MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

CHARTE DES ADMINISTRATEURS DU SYSTEME D'INFORMATION ET DES SERVICES NUMERIQUES DU MINISTÈRE DE LA JUSTICE

Version - Date	Emetteur	Statut/Suivi des modifications
V1 07/11/2022	Cellule HFDS	En cours

Table des matières

Préambule

La charte des administrateurs du ministère de la Justice s'inscrit dans un cadre règlementaire décliné à l'article 7 de la présente. Les administrateurs du ministère de la Justice interviennent directement pour installer, paramétrer, maintenir, assurer l'assistance, développer ou contrôler les systèmes d'information et de communication du ministère de la Justice. Ils peuvent le cas échéant disposer de droits d'accès et de privilèges étendus sur certains systèmes (en particulier des systèmes d'exploitation, des applications, des logiciels ou des micro-logiciels).

Dans le cadre de leur mission professionnelle confiée par le ministère, ces personnels bénéficient de droits spécifiques et peuvent être amenés, de manière incidente, à avoir accès aux informations d'autres utilisateurs et des justiciables susceptibles de présenter un caractère sensible. C'est pourquoi, ils doivent respecter des règles complémentaires à celles prévues par la charte d'usage des services numériques du ministère de la Justice.

ARTICLE 1 - Objet

La présente charte a pour objet de définir de façon complémentaire à la charte d'usage des services numériques du ministère de la Justice, les principales prérogatives, les obligations, les engagements et la responsabilité des « administrateurs » opérant pour le compte du ministère de la Justice.

ARTICLE 2 – Portée et opposabilité

La présente charte et les modifications ultérieures qui pourraient intervenir sont publiées au *Bulletin Officiel* du ministère de la Justice. En conséquence, elle s'impose à l'administrateur des services numériques.

ARTICLE 3 - Définitions

Les définitions suivantes s'appliquent dans la suite du document :

- **CSSI** : Correspondant à la Sécurité des Systèmes d'Information

  Utilisateur(s) : tout agent du ministère de la Justice qui est amené à utiliser les services numériques du ministère de la Justice. Toute personne extérieure dont l'accès au service utilisé fait l'objet d'un lien contractuel (plan assurance sécurité).

- Au sens de la présente charte, le terme administrateurs recouvre les administrateurs fonctionnels et les administrateurs techniques

- **Administrateur fonctionnel** : en charge des activités de suivi d'exploitation (gestion des traitements et des données) liées à une application ou à un ensemble d'applications. Les droits d'accès sont mis en place par un administrateur technique. L'administrateur fonctionnel intervient dans un cadre et une mission spécifique.

- **Administrateur technique** : assure le fonctionnement opérationnel d'une catégorie ou d'un ensemble de matériels et logiciels techniques. L'administrateur technique intervient dans un cadre et une mission spécifique.

- **Justiciable** : toute personne en relation avec le service public de la justice quel que soit son statut (témoin, victime, mis en cause …) et par extension toutes les données à caractère personnel le concernant

- **Services numériques** : ensemble de processus et de ressources permettant d'acquérir, de générer, de traiter, de stocker, de détruire, de diffuser, de transmettre ou d'accéder à des informations électroniques au sein du ministère de la Justice.
- **Ressources numériques** : ensemble de moyens informatiques et de télécommunications, matériels ou logiciels, que le ministère met à disposition des utilisateurs et des justiciables afin que ceux-ci puissent accomplir leurs activités et tâches professionnelles. Ainsi, les micro-ordinateurs fixes ou portables, les moyens de communication (messagerie, accès à l'Internet, réseaux de transmission voix ou données, téléphones fixes ou portables, télécopieurs, service de visio-conférence, etc.), les équipements de stockage de données (disques durs externes, clés USB, supports optiques tel que le DVD, etc.), les données contenues sur les équipements précédemment cités, les applications informatiques et autres logiciels font partie des ressources du système d'information du ministère.
- **RSSI** : Responsable de la sécurité du système d'information. A noter que selon les périmètres fonctionnels, on emploie parfois les termes de RCSSI ou de RGSSI
- **RCSSI :** Responsable Central de la Sécurité du Système d'Information.
- **RGSSI :** Responsable Général de la Sécurité du Système d'Information.

ARTICLE 4 - Champ d'application

La présente charte s'applique de plein droit aux agents intervenant sur les systèmes d'information et de communication du ministère de la Justice désignés ci-après Administrateurs, et disposant de droits d'accès et de privilèges sur tout ou partie de ces systèmes, dans la mesure où ces droits sont plus élevés et plus étendus que ceux accordés aux autres utilisateurs et justiciables.

En particulier, les Administrateurs des systèmes et des réseaux peuvent, selon leur(s) privilège(s), être affectés à un certain nombre de missions comme :

- la gestion, l'exploitation et la maintenance des systèmes d'information et de communication ;
- le suivi et le contrôle de l'utilisation des systèmes d'information et de communication ;
- la mise en œuvre des logiciels et autres applications ;
- la gestion des anomalies et incidents ;
- la collaboration à la gestion des notifications des incidents de sécurité et des violations de données à caractère personnel, en lien avec le délégué à la protection des données et le haut fonctionnaire de défense et de sécurité ;
- des actions de remédiation des systèmes d'information et de communication.

La présente charte doit être incluse dans les clauses contractuelles avec les prestataires pour application.

ARTICLE 5 - Prérogatives de l'Administrateur

Le rôle de l'Administrateur, qui est de garantir le bon fonctionnement des systèmes et des réseaux d'un organisme tout en veillant à la bonne qualité et continuité du service informatique, a connu une importante évolution ces dernières années, en particulier avec le développement des risques numériques.

De fait, la maintenance préventive et curative, ainsi que le contrôle du niveau de sécurité du système d'information et de communication sont assurés par l'Administrateur. Il procède, dans ce cadre, à l'implémentation des mesures de sécurité en adéquation avec les objectifs fixés par la maîtrise d'ouvrage du système. Il met également en œuvre la correction de toute anomalie des systèmes numériques. Enfin, il préconise et met en place des solutions de contournement permettant d'assurer la continuité des services.

Pour répondre à ses missions, l'Administrateur s'engage à prendre connaissance et appliquer les bonnes pratiques de sécurité préconisées par le ministère de la Justice.
Sans que cette liste soit exhaustive, ses prérogatives sont détaillées ci-après.

ARTICLE 5.1 – Actes d'administration

- Intervention sur le système d'information

Dans le cadre de sa mission, l'Administrateur sera amené à intervenir sur les systèmes d'information (opérer des modifications). En cas de doute sur l'efficacité des modifications, l'Administrateur devra appliquer le principe de précaution et mettre en quarantaine ou à défaut détruire, sur autorisation préalable de son responsable hiérarchique et du RSSI, les fichiers qu'il estimerait pouvoir porter atteinte à l'intégrité, à la confidentialité ou à la disponibilité des systèmes d'information qu'il administre.

L'Administrateur devra notifier toute mise en quarantaine ou destruction de tout type de fichiers, dans les meilleurs délais et au plus tard dans les 48 heures suivant ladite mise en quarantaine ou destruction, à son responsable hiérarchique et au RSSI.

- Accès au système d'information

Les actions d'administration sont réalisées à partir des dispositifs de rebond ou d'accès mis en place par le service en charge de l'exploitation, en particulier le dispositif de rebond appelé « accès admin ».
Il est interdit de réaliser des actions d'administration par un autre moyen sans autorisation expresse du chef de département ou de son représentant (adjoints ou manager de permanence en dehors des heures ouvrées).
L'ensemble des actions réalisées via ces dispositifs font l'objet d'un recueil de traces.

Lorsqu'il procède à des interventions à distance sur du matériel professionnel sur demande de l'utilisateur ou du justiciable, l'Administrateur, devra, dans la mesure du possible, requérir la présence ou à défaut le consentement de l'utilisateur ou du justiciable.

- Données et traces

Il est interdit à un Administrateur de consulter des données, logs ou autres informations qui ne sont pas nécessaires aux missions qui lui ont été confiées par le responsable hiérarchique (chef de bureau par exemple) ou fonctionnel (maitrise d'œuvre par exemple) :

- les traitements sur les données et traces pour des besoins de sécurité sont réalisés par l'équipe dédiée à cette mission au sein du service du numérique ;
- les traitements sur les données et traces mises à disposition des administrateurs techniques sont uniquement réalisés pour des besoins d'analyse de performance et de diagnostics d'incidents.

L'Administrateur ne doit pas diffuser à des tiers des traces ou données auxquelles il a accès dans le cadre de ses missions sans autorisation de son supérieur hiérarchique ou en dehors de procédures prédéfinies.
L'Administrateur ne doit pas conserver, au-delà d'un besoin ponctuel ou de respect d'une procédure, des traces et données, issues d'actions d'administration, sur des supports amovibles. Les supports utilisés dans le cadre d'un besoin ponctuel ou d'une procédure, restent dans les locaux professionnels sauf nécessité de transport entre deux sites de l'administration avec une validation au préalable du supérieur hiérarchique.

L'Administrateur ne doit pas conserver sur les ordinateurs mis à disposition, au-delà d'un potentiel délai de traitement indispensable, des traces et données issues d'actions d'administration.

ARTICLE 5.2 – Maintien en condition de sécurité et continuité de service

L'Administrateur est un élément clé dans la réussite du maintien en condition de sécurité et dans la continuité de service. Il s'engage à respecter les procédures d'exploitation définies par le ministère de la Justice.

ARTICLE 5.3 – Détection d'incidents de sécurité

L'Administrateur peut, à l'occasion de ses missions, identifier des comportements qui constituent une violation grave de la charte des utilisateurs des services numériques de la part des utilisateurs .

Lorsqu'il constate une anomalie de ce type, il en informe immédiatement, et au plus tard dans un délai de six heures (délai recommandé) à compter de ladite constatation sa hiérarchie directe et le RSSI de son entité

ARTICLE 6 - Engagements et obligations de l'Administrateur

Afin d'opérer efficacement ses missions, l'Administrateur s'engage à :

- agir exclusivement dans le cadre de ses fonctions et à ce que son action ne découle pas d'une initiative personnelle mais d'une nécessité justifiée par des impératifs de mission ou de sécurité validés par sa hiérarchie (hiérarchie directe ou acteur de la chaine SSI) ;
- respecter le besoin d'en connaître : à savoir n'accéder qu'aux informations qui lui sont indispensables dans le cadre de ses fonctions ;
- respecter le droit à la vie privée, le secret des correspondances privées et des données à caractère personnel des utilisateurs et des justiciables ARTICLE 6.1 - Coopération

ARTICLE 6.1 - Coopération

Tout Administrateur doit rendre compte (analyse, résultats) à sa hiérarchie fonctionnelle, aux autorités compétentes en interne (FSSI de la cellule HFDS, délégué à la protection des données ministériel (DPD), pôle protection des données personnelles (PDP) du SNUM), et à toute autorité publique et/ou judiciaire qui pourrait requérir la communication d'informations.

Dans le cas où l'Administrateur aurait le moindre doute sur la légitimité d'une demande de création, de modification ou de suppression ou encore d'une demande de transmission d'informations (exemple : demandes illégitimes d'effacement de données), il ne doit pas effectuer d'action sans en référer immédiatement à sa hiérarchie qui lui donnera les instructions à suivre.

L'Administrateur remet toute information demandée uniquement après autorisation expresse de son responsable hiérarchique et des autorités compétentes en interne (RSSI, HFDS, DPD).

ARTICLE 6.2 - Information, conseil et alerte

Tout Administrateur s'engage à informer, conseiller, alerter et mettre en garde le SNUM du ministère de la Justice via le responsable fonctionnel.

Aucune action qui pourrait avoir pour conséquence de détruire, supprimer ou corrompre des éléments de preuve ne doit être engagée sans vérifier le respect des règles d'archivage légal et sans la validation préalable du SNUM (sa hiérarchie directe, le RCSSI / CSSI de l'entité voire le RGSSI) du ministère de la Justice.

ARTICLE 6.3 - Confidentialité renforcée

Tout Administrateur s'engage à respecter toutes les mesures de sécurité nécessaires à la protection des informations et au maintien de leur confidentialité, conformément à la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

Tout Administrateur s'engage à garder confidentielles et à ne pas divulguer à des tiers, toutes les informations, y compris à caractère privé, qui lui ont été révélées et dont il a eu connaissance dans le cadre de ses missions ou de son travail, quel qu'en soit le support (numérique, écrit, oral).

A cet égard, l'Administrateur s'engage à :

- Veiller à ce que les tiers non autorisés n'aient pas connaissance de ces informations ;
- Respecter l'obligation de réserve et le devoir de discrétion en usage au sein du ministère de la Justice ;
- S'assurer de l'identité et des privilèges de l'utilisateur pour l'accès à tout ou partie d'éléments du système d'information, en collaboration avec son responsable hiérarchique ;
- Garantir la confidentialité de son moyen d'identification d'Administrateur. L'administrateur s'engage à respecter les règles définies dans la PSSIMJ.
- Réaliser la télémaintenance sur le poste de travail d'un utilisateur seulement à la demande et en présence de ce dernier, et ne se connecter qu'aux seules ressources nécessaires à l'accomplissement de sa mission d'assistance ;

- Garantir la transparence dans l'emploi d'outils de prise en main à distance ou tout autre intervention sur l'environnement de travail individuel de l'utilisateur (notamment en cas d'utilisation du mot de passe de l'utilisateur).

Dans le cadre d'une alerte de sécurité ou de violation de la charte d'usage des services numériques du ministère de la Justice, un Administrateur ne doit partager les informations dont il a connaissance qu'à un nombre restreint de personnes (hiérarchie directe, chaîne de la sécurité des systèmes d'information (SSI) dont le RSSI ou CSSI, le fonctionnaire de la sécurité des systèmes d'information (FSSI).

L'Administrateur n'a pas le droit de communiquer au supérieur hiérarchique de l'utilisateur l'identifiant et le mot de passe de ce dernier, sous réserve des nécessités de services et dans le respect de la vie privée de l'agent.
Comme mentionné au sein de la charte d'usage des services numériques du ministère de la Justice (partie « Nécessité impérieuse de service »), « en cas d'absence prolongée, l'accès aux ressources informatiques de l'utilisateur ou du justiciable (messagerie électronique, base collaborative, répertoire réseau, poste de travail, ou tout service numérique ou matériel informatique et de communication), peut être autorisé en cas de nécessité par son supérieur hiérarchique. Ce dernier doit pour cela en faire la demande expresse au responsable de l'administrateur du système, et en informer en parallèle le responsable des ressources humaines.
Dans tous les cas, l'intéressé est averti au préalable, dans toute la mesure du possible, des demandes d'autorisation d'accès à ses ressources. »

ARTICLE 6.4 - Protection des données à caractère personnel

Dans le cadre de l'exercice de ses missions, l'Administrateur s'engage à respecter la réglementation en vigueur applicable en matière de protection de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (dit règlement général sur la protection des données ou RGPD) ainsi que la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

A cet égard, l'Administrateur s'engage :

- à ne pas porter atteinte, sous quelque forme que ce soit et pour quelque motif que ce soit, à la vie privée des utilisateurs et des justiciables et au secret de leurs correspondances privées ;
- à effectuer les accès aux fichiers et dossiers marqués « PERSONNEL » ou « Personnel » qu'en présence de l'utilisateur ou après l'avoir invité à être présent. En l'absence de l'utilisateur et en cas d'évènement ou de risque particulier pour le ministère de la Justice, l'Administrateur peut y accéder, après autorisation expresse de son responsable hiérarchique, sans en informer au préalable l'utilisateur ;
- à ne pas accéder aux courriels marqués « PERSONNEL » ou « Personnel » envoyés ou reçus depuis la messagerie professionnelle de l'utilisateur, sauf dans le cas d'une réquisition judiciaire ou d'une décision d'un juge autorisant ledit accès.

L'Administrateur qui est amené à accéder, dans le cadre de ses missions et prérogatives, à des fichiers, des données et des messages des utilisateurs et des justiciables comportant la mention « PERSONNEL » ou « Personnel » et pouvant être contenus dans tout ou partie des services numériques, s'engage à en assurer la confidentialité et l'intégrité. En tout état de cause, la violation du secret des correspondances constitue une infraction pénale.

ARTICLE 6.5 - Sécurité

Tout Administrateur s'engage :

- à n'utiliser que les moyens informatiques et de communication autorisés par le SNUM du ministère de la Justice et s'interdit d'utiliser toute autre solution, notamment dans le cadre d'opérations de contrôle ou d'audit ;
- à n'utiliser les outils mis à sa disposition que dans un but professionnel lié aux tâches qui lui incombent (supervision, exploitation, maintenance ou assistance) ;
- à ne pas supprimer ou porter atteinte à l'intégrité des fichiers de journalisation pendant leur durée de conservation ;
- à ne pas procéder, ou faire procéder par l'intermédiaire d'un prestataire, à des changements de configuration permettant de supprimer les traces informatiques sans autorisation hiérarchique, ou en dehors des cas prévus par la politique de sécurité et par la réglementation en vigueur au sein du ministère de la Justice;
- à ne pas chiffrer les données ou fichiers sans procédure ni autorisation spécifique de son supérieur hiérarchique (PSSIE, référentiel général de sécurité (RGS));
- à n'utiliser les comptes privilégiés ou les droits ou privilèges étendus que pour les activités et les besoins directement liés aux tâches d'administration ou d'exploitation dont il a la charge ;
- à ne pas abuser de ses prérogatives et veiller à ce que les contrôles soient réalisés après information préalable et de manière proportionnelle et adaptée à la finalité présentée à l'utilisateur lors de l'information préalable à ces contrôles ;
- à répondre à toute consigne de surveillance, de recueil d'information ou d'audit émise par les RSSI concernés (issus de la maîtrise d'ouvrage et de la maîtrise d'œuvre) ou la cellule HFDS ;
- à ne prendre aucune consigne d'une personne non identifiée et, le cas échéant, à transmettre à son responsable hiérarchique toute requête lui paraissant abusive ;
- pour les usages réalisés dans le cadre de sa vie privée résiduelle au travail, à n'utiliser qu'un compte utilisateur sans droits d'accès ni privilèges étendus.

ARTICLE 6.6 - Respect des droits de propriété

Dans le cadre de l'exercice de ses missions, l'Administrateur s'engage à ne pas porter atteinte aux droits de propriété intellectuelle.

Il s'engage notamment à :

- ne pas installer et ne pas utiliser, sur les matériels informatiques, un logiciel et/ou un progiciel sans qu'une licence d'utilisation appropriée n'ait été préalablement souscrite ;
- ne pas pratiquer des téléchargements illicites ;
- ne pas reproduire ou utiliser des créations protégées par le droit de la propriété intellectuelle ou droit à l'image sans autorisation ;
- maintenir les formules de droits d'auteur.

ARTICLE 6.7 – Habilitation

Toute personne assurant des actes d'administration « systèmes et réseaux » peut être amenée à être habilitée selon les missions qui lui sont attribuées par le ministère selon les procédures de gestion du secret de la Défense Nationale. L'administrateur s'engage à renseigner le document qui lui est transmis par l'officier de sécurité pour initier la démarche.

Si l'autorisation lui est refusée après le démarrage de l'activité au sein du ministère, il sera mis fin à son activité d'administration dès connaissance par la hiérarchie du refus d'autorisation.

Les administrateurs respectent strictement les règles afférentes au secret lié aux procédures judiciaires.

- Habilitation applicative

Certaines parties du SI peuvent nécessiter une habilitation « intuitu personae » supplémentaire. De même, l'échange d'informations ne peut avoir lieu qu'entre Administrateurs dûment habilités sur cette partie du SI. Dans le cas d'espèce, un document indiquant les spécificités de gestion et la liste des administrateurs habilités sera fournie.

- Délégation des droits d'administration

Les droits d'administration ne sont pas transférables de la propre décision de l'agent. L'attribution de droits d'administration sur le SI fait l'objet d'une procédure validée par son supérieur hiérarchique.

ARTICLE 7 - Responsabilité de l'Administrateur

- Responsabilités

Les moyens mis à la disposition de l'Administrateur le sont à des fins exclusivement professionnelles.

L'administrateur engage sa responsabilité et peut répondre, pénalement et administrativement, de tout acte de malveillance, d'imprudence, de négligence ou d'inattention ayant pour résultat qu'une information ou un support dont il est le dépositaire ait été détruit(e), détourné(e), soustrait(e), ou reproduit(e).

En cas de violation ou de non-respect des obligations lui incombant dans le cadre de sa mission ou des dispositions de la présente charte, en particulier dans le cas de dépassement non justifié de ses prérogatives, l'Administrateur sera tenu responsable de ses actes et pourra encourir des sanctions disciplinaires ou administratives adaptées à la gravité des agissements constatés, sans préjudice d'éventuelles sanctions pénales ou civiles à son encontre.

Dans l'un ou l'autre de ces cas, tout ou partie de ses droits d'accès et privilèges sur les services numériques pourront être suspendus voire supprimés.

- Rappels de textes applicables

La responsabilité de l'administrateur est encadrée par :

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée (dite loi informatique et libertés)
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère

personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, RGPD)
- Loi de programmation militaire (LPM)-Arrêté du 23 décembre 2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Activités judiciaires » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense (rectificatif) NOR : PRMD2138744Z
- Politique de sécurité des systèmes d'information e l'Etat du 17 juillet 2014
- Contrat liant l'entreprise de services du numérique (ESN) et l'Administration
- Contrat entre l'employeur et l'employé (Code du travail et code civil, articles 1134 du Code civil et L1222-1 du Code du travail, Code de la fonction publique

Les moyens mis à la disposition de l'Administrateur le sont à des fins exclusivement professionnelles.

Il veille particulièrement à respecter les articles suivants du Code pénal :
- Article 226-13 : la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire
- Article 226-21 du code pénal sur le fait, par toute personne détentrice de données à caractère personnel, de détourner ces informations de leur finalité
- Article 226-22 du code pénal sur le fait, par toute personne qui a recueilli des données à caractère personnel de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir
- Article 441-1 sur *toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit*

ARTICLE 8 – Entrée en vigueur de la charte

La présente charte entre en vigueur à compter de sa publication et pourra faire l'objet de révisions, en fonction des évolutions technologiques et juridiques du système d'snformation et de ses impératifs de sécurité.