont envoyés sous enveloppe et en cas de nécessité sous "double enveloppe". **Les courriels sont chiffrés**, avec envoi du mot de passe de déchiffrement par un autre canal (SMS, téléphone). **Les documents numériques** communiqués par support de stockage amovible (clé USB, disque dur externe, etc.) sont chiffrés pour réduire le risque en cas de perte.
Conservation des documents	**Les documents papier** sont conservés dans des armoires fermées par une clé ou une combinaison. **Les documents numériques** sont stockés sur les répertoires réseau individuels ou sur des répertoires partagés spécifiques, **dont les droits d'accès sont maîtrisés**. Ces droits doivent faire l'objet de revues régulières. Les documents les plus sensibles doivent être chiffrés pour être stockés sur les répertoires individuels ou sur des répertoires partagés spécifiques ou idéalement stockés dans des espaces **chiffrés** (dans ce cas le chiffrement du document n'est pas nécessaire).
Impression des documents	Les documents imprimés doivent être **récupérés sans délai** à l'imprimante. Les impressions peuvent être protégées par un code à saisir sur les imprimantes (cf. procédure DSI sur PACO).
Destruction des documents	**Les documents papier** qui n'ont plus d'utilité doivent être **systématiquement détruits dans des destructeurs de documents.** **Les documents numériques** présents sur les postes de travail doivent être supprimés définitivement par mise à la corbeille puis **vidage de la corbeille**. **Les supports de stockage** tels que les clés USB ou CD-ROM doivent faire l'objet **d'un reformatage ou d'une destruction physique**.
Principes de précaution	**Dans les lieux publics** L'utilisateur reste vigilant quant au risque de divulgation d'informations sensibles dans le cadre de conversations, réunions ou consultations d'information, ceci notamment dans les lieux publics (transports en commun, gares, aéroports...). **Au téléphone** L'utilisateur reste vigilant dans l'utilisation des réseaux téléphoniques publics fixes ou mobiles, la confidentialité des échanges n'étant pas garantie sur ces réseaux. Il n'utilise pas de renvoi automatique de son numéro de téléphone interne au MCAS vers un numéro privé de téléphone fixe ou mobile. **Internet, accès Webmail** En cas d'utilisation d'un équipement non maitrisé par l'administration (poste personnel ou en libre-service Hôtel, cyber café...), l'utilisateur ne doit jamais utiliser la fonctionnalité d'enregistrer ses moyens d'accès au système d'information (login/ mot de passe) proposé par les navigateurs. S'il est amené à travailler sur des pièces jointes il doit s'assurer qu'elles ne sont pas enregistrées sur le poste hôte ou les supprimer complètement le cas échéant (Purge de l'historique du navigateur, suppression des téléchargements, suppression des fichiers, vidage de la corbeille).

3 SECURITE DES SYSTEMES D'INFORMATION

PRINCIPES

Un usage responsable des systèmes d'information

L'accès aux systèmes d'information des MCAS (poste de travail, serveurs, applications, messagerie, Internet, téléphone...) **est fourni à l'utilisateur pour l'exercice de son activité professionnelle.**

L'utilisateur stocke ses documents de travail dans un dossier placé sur le réseau des MCAS :

- soit sur un espace individuel auquel il est seul à accéder, en dehors des équipes de la DSI. Le contenu de cet espace sera détruit à son départ ;
- soit sur un ou plusieurs espaces partagés, accessibles par les agents de son entité ou d'autres entités.

Les systèmes d'information des MCAS ont une vocation professionnelle

Un usage personnel de ces ressources peut être toléré à titre occasionnel, à condition qu'il :

- reste de courte durée ;
- n'affecte pas l'usage professionnel ;
- ne porte pas atteinte à la confidentialité des informations ;
- ne remette pas en cause l'intérêt et la réputation des MCAS ;
- n'enfreigne pas la législation en vigueur.

Afin de concrétiser le droit au respect de sa vie privée, l'utilisateur mentionne explicitement le caractère privé de ses documents personnels, en les consignant, par exemple, dans un dossier nommé "personnel". **A défaut, tout document est présumé professionnel.**

En revanche, l'exercice consistant à placer de façon disproportionnée un très grand nombre de données, normalement professionnelles, dans un dossier intitulé « personnel », afin de contourner la règle, permettrait d'accéder à ce dossier est interdit. Cela en cas d'enquête à la suite d'un préjudice ne saurait conférer un caractère personnel à l'intégralité des données qu'il contient.

Respect des lois et réglementations

Sauf autorisation individuelle, dans le cadre d'une mission précisément définie, validée par sa hiérarchie, l'utilisateur ne manipule jamais d'information **contraire aux bonnes mœurs et à l'ordre public** (accès à des sites Internet, stockage ou diffusion de fichiers, envoi de messages...), notamment :

- des informations à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste ou pédophile, ou pouvant constituer une incitation à la haine, la violence ou la débauche ;
- des copies illicites d'éléments (logiciels, images, textes, musiques...) protégés par les lois sur la propriété intellectuelle ou la protection de la vie privée.

Rôle d'alerte en cas d'incident

L'utilisateur **contribue à son niveau à la sécurité des systèmes d'information.**

A ce titre, il signale immédiatement à son support informatique de proximité ou à sa hiérarchie tout dysfonctionnement ou tout événement lui apparaissant anormal.

Le cas échéant, il met en application les règles et recommandations établies par ces acteurs afin de résoudre ces dysfonctionnements.

PROTECTION DES EQUIPEMENTS

L'utilisation d'équipements autorisés...

Seuls les équipements (ordinateur, smartphones, équipements spécialisés, etc.) agréés techniquement et fournis par l'administration peuvent être connectés, de façon directe ou indirecte, au réseau des MCAS[4].

L'utilisation de supports de stockage personnels (clé USB, disquette, CDROM...) ou de moyens de connexion (l'accès Webmail à partir de matériels personnels) peut être tolérée à des fins d'échanges ponctuels, à condition de respecter les précautions qui s'imposent pour garantir la confidentialité et la sécurité des échanges (chiffrement des documents obligatoire et destruction de ces derniers à la fin de l'usage – Cf. principes de précaution)

[4] La connexion au réseau des MCAS de matériels personnels ou apportés par des visiteurs (ordinateur, assistant personnel) qui, par définition, ne mettent pas en place les mécanismes de protection établis par les MCAS, présente le risque de faire pénétrer sur le réseau interne des codes malveillants et/ou de divulguer ensuite des informations recueillies sur le réseau interne.

... dans le respect de la configuration standard	L'utilisateur ne modifie jamais la configuration de son poste de travail et des autres équipements mis à sa disposition par les MCAS, sauf demande explicite des équipes informatiques. En particulier : ▪ il n'ajoute pas et ne retire pas de composant matériel (disque dur, carte réseau...) ; ▪ il n'installe pas de logiciels non autorisés par les MCAS ; ▪ il ne tente pas de modifier ou désactiver les mécanismes de protection (antivirus, paramétrage des mots de passe, installation des correctifs de sécurité...) ; ▪ il ne tente pas de démarrer son poste de travail à partir d'un support amovible (clé USB, CD ROM...).
Protéger et surveillance des équipements	L'utilisateur est responsable de la protection des équipements mis à sa disposition : ▪ **En cas d'absence, même momentanée, il verrouille l'accès à son ordinateur**. En cas d'absence prolongée, et en particulier chaque soir, il ferme les sessions ouvertes sur son poste de travail ; ▪ Il utilise les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé) pour garantir la protection des équipements mobiles (ordinateur portable, smartphone, etc.) et de leurs accessoires ; ▪ L'affectation des équipements mobiles et de leurs accessoires est nominative, conditionnée à la signature d'un document de remise de matériel, se trouvant ainsi sous son entière responsabilité. De tels équipements ne doivent jamais être laissés sans surveillance dans des lieux dont l'accès n'est pas contrôlé (ex : lieux publics) ; ▪ En cas de mise à disposition d'un équipement mobile, l'utilisateur se connecte régulièrement au réseau des MCAS pour s'assurer de la bonne mise à jour de la solution antivirus et de l'application des correctifs de sécurité. Il signale le plus rapidement possible à sa hiérarchie toute perte ou vol d'un équipement mis à sa disposition et effectue les démarches nécessaires de dépôt de plainte (commissariat de police ou gendarmerie de son domicile). Il change ses identifiants dans les meilleurs délais.
Un classement efficace pour une bonne conservation des données	L'utilisateur s'assure que les informations à conserver pour des raisons légales ou nécessaires à l'activité des MCAS font l'objet de traitements adaptés, tenant compte de leur sensibilité et des différents types de supports utilisés (documents papiers, supports informatiques). A cette fin, l'utilisateur respecte les règles de classement en vigueur au sein de son service.

UTILISATION DE LA MESSAGERIE ELECTRONIQUE

La messagerie des MCAS a une vocation professionnelle

Tous les messages sont présumés professionnels.

L'utilisation de la messagerie à des fins personnelles est tolérée sous réserve qu'elle reste exceptionnelle et sans impact sur le bon fonctionnement général du système ou sur la bonne marche du service.

Afin de concrétiser le droit au respect de sa vie privée, il doit être indiqué dans le champ objet des messages le caractère privé de la correspondance.

Usage de la messagerie personnelle

L'utilisateur n'emploie pas de messagerie personnelle à des fins professionnelles.

De même, il ne met pas en œuvre des fonctions d'envoi ou de redirection automatique vers des adresses de messagerie externes. Cet usage expose en effet des informations internes et potentiellement sensibles à un risque important de divulgation.

L'accès à une messagerie personnelle sur un équipement professionnel fragilise le niveau de sécurité des systèmes d'information des MCAS. Il peut être la source d'infections virales massives, notamment par l'ouverture de pièces jointes potentiellement infectées. Il doit être réalisé à partir d'un matériel personnel non connecté aux réseaux des MCAS, tel qu'un smartphone personnel.

En cas de cyberattaque, les MCAS peuvent décider du blocage de l'accès aux services de messageries externes.

Précautions lors de l'envoi de messages...

L'utilisateur est responsable des messages émis avec son adresse de messagerie. A ce titre :

- Il veille à ce que le contenu des messages qu'il envoie n'engage pas à tort les MCAS ;
- Il n'envoie pas (ni ne fait suivre) de message non sollicité (spam) ou contenant des informations illicites ou offensantes.

Les utilisateurs doivent utiliser les adresses de messagerie mises à leur disposition à bon escient, à savoir :

- L'adresse de messagerie professionnelle est l'adresse de messagerie interne nominative attribuée à titre professionnel à tout utilisateur des SI. Des procédures de protection, de classement et d'archivage de ces messages au départ de l'utilisateur sont mises en place par les MCAS. Jusqu'à son départ, l'archivage ou la suppression de ces messages est à la charge de l'utilisateur ;
- Une adresse de messagerie fonctionnelle (boîte aux lettres non nominative) est une adresse des MCAS. Les messages reçus sont considérés comme du courrier officiel des MCAS et sont leur propriété. Des procédures de protection, de classement et d'archivage de ces messages sont mises en place par les MCAS. Ces adresses ne doivent pas être utilisées pour émettre des messages de manière anonyme. A ce titre, les boîtes de messagerie fonctionnelles ne peuvent être accédées que par le biais d'autorisations données à des comptes d'utilisateurs nominatifs.

...et à la réception

L'utilisateur doit faire preuve de vigilance à l'égard des messages qu'il reçoit et dont l'origine, l'objet ou le contenu paraissent douteux[5]. En particulier :

- Il ne transfère pas et ne répond pas aux messages à caractère douteux ;
- Il n'enregistre pas et n'ouvre pas les pièces jointes suspectes ;
- Il ne clique pas sur les liens qui lui paraissent suspects ;
- En cas de doute sur un message demandant une action particulière et inhabituelle, il contacte l'émetteur du message par un autre moyen de communication pour s'assurer de l'authenticité et la légitimité de la demande.

Conservation et protection des courriels

Selon le type de messagerie et la politique de conservation des données, l'utilisateur est informé de règles de conservation et de protection des courriels en vigueur dans son entité (il s'agit de la taille maximum de la boîte aux lettres et de la durée technique de conservation avant effacement).

Les boîtes aux lettres peuvent faire l'objet de restrictions d'usage ou être vidées automatiquement de leur contenu après l'avertissement préalable des utilisateurs.

[5] L'adresse de messagerie électronique peut être usurpée ou modifiée légèrement de manière à tromper le destinataire sur l'origine d'un message. Il faut donc rester attentif aux messages reçus.

Protection des moyens d'authentification	**L'utilisateur est responsable de l'utilisation des systèmes d'information réalisée avec ses droits d'accès. Il doit donc assurer la protection des moyens d'authentification qui lui ont été affectés.** **Il ne les communique ou ne les confie jamais à une tierce personne**, y compris aux intervenants en charge des systèmes d'information, à ses collaborateurs ou à sa hiérarchie. Réciproquement il ne fait en aucun cas usage des moyens d'authentification ou des habilitations d'une tierce personne. Le mot de passe de connexion doit répondre à des exigences de complexité définies dans la politique de mots de passe des MCAS. Il doit être d'une longueur suffisante et comprendre majuscules, minuscules, chiffres et caractères spéciaux.
Respect des droits d'accès	L'utilisateur fait usage de ses droits d'accès uniquement pour accéder à des informations ou des services nécessaires à l'exercice des missions qui lui ont été confiées.
Un accès aux SI contrôlé	La possibilité d'accès distant au réseau interne des MCAS, et plus particulièrement l'accès à la messagerie depuis Internet et/ou depuis un équipement non maîtrisé par les MCAS, est soumise à autorisation préalable. Lorsque cette autorisation est accordée, l'utilisateur respecte les règles d'usage et de sécurité qui lui ont été spécifiquement communiquées.

UTILISATION DE L'INTERNET

Un usage maîtrisé	L'utilisateur accède à Internet (ou à un autre réseau externe) uniquement depuis les équipements mis à sa disposition par les MCAS. Cette solution met en place un certain nombre de filtrages dans l'objectif d'assurer la sécurité des systèmes d'information.[6] Dans le cadre de leurs activités, les agents bénéficient d'un accès individuel aux services Internet qui pourra être restreint ou clos en cas d'utilisation abusive ou non conforme. Si l'utilisateur constate le blocage d'un site consécutif à une mauvaise catégorisation, il lui est possible de contacter son support pour en demander la réévaluation.
Vigilance quant aux sites consultés	Le simple fait de consulter un site Internet depuis le réseau des MCAS peut engager l'image des MCAS, des traces de connexion étant généralement conservées par les sites. **En cas d'accès accidentel à un site Internet illicite, l'utilisateur se déconnecte immédiatement de ce site et en informe sa hiérarchie**. **L'utilisateur reste vigilant et n'utilise pas ses identifiants professionnels sur des services sur Internet**.
Protection de l'image et des intérêts des MCAS	L'utilisateur ne communique jamais ses coordonnées, en particulier son adresse électronique, sur des sites sans rapport avec son activité professionnelle ou dont l'image est incompatible avec celle des MCAS. En particulier, **l'utilisateur n'engage pas à tort l'image des MCAS, notamment dans le cadre d'interventions sur des forums ou des espaces de discussion**. Toute intervention sur Internet respecte les dispositions relatives à l'obligation de réserve, à la discrétion professionnelle et au secret professionnel.

[6] Les services et infrastructures techniques mis en place par les MCAS pour l'accès à Internet font intervenir des moyens destinés à protéger les utilisateurs (filtrage réseau, antivirus...). L'accès à Internet ou à un autre réseau externe par d'autres moyens (modem téléphonique, téléphone mobile ...) ne permet pas à l'utilisateur de bénéficier de cette protection et l'expose à des attaques diverses pouvant se répercuter sur l'ensemble des SI des MCAS. Les MCAS mettant à disposition des utilisateurs une connexion à Internet, ils se trouvent soumis aux exigences imposables aux fournisseurs d'accès, et notamment à l'obligation d'identifier l'utilisateur lors de son accès à Internet et à journaliser des éléments probants de sa navigation pour une durée de 1 an. Les journaux de navigation sont confidentiels et accédés uniquement dans le cadre de procédures légales, sur commission rogatoire.

TRAVAIL A DISTANCE

Attention particulière	Dans le cadre du travail à distance, incluant le nomadisme et le télétravail, il convient d'avoir une attention particulière sur les matériels mis à disposition. Les utilisateurs doivent être vigilants face aux risques de pertes ou de vol. Ils doivent prendre les précautions suivantes : • Ne pas laisser des informations et équipements sans surveillance ; • Protéger les informations et équipements des indiscrétions ou du vol lorsqu'ils ne sont pas utilisés (mise sous clé); • Utiliser des moyens de chiffrement pour l'envoi d'informations sensibles (chiffrement des pièces jointes, utilisation des moyens de connexion sécurisés au SI) ; • Protéger les moyens d'identification (mots de passe, cartes à puce, calculettes, etc.) ; • Sauvegarder régulièrement ses données.
En environnement public	Etre attentif aux indiscrétions. Ne pas consulter de documents sensibles depuis un lieu public. Demander la dotation d'un filtre de confidentialité en cas de besoin.

4 REGLES ET RESPONSABILITES SPECIFIQUES

SUPERIEURS HIERARCHIQUES

Les autorités hiérarchiques respectent comme tout autre utilisateur les règles générales d'usage préalablement mentionnées. Ils exercent par ailleurs un rôle important en matière de sécurité des systèmes d'information auprès de leurs agents et des tiers sous leur responsabilité. A ce titre, un certain nombre de responsabilités spécifiques leur incombent.

Des règles de fonctionnement à définir…	Les autorités hiérarchiques définissent les règles de fonctionnement en matière de sécurité des SI propres à leur service, à travers notamment : ▪ la catégorisation des informations en fonction de leurs besoins de sécurité (disponibilité, intégrité, confidentialité, traçabilité) ; ▪ la définition des conditions d'exportation, de communication et d'archivage des données propres à leur service ; ▪ la définition d'un plan de classement des documents et fichiers électroniques et d'une nomenclature associée ; ▪ le cas échéant, la modification des fiches de tâches des agents pour y ajouter les rôles et responsabilités spécifiques à la sécurité des systèmes d'information.
…et à faire observer	Les autorités hiérarchiques s'assurent du respect des règles de sécurité des SI et de la bonne prise en compte de la sécurité des SI dans les missions de tous les agents et tiers (notamment les stagiaires et les vacataires) intervenant sous leur responsabilité. De plus, ils s'assurent du respect des principes et règles de sécurité des SI dans la conduite des projets.
Des accès à maîtriser	Les autorités hiérarchiques sont en charge de la validation des demandes d'habilitation d'accès aux systèmes d'information (messagerie, intranet, internet, applications, répertoires partagés, etc.) des agents et tiers intervenant sous leur responsabilité. Ils signalent également à la direction des systèmes d'information ou à leur service informatique le départ et les mouvements internes des agents permanents ou temporaires afin de demander la fermeture de leurs comptes, la destruction (et l'archivage à la demande de l'utilisateur) des données personnelles et en conséquence la suppression des droits d'accès.
Une communication nécessaire	Les autorités hiérarchiques, avec l'appui de la chaîne SSI, veillent à la sensibilisation de leurs équipes et sont eux-mêmes exemplaires dans l'application des règles et des principes de sécurité.
Incidents de sécurité	En cas d'incident de sécurité Les autorités hiérarchiques doivent informer la chaîne SSI. Le fonctionnaire à la sécurité des systèmes d'information (FSSI) des MCAS sera également prévenu pour information dans les plus brefs délais via l'adresse: ssi@sg.social.gouv.fr

ADMINISTRATEURS ET EXPLOITANTS DES SYSTEMES D'INFORMATION

Les administrateurs des systèmes d'information sont en charge du bon fonctionnement des ressources (applications, réseaux, bases de données, …). Dans le cadre de leurs missions, ils peuvent disposer de droits étendus. Par leurs actions, ils contribuent à assurer la sécurité des systèmes d'information.

Les exploitants des systèmes d'information, membres de la direction des systèmes d'information ou non, disposent d'un contrôle partiel sur certaines ressources et peuvent assister les utilisateurs dans le cadre de leurs opérations liées aux systèmes d'information.

Les administrateurs et exploitants respectent comme tout autre utilisateur les règles générales d'usage préalablement mentionnées. Du fait de leur rôle clé dans le maintien de la sécurité des systèmes d'information, un certain nombre de responsabilités spécifiques leur incombent et ils sont soumis à des contrôles particuliers.

Des droits étendus à utiliser dans un cadre limité

Les administrateurs et exploitants des systèmes d'information ne doivent pas abuser des droits d'accès spécifiques qui leur sont accordés. En particulier :

- Ils sont soumis à une obligation de discrétion. Notamment, ils ne prennent pas connaissance des données personnelles des utilisateurs, ils respectent la confidentialité des informations auxquelles ils ont accès, ils ne se connectent pas et ne donnent pas accès à des ressources. Néanmoins, ils peuvent en prendre connaissance, en cas d'anomalie, de risque détecté, réel ou supposé, pour remplir leur mission de préservation de la sécurité des systèmes d'information. Certaines informations sont couvertes par le secret des correspondances ou relèvent de la vie privée. Dès lors, les administrateurs, les gestionnaires de réseaux, les personnels de la chaîne SSI sont soumis à la règle du respect du besoin d'en connaitre. Dans ce cadre ils peuvent être amenés à communiquer les informations dont ils ont connaissance à leurs supérieurs hiérarchiques si ces derniers ont la nécessité impérieuse d'en connaitre dans le cadre de leurs fonctions et pour la bonne exécution de la mission.
- Ils limitent leurs actions aux ressources informatiques dont ils ont la charge, dans le respect de la finalité de leur mission. Ils sont tenus d'observer strictement les limites fixées à leur intervention ;
- Ils utilisent les comptes privilégiés **exclusivement** pour les activités et les besoins liés aux tâches d'administration et respectent les règles de sécurité dans l'utilisation des identifiants et des mots de passe associés. Les actions d'administration et d'exploitation sont susceptibles d'être systématiquement tracées et contrôlées ;
- **Il est strictement interdit d'accéder à la navigation sur internet en utilisant des privilèges d'administration (administrateur local, de domaine…)**

Des règles à respecter

Les administrateurs et exploitants des systèmes d'information sont tenus d'informer sans délai leur responsable hiérarchique de toute vulnérabilité ou faille de sécurité qu'ils pourraient découvrir ou dont ils pourraient avoir connaissance.

Ils ne contournent pas les procédures de sécurité établies, ne désactivent pas de leur propre initiative les mécanismes de trace et ne portent pas atteinte à l'intégrité des fichiers de journalisation.

Ils utilisent pour mener leurs missions uniquement des logiciels répondant aux standards agréés techniquement.

Toute installation de logiciel ne faisant pas partie de ces standards doit faire l'objet d'une demande visée préalablement par le responsable hiérarchique et soumise à agrément technique.

ORGANISATION SYNDICALES

Les organisations syndicales s'engagent, pour l'ensemble des outils considérés (Intranet et messagerie), à respecter les conditions de sécurité fixées par le secrétaire général, haut fonctionnaire de défense et de sécurité des MCAS ou par la DSI.

Confidentialité des échanges syndicaux

Dans le cadre des textes en vigueur et de la jurisprudence relative au secret de la correspondance, l'administration s'engage à respecter la confidentialité :

- des messages électroniques en provenance ou à destination des boîtes aux lettres syndicales (contenu, auteurs et destinataires) ;
- de l'intégrité des listes de diffusion élaborées par les organisations syndicales. Le contenu des listes de diffusion syndicales est public comme pour toute liste de diffusion ;
- de l'identité des auteurs des messages destinés à un forum de discussion modéré par une organisation syndicale lorsque qu'il est décidé d'un commun accord entre l'administration et les syndicats d'utiliser une liste restreinte de participants.

Responsabilité des organisations syndicales et de leurs membres

Les organisations syndicales, ainsi que leurs membres, engagent leur responsabilité sur les informations ou prises de position qu'ils décident de rendre publiques par l'intermédiaire des systèmes d'information des MCAS

L'usage des listes de diffusion

Lorsque les organisations syndicales utilisent des listes de diffusion qui leurs sont propres, elles devront indiquer aux destinataires des messages syndicaux qu'ils peuvent demander à tout moment à en être retirés.

5 CONTROLES

Des contrôles nécessaires...	Les MCAS disposent de moyens permettant d'analyser et de contrôler l'utilisation des ressources matérielles et logicielles ainsi que les échanges, quel que soit leur objet ou leur nature, effectués via les systèmes d'information des MCAS. Ainsi, les traces des actions des utilisateurs sont journalisées et conservées.
... mais encadrés...	Les contrôles mis en œuvre par les MCAS sont réalisés : ▪ dans l'objectif de garantir le bon fonctionnement technique et la sécurité des systèmes d'information ; ▪ dans le respect de la législation applicable, notamment la loi « Informatique et Libertés». Tout traitement automatisé fait notamment l'objet d'une déclaration à la CNIL ; ▪ exclusivement sous la responsabilité du responsable de la sécurité des systèmes d'information et des administrateurs des systèmes d'information qui gardent confidentielles les informations qu'ils pourraient être amenés à connaître. Le Fonctionnaire de sécurité des systèmes d'information est informé des actions de contrôle. En fonction du type de contrôle demandé il peut y participer.
... pouvant conduire à des actions...	En cas de constatation d'un fonctionnement anormal des SI, il peut être décidé d'interrompre les opérations usuelles et mettre en œuvre des mesures adaptées et proportionnées de contrôle, de restriction ou encore de fermeture, jusqu'à un retour à la normale.
... voire à des sanctions	La violation des principes et règles inscrits dans la politique de sécurité des systèmes d'information des ministères chargés des affaires sociales et dans les chartes de sécurité peut donner lieu à des sanctions disciplinaires adaptées à la nature de la faute. En cas de non-respect de la législation en vigueur, l'utilisateur est responsable de ses actes et encourt les sanctions civiles ou pénales prévues par la loi. L'ensemble des documents est disponible sur PACO.

6 Glossaire

Administrateur	Personne en charge de la responsabilité des opérations d'installation, de paramétrage, de support et de gestion des ressources numériques
Confidentialité	La confidentialité fait référence à la propriété de l'information d'être uniquement disponible ou divulguée à des individus, entités ou processus autorisés. L'accès à l'information est en quelque sorte réservé aux seules personnes admises à la connaître pour des besoins clairement identifiés.
Disponibilité	Il s'agit de la propriété (pour un système d'information) d'être accessible et de remplir les fonctions envisagées au moment de la demande d'une entité autorisée, dans les conditions de délais et de performance prévues, c'est-à-dire la protection de l'aptitude d'un système d'information à remplir une fonction dans des conditions définies d'horaires, de délais et de performances.
DSI	Direction des systèmes d'information
FSSI	Fonctionnaire de sécurité des systèmes d'information
HFDS	Haut fonctionnaire de défense et de sécurité
Intégrité	L'intégrité d'une information concerne le caractère d'exactitude et d'entièreté des ressources relatives à l'information. C'est-à-dire il s'agit de protéger la véracité et l'entièreté de l'information, ainsi que les méthodes de traitement de cette information.
Preuve	Garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
RSSI	Responsable de la sécurité des systèmes d'information
Système d'information	Ensemble des ressources (les personnels, le matériel, les logiciels, les procédures) permettant, en support à l'activité, de : créer, collecter, stocker, traiter, échanger, partager et communiquer des informations entre des acteurs internes et externes d'une entité, quelle que soit la forme sous laquelle elles sont exploitées (manuscrite, imprimée, vocale, image, électronique, numérique, etc.).
Traçabilité (ou preuve)	garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

7 Textes de références

Obligation de discrétion professionnelle et Secret professionnel	▪ Loi n° 83-634 du 13 juillet 1983 portant droits et obligation des fonctionnaires, article 26 "Les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées dans le code pénal. Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions."
Protection de la vie privée	▪ Article 9 du code civil ▪ Article 226-1 du code pénal ▪ Article 226-15 du code pénal ▪ Article 432-9 du code pénal
Usage illicite de moyens	▪ Article 227-24 du code pénal
Protection des données à caractère personnel	▪ Article 226-16 à 23 du code pénal ▪ Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ▪ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
Protection des données de santé	▪ Article L.1110-1 du code de la santé publique ▪ Article L.1111-8 alinéas 1 et 2 du code de la santé publique ▪ Article L.1460-1 alinéa 1 code de la santé publique
Protection des droits d'auteur	▪ Article L.122-6 du code de la propriété intellectuelle ▪ Article L.335-2 du code de la propriété intellectuelle ▪ Article L.335-3 alinéa 1 du code de la propriété intellectuelle ▪ Article L.335-9 du code de la propriété intellectuelle ▪ Article L.343-1 du code de la propriété intellectuelle ▪ Article L.343-4 du code de la propriété intellectuelle
Protection des données statistiques	▪ Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques
Cryptologie	▪ Loi 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique, article 29 ▪ Article 230-1 du code de procédure pénale
Fraude et attaques informatiques	▪ Article 323-1 à 7 du code pénal
Protection des informations relevant du secret de la défense nationale	▪ Instruction générale interministérielle n° 1300
Protection des systèmes d'information sensibles, notamment ceux traitant des informations portant la mention Diffusion Restreinte.	▪ Instruction interministérielle n°901
Politique de sécurité des systèmes d'information	▪ Politique de sécurité des systèmes d'information de l'Etat ▪ Politique de sécurité des systèmes d'information des ministères chargés des affaires sociales
Numérique	▪ LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique

Recommandations CNIL et ANSSI

Contrôle de l'utilisation d'internet et de la messagerie	▪ https://www.cnil.fr/fr/le-controle-de-lutilisation-dinternet-et-de-la-messagerie-electronique
Guides techniques et hygiène informatique	▪ https://www.cert.ssi.gouv.fr/information/CERTA-2006-INF-006/ ▪ https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf ▪ https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf ▪ https://www.ssi.gouv.fr/uploads/2015/02/NP_SDE_DAT_NT_Archi_Admin.pdf