

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



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

REVISIONS

| Date | Objet |
|-----------|------------------|
| Juin 2017 | Version initiale |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Table des matières

| | |
|---|----|
| PREAMBULE | 4 |
| 1. CHAMP D'APPLICATION..... | 4 |
| 2. DEFINITIONS | 5 |
| 2.1 LE SYSTEME D'INFORMATION..... | 5 |
| 2.2 L'ADMINISTRATEUR DU SYSTEME D'INFORMATION..... | 5 |
| 3. LE PERIMETRE D'INTERVENTION..... | 5 |
| 4. LES MOYENS D'ACTIONS | 6 |
| 5. LES DEVOIRS | 6 |
| 5.1 L'OBLIGATION DE SECRET PROFESSIONNEL, DE CONFIDENTIALITE, DE DISCRETION ET DE NON DIVULGATION | 6 |
| 5.2 UNE DEMARCHE LOYALE | 8 |
| 5.3 UNE DEMARCHE TRANSPARENTE | 8 |
| 5.4 UNE DEMARCHE PROPORTIONNEE..... | 8 |
| 5.5 UNE DEMARCHE DE SECURITE..... | 9 |
| 5.6 L'OBLIGATION DE SIGNALER UNE INFRACTION..... | 9 |
| 6. RESPECT DE LA LEGISLATION ET DE LA PRESENTE CHARTE | 10 |
| 7. ANNEXE | 11 |

PREAMBULE

L'administrateur du système d'information est un acteur important au sein de l'organisme¹. En effet il lui appartient d'assurer la sécurité et le bon fonctionnement du système d'information en opérant, en outre, des contrôles tout en veillant à la protection des données à caractère personnel et des données privées des utilisateurs notamment au regard de la loi informatique et liberté [\(1\)](#), du secret des correspondances [\(2\)](#) ou de l'article 9 du code civil [\(3\)](#).

Cette charte s'applique aux administrateurs du système d'information de la branche Famille. La présente charte précise les moyens d'action, les droits et les devoirs de l'administrateur du système d'information dans l'exercice de son activité en rappelant le cadre juridique applicable ainsi que les droits et devoirs de l'organisme. Il est important de noter que l'administrateur du système d'information est également soumis au respect de la charte nationale de sécurité de l'utilisateur, comme tout utilisateur au sein de la branche Famille.

1. CHAMP D'APPLICATION

La charte nationale de sécurité de l'administrateur 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 aux administrateurs du système d'information (SI). En revanche, elle requiert l'acceptation individuelle de chaque administrateur du SI non soumis au règlement intérieur ou en l'absence de celui-ci.

Elle ne se substitue pas à une fiche de poste ou de mission, ni à un référentiel emploi. Elle complète la charte nationale de sécurité du système d'information de la branche Famille.

La désignation des administrateurs du système d'information et le maintien de la liste des intervenants désignés sont assurés par le Directeur de l'organisme.

En cas de perte de la qualité d'administrateur, les moyens d'action et les droits relatifs à cette charte ne s'appliquent plus, en revanche les obligations de l'administrateur SI demeurent applicables et notamment les celles relatives à l'article 5.1 de la présente charte.

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.

2. DEFINITIONS

2.1 *LE SYSTEME D'INFORMATION*

Ensemble de tous les éléments qui contribuent au traitement et à la circulation de l'information dans l'organisme (base de données, logiciels d'application, procédures, documentation, ...), y compris les ressources du système informatique proprement dit (tels que les serveurs, les équipements réseaux et de stockage, de sécurité et de téléphonie, les stations de travail et les périphériques, le système d'exploitation,).

L'acronyme SI sera utilisé dans le reste du document.

2.2 *L'ADMINISTRATEUR DU SYSTEME D'INFORMATION*

Au sens utilisé dans le présent document, le terme "administrateur du système d'information" désigne tout agent de la branche Famille quelle que soit sa fonction, qui a pour rôle et missions d'assurer le bon fonctionnement et la sécurité des ressources du système d'information dans son domaine d'activité.

Afin de conduire les actions d'administration et de production informatique afférentes à sa mission, (notamment la configuration, la supervision, la maintenance, l'évolution, le support) l'administrateur du système d'information dispose de comptes à privilèges : ce sont des comptes qui n'interagissent pas avec des composants applicatifs, mais directement avec les composants techniques. Ils sont associés à des droits d'accès privilégiés sur les ressources du système d'information.

3. LE PERIMETRE D'INTERVENTION

Le périmètre d'intervention de l'administrateur dépend de son domaine d'activité qui diffère selon les organismes ou sites de la branche Famille auxquels il appartient. En effet ce périmètre est généralement circonscrit à l'organisme ou au site d'appartenance.

Toutefois, dans le cadre d'activités mutualisées, de support ou spécifiques à la Direction des Systèmes d'Information (DSI), ce périmètre peut se trouver élargi à plusieurs organismes ou sites. Dans ces cas une convention de service ou une lettre de mission vient préciser le périmètre d'intervention.

La présente charte ne peut donc définir précisément ce périmètre, cependant, d'une manière générale et non exhaustive, il englobe des tâches d'administration, de production, de maintenance de systèmes et logiciels, de suivi de l'utilisation des ressources du SI, des télécommunications.

4. LES MOYENS D' ACTIONS

Afin de déceler tout incident ou anomalie qui pourrait porter atteinte au bon fonctionnement ou à la sécurité du SI, l'administrateur peut :

- ✓ isoler, arrêter, suspendre ou reconfigurer les ressources du SI (notamment les équipements, les applications informatiques, les comptes utilisateurs) ;
- ✓ procéder à des vérifications techniques sur les ressources du SI (notamment les fichiers, la messagerie, les connexions à Internet, les postes de travail) y compris celles comportant des données à caractère personnel ou des données privées ;
- ✓ traiter (notamment détecter, analyser, éradiquer, filtrer) tout flux informatique présentant un risque de sécurité ;
- ✓ activer et exploiter sur les systèmes dont il a la responsabilité les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements ;
- ✓ prendre le contrôle du poste de travail d'un utilisateur (même à distance) avec l'autorisation expresse de ce dernier ;
- ✓ mettre en place des outils de surveillance, de mesure ou d'administration.

5. LES DEVOIRS

L'administrateur, ayant pour mission d'assurer le bon fonctionnement et la sécurité du système d'information, est conduit par sa fonction même et par ses droits d'administration à avoir accès, dans son périmètre d'intervention, à l'ensemble des informations émises, reçues et créées par les utilisateurs, notamment des données privées (messagerie, historique des sites visités, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers, cookies, etc.).

Toutefois, ce statut atypique est limité par l'obligation de secret professionnel, de confidentialité, de discrétion et de non divulgation ainsi que par des modalités d'intervention qui doivent être loyales, transparentes, proportionnées et sécurisées.

Les administrateurs ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'organisme. Ils ne sauraient être contraints de le faire, sauf décision de justice particulière ou enquête pénale en ce sens.

5.1 L'OBLIGATION DE SECRET PROFESSIONNEL, DE CONFIDENTIALITE, DE DISCRETION ET DE NON DIVULGATION

L'administrateur est soumis à l'obligation de secret professionnel, de confidentialité, de discrétion et de non divulgation.

En particulier, cette obligation de confidentialité concerne aussi bien les correspondances privées des utilisateurs dont les dispositions sont couvertes par le secret des correspondances privées que les fichiers privés dont les dispositions relèvent de la vie privée des utilisateurs.

Si la jurisprudence reconnaît la possibilité à l'administrateur, dans le cadre de sa mission de sécurité, de lire le contenu des messages et des fichiers privés. En revanche il n'est pas autorisé à les divulguer, même à ses supérieurs hiérarchiques(4).

Si l'administrateur divulgue de telles informations, il engage sa responsabilité pénale, notamment pour non-respect du secret des correspondances privées. En revanche, il devra prendre toutes les dispositions afin de préserver les traces et les indices qui pourraient être demandés dans le cadre d'une procédure judiciaire(5).

L'administrateur peut être amené à ouvrir des fichiers informatiques créés par un utilisateur

Dans le cadre de sa mission de sécurité et de bon fonctionnement du SI définie au chapitre 2.2 de la présente charte, l'administrateur peut être amené à ouvrir des fichiers, à caractère professionnel ou privé, créés par l'utilisateur à l'aide de l'outil informatique mis à sa disposition par l'organisme. Cette action peut être effectuée hors de la présence de l'utilisateur.

En revanche, en dehors de sa mission de sécurité et de bon fonctionnement du SI et sur demande de l'organisme, l'administrateur peut être amené à ouvrir les fichiers informatiques créés par l'utilisateur :

- ✓ sauf risque ou événement particulier uniquement en sa présence ou celui-ci dûment appelé s'ils sont identifiés comme privés ;
- ✓ même en dehors de sa présence s'ils ne sont pas identifiés comme privés.

L'administrateur peut accéder à la liste des sites internet consultés par les utilisateurs

Les connexions établies par un utilisateur sur des sites internet, pendant son temps de travail et grâce aux outils informatiques mis à sa disposition par l'organisme, sont présumées avoir un caractère professionnel.

Par conséquent et dans le cadre de sa mission, si l'administrateur découvre une utilisation abusive ou frauduleuse de l'outil informatique, il est à même d'informer l'organisme.

Si l'administrateur constate une utilisation illicite de l'outil informatique (Cf. chapitre 5.6), il a le devoir d'en informer l'organisme.

L'administrateur peut être amené à ouvrir des messages électroniques émis ou reçus par un utilisateur

Dans le cadre de sa mission de sécurité et de bon fonctionnement du SI définie au chapitre 2.2 de la présente charte, l'administrateur peut être amené à ouvrir des messages électroniques, à caractère professionnel ou privé, émis ou reçus par un utilisateur. Cette action peut être effectuée hors la présence de l'utilisateur.

En dehors de sa mission de sécurité et de bon fonctionnement du SI et sur demande de l'organisme, l'administrateur peut être amené à ouvrir les messages électroniques émis ou reçus par un utilisateur :

- ✓ uniquement en sa présence ou celui-ci dûment appelé par l'organisme, s'ils sont identifiés comme privés sauf risque ou événement particulier ;
- ✓ même en dehors de sa présence s'ils ne sont pas identifiés comme privés.

En effet, le régime des messages électroniques identifiés comme privés est soumis au respect du principe du secret absolu des correspondances privées. L'organisme ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages privés émis ou reçus par l'utilisateur grâce à un outil informatique mis à sa disposition.

Il est à noter que le secret des correspondances privées peut être levé dans le cadre d'une enquête pénale ou sur décision de justice⁽⁶⁾. Cette démarche doit être initiée par le Directeur de l'organisme en saisissant la juridiction compétente.

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

5.2 UNE DEMARCHE LOYALE

La démarche de l'administrateur doit être loyale et ses actions doivent être justifiées par des impératifs de sécurité ou de bon fonctionnement du SI.

L'administrateur doit agir dans le cadre de ses fonctions professionnelles, à l'exclusion de toute autre mission éventuellement exercée dans l'organisme et ne doit tirer aucun profit de quelque nature que ce soit des informations auxquelles il aurait accès.

Il appartient à l'administrateur d'agir dans le respect de la vie privée des utilisateurs du SI et pour cela, il doit privilégier les moyens d'investigation les moins intrusifs.

5.3 UNE DEMARCHE TRANSPARENTE

Afin que la démarche de l'administrateur puisse s'effectuer dans une logique de transparence, l'organisme doit informer les utilisateurs du contenu de cette présente charte.

Les logiciels de prise de main à distance peuvent permettre aux administrateurs du SI, dans le cadre de leurs fonctions, d'accéder à l'ensemble des données de n'importe quel poste de travail.

Dans cette hypothèse, leur utilisation doit s'entourer de certaines précautions pour garantir la transparence dans leur emploi et la confidentialité des données auxquelles l'administrateur a accès par ce moyen, et ce, dans la stricte limite de ses besoins professionnels.

Cette démarche doit être encadrée d'une part, par le recueil de l'accord de l'utilisateur avant intervention sauf en cas de risque potentiel sur la sécurité du SI, et d'autre part par la conservation des traces de son intervention.

L'administrateur a alors l'obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de ses missions et d'en assurer la confidentialité.

L'administrateur est informé que ses actions au sein du SI sont susceptibles d'être tracées.

5.4 UNE DEMARCHE PROPORTIONNEE

L'organisme peut apporter des restrictions aux droits et libertés des utilisateurs, sous réserve qu'elles soient justifiées et proportionnées au but recherché.

En l'espèce, l'atteinte aux droits et libertés relatives aux correspondances et fichiers privés se justifie par la nature des fonctions de l'administrateur.

Les interventions de l'administrateur doivent être proportionnées au but recherché, il appartient à l'administrateur d'utiliser les moyens permettant de remplir sa mission sans aller au-delà(7).

Par exemple, il n'y a pas lieu pour l'administrateur de contrôler le contenu même des messages émis ou reçus si seul le contrôle du volume des pièces jointes lui permet de vérifier l'utilisation optimale du réseau.

De plus, les interventions de contrôle ou de surveillance individuelles mises en place doivent avoir un caractère ponctuel.

5.5 UNE DEMARCHE DE SECURITE

L'administrateur du SI observe strictement les règles de sécurité et les limites fixées à ses interventions :

- ✓ il a le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention susceptible de perturber ou d'interrompre l'utilisation des ressources informatiques ;
- ✓ il est tenu de déclarer tout incident de sécurité qu'il pourrait découvrir au correspondant sécurité ou au comité de pilotage de la sécurité du SI et de conserver une trace de l'évènement par tout moyen mis à sa disposition ;
- ✓ il est tenu de déclarer toute violation des règles du SI, qu'il pourrait découvrir, à son supérieur hiérarchique et conserver une trace de l'évènement par tout moyen mis à sa disposition ;
- ✓ il protège l'utilisation des comptes et des équipements qui lui sont attribués. Il veille notamment à la protection des postes de travail à partir desquels il exerce ses fonctions ainsi qu'aux identifiants et dispositifs d'authentification des comptes à privilège. Plus spécifiquement, les mots de passe utilisés pour les opérations d'administration, de production ou de maintenance doivent être complexes et changés régulièrement conformément à la politique de sécurité en vigueur ;
- ✓ il utilise les comptes à privilège uniquement pour des activités et besoins directement liés aux tâches d'administration, de production ou de maintenance les nécessitant ;
- ✓ il crée et modifie des configurations et des droits d'accès dans le respect des procédures définies. Il veille notamment à respecter les procédures d'attribution et de communication des mots de passe utilisateur ;
- ✓ il utilise les logiciels et les outils approuvés par l'architecture nationale. L'installation d'outils complémentaires doit être justifiée et autorisée par le responsable hiérarchique ;
- ✓ il documente ses actions et interventions afin d'assurer la continuité d'activité de son périmètre d'intervention ;
- ✓ il collabore et coopère avec la personne en charge des aspects informatiques et libertés de l'organisme afin d'accomplir les formalités préalables à la mise en œuvre de traitement de données à caractère personnel.

5.6 L'OBLIGATION DE SIGNALER UNE INFRACTION

S'agissant des correspondances et des fichiers non identifiés comme privés l'administrateur du système informatique signale à l'organisme les pratiques illicites des utilisateurs qu'il détecterait dans l'exercice de ses fonctions. Si ces pratiques sont susceptibles de qualifications pénales, le Directeur, en sa qualité de supérieur hiérarchique et de représentant légal de l'organisme, a qualité pour déposer plainte ou du moins dénoncer les faits au procureur de la République. Une intervention à titre personnel de l'administrateur n'est pas autorisée.

Sans que cette liste soit exhaustive, les pratiques ou comportements suivants sont illicites :

- ✓ le stockage, la diffusion de contenus faisant l'apologie des crimes contre l'humanité, provoquant à la commission d'actes de terrorisme et de 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, incitant à la violence, portant atteinte à la dignité humaine ;
- ✓ la diffusion d'information à caractère injurieux, diffamatoire, dénigrant, attentatoire à la vie privée, raciste, xénophobe, révisionniste et terroriste ;
- ✓ l'utilisation de l'outil informatique professionnel afin de mener des actions d'escroqueries ou de malversations informatiques (par exemple : hameçonnage, intrusion frauduleuse dans un système informatique, usurpation d'identité, entrave au bon fonctionnement d'un système informatique, ...) ;
- ✓ le non-respect de la protection des mineurs ;
- ✓ le non-respect des droits d'auteurs et des droits de propriété intellectuelle de tiers ;
- ✓ l'atteinte au secret professionnel ;
- ✓ l'introduction, la suppression ou la modification frauduleuse de données contenues dans un système de traitement automatique de données ou l'extraction, la détention, la reproduction ou la transmission frauduleuse de données issues d'un système de traitement automatique de données.

6. RESPECT DE LA LEGISLATION ET DE LA PRESENTE CHARTE

L'administrateur du système d'information s'engage à respecter la législation en vigueur et les règles de ce document. Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'administrateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information, voire des sanctions disciplinaires proportionnées selon la gravité des faits concernés.

7. ANNEXE

Cadre juridique

1) La loi n° 78-17 du 06/01/78 dite « informatique et libertés », modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

2) Article 226-15 du code pénal: Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000€ d'amende. Est puni des mêmes peines, le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises et reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.

3) Article 9 du code civil : chacun a droit au respect de sa vie privée.

4) Article 432-9 du code pénal : Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter , hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances est puni de trois ans d'emprisonnement et de 45000€ d'amendes.

5) Article 434-4 du code pénal : Est puni de trois ans d'emprisonnement et de 45000€ d'amende le fait, en vue de faire obstacle à la manifestation de la vérité : 1° De modifier l'état des lieux d'un crime ou d'un délit soit par l'altération, la falsification ou l'effacement des traces ou indices, soit par l'apport, le déplacement ou la suppression d'objets quelconques ; 2° De détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.

6) Ordonnance sur requête d'un juge en application de l'article 145 du code de procédure civile désignant un huissier pour accéder aux messages.

7) Article 1121-1 du code du travail : Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.