# CHARTE DU SYSTEME D'INFORMATION DE LA DIRECTION DES SERVICES JUDICIAIRES

**Annexe à l'arrêté du Secrétaire d'État à la Justice,**
**Directeur des Services Judiciaires n° 2022-7**

**ANNEXE AU « JOURNAL DE MONACO » N° 8.583**

**DU 25 MARS 2022**

## TABLE DES MATIERES

**AVANT PROPOS :**

L'objet de la présente charte est de favoriser l'usage des ressources informatiques et de communication électronique tout en assurant une utilisation conforme aux meilleures pratiques et respectueuse des capacités techniques disponibles.

Elle vise également à harmoniser et organiser cet usage en rappelant les règles à respecter, ainsi qu'à définir les moyens de contrôle susceptibles d'être mis en œuvre si les utilisations n'étaient pas conformes à l'éthique ainsi qu'aux obligations professionnelles.

Elle respecte les principes d'utilisation posés par la Charte des systèmes d'information de l'Etat, en prenant en considération les spécificités propres à la Direction des Services Judiciaires.

Il convient en effet de rappeler, d'une part que les serveurs du Palais de Justice, reliés au réseau Internet pour les besoins des utilisateurs internes, doivent permettre aussi aux prestataires, voire à des magistrats non permanents, d'y accéder depuis ce réseau, et d'autre part que des règles particulières de confidentialité sont applicables au sein de la Direction des Services Judiciaires en raison de la nature même de sa mission.

## 1. DEFINITIONS ET OBJECTIFS

### *1.1 Définitions*

Sont appelés dans la présente Charte :

« Système d'Information de la Direction des Services Judiciaires » : L'ensemble des moyens techniques, de ressources humaines dédiées à l'activité informatique, de procédures régissant son contexte d'application et de bon usage, de traitement de l'information et de communication électroniques de la Direction des Services Judiciaires, incluant les éléments suivants: ordinateurs (fixes ou portables ou tout matériel permettant un accès), périphériques, réseau interne (serveurs, routeurs et connectique), photocopieurs reliés au réseau, logiciels, fichiers, données et bases de données, système de messagerie, réseau internet, abonnements à des services interactifs.

« Utilisateur»: toute personne disposant d'un accès ou utilisant le Système d'Information, quel que soit son statut (magistrat, fonctionnaire, agent contractuel, visiteur occasionnel).

« Administrateur » : la personne désignée à cet effet par le Directeur des Services Judiciaires et chargée de veiller à la protection, à la maintenance et au bon fonctionnement du Système d'information, ainsi qu'au respect de la présente Charte.

« Référents Informatiques»: les personnes pressenties par l'Administrateur, et acceptées par le Chef de Juridiction ou Chef de Service concerné, pour assurer la liaison entre l'Administrateur et les utilisateurs de chaque catégorie statutaire, et faciliter l'utilisation optimale du Système d'Information de la Direction des Services Judiciaires.

« Accès distant»: il s'agit d'un accès à partir d'un site extérieur et quel que soit le lieu de cet accès (domicile, etc.) au Système d'Information de la Direction des Services

Judiciaires qui ne sont pas présents sur le moyen informatique local, et ce grâce à une technologie d'accès à distance (exemple: Xendesktop,Netscaler, Palo Alto)

« Matériel nomade»: moyens et ressources informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de la Direction des Services Judiciaires tels que par exemple ordinateur portable, téléphone mobile, Personal Digital Assistant (PDA), tablettes et autres accessoires (disquette, disque dur, carte mémoire, CD-Rom, clé USB, équipement réseaux, équipement sans fil, carte de communication à distance), et autres existants ou à venir;

### *1.2 Objectifs*

L'utilisation du Système d'Information de la Direction des Services Judiciaires suppose le respect de règles destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance, ainsi que le respect des dispositions constitutionnelles, légales et réglementaires applicables.

La présente Charte est rédigée dans l'intérêt de chaque utilisateur et manifeste la volonté de la Direction des Services Judiciaires d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des ressources informatiques et de communication électronique.

Elle a pour objectif de formaliser les règles de déontologie et de sécurité applicables aux utilisateurs au titre de la mise à disposition du Système d'Information de la Direction des Services Judiciaires.

## 2. REGLES D'UTILISATION

### *2.1 Généralités*

Les équipements et services, mis à la disposition de l'utilisateur, sont exclusivement installés, configurés et paramétrés par les prestataires sous la supervision de l'Administrateur, ou par l'Administrateur lui-même.

L'utilisateur s'interdit de modifier les équipements mis à sa disposition par l'ajout de logiciels ou de matériels sans consultation préalable de l'Administrateur, et ce pour des raisons de sécurité.

Les opérations demandées pourront être refusées par l'Administrateur si l'ajout de matériel ou de logiciel envisagé est susceptible, soit de créer une faille dans les protocoles de sécurité du réseau du Palais de Justice ou un risque de déperdition de données, soit de porter atteinte au bon fonctionnement du système.

Les ressources informatiques, mises à la disposition des utilisateurs, sont et demeurent la propriété de l'Etat.

Pour tout élément non explicitement spécifié dans la présente charte qui relèverait des règles de sécurité ou de bon usage des systèmes d'information de l'Etat ne dépendant pas directement de la Direction des Services Judiciaires (bases lotus registre parquet général, courrier greffe général, enregistrement des sociétés greffe général, fiche de carrière...), il est nécessaire de se reporter à la charte des systèmes d'information de l'Etat, celle-ci ayant vocation à s'appliquer

de manière générale aux fonctionnaires et agents de l'Etat ayant accès aux ressources informatiques de l'Administration.

***2.2 Conditions d'utilisation***

L'utilisateur est responsable du bon usage du Système d'Information de la Direction des Services Judiciaires et s'engage à l'utiliser dans le respect des lois, des textes en vigueur et de la présente Charte.

Il ne doit en aucune manière se livrer à la consultation, au chargement, au stockage, à la publication ou à la diffusion de fichiers et de messages électroniques, dont le contenu présente un caractère injurieux, raciste, pornographique ou diffamatoire. Ceci s'applique tant aux sites et fichiers qu'aux messages électroniques, avec ou sans pièces attachées, ainsi qu'à toute forme de communication quelle que soit la forme des contenus (sonores, audiovisuels, multimédias ou logiciel).

Il doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents et les détruire en cas de réception fortuite.

Dans l'hypothèse où l'utilisateur recevrait des messages non sollicités, il lui appartiendra de les supprimer.

Si de tels messages provenaient régulièrement du même expéditeur, ou présentaient un caractère manifestement illicite, il appartiendra à l'utilisateur de prévenir l'Administrateur, afin que celui-ci puisse prendre les mesures d'exclusion technique nécessaires.

***2.3 Accès et identification***

Chaque utilisateur est doté d'un ou plusieurs identifiants auxquels sont associés un ou plusieurs codes confidentiels d'accès au Système d'Information de la Direction des Services Judiciaires, et aux équipements nomades ou non qui sont mis à sa disposition, tout comme n'importe quel matériel personnel de type ordinateur fixe, ordinateur portable, Smartphone ou tablette à partir desquels il serait possible de se connecter au Système d'Information de la Direction des Services Judiciaires.

Ces codes confidentiels, qui sont strictement personnels, ne doivent pas être divulgués, même à l'intérieur d'un service, ni conservés de manière permanente et facilement accessible par d'autres personnes.

Afin de protéger l'accès au Système d'Information et aux données, il est nécessaire de choisir et d'utiliser des codes confidentiels robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Les codes confidentiels doivent être complexes en comportant au moins neuf caractères au format alphanumérique de types différents (majuscules, minuscules, chiffres, caractères spéciaux) et être renouvelés tous les six mois.

Le système d'information est configuré pour rendre impossible l'utilisation des trois derniers mots de passe.

Les conditions d'accès peuvent varier selon les catégories d'utilisateurs; ils sont définis pour chaque catégorie par l'autorité hiérarchique compétente.

L'utilisateur s'interdit d'utiliser un identifiant autre que le sien.

***2.4 Mobilité***

Des ressources informatiques dites « nomades » peuvent être mises à la disposition de l'utilisateur par la Direction des Services Judiciaires.

Lorsque ces matériels sont utilisés à distance, l'utilisateur en assure la garde. Il assiste ou procède lui-même selon les cas à toutes les démarches (dépôt de plainte...) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

L'utilisation d'appareils nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcé. En cas d'incident avéré mais aussi en cas de doute sur une possibilité d'utilisation inappropriée du Système d'Information, il doit immédiatement en aviser l'Administrateur ainsi que sa hiérarchie.

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser les moyens techniques d'authentification, de restrictions d'accès, et de conformité d'accès, qui lui seront remis et aucun autre.

***2.5 Gestion des absences et accès aux systèmes d'information***

Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation du service, telles que définies par la hiérarchie et le cas échéant, avec le concours de l'Administrateur informatique habilité.

A cette fin, en cas d'absence, l'utilisateur doit mettre en œuvre l'une des procédures suivantes:

- le message d'absence, en précisant de préférence le nom de la ou des personne à contacter susceptible de le suppléer ainsi que l'adresse de la boîte mail du service, lorsqu'elle existe, pouvant recueillir les messages professionnels durant ladite absence;
- Le système de reroutage des messages, exclusivement vers un destinataire au sein du service ou vers la messagerie du service.

Par ailleurs, afin d'assurer le bon fonctionnement du service, en cas d'urgence ou de nécessité professionnelle, l'Administrateur informatique pourra être saisi par le chef de Service en cas d'absence de l'utilisateur, afin d'accéder directement, à l'aide du compte Administrateur, aux différents dossiers et répertoires stockés dans le Bureau Windows de l'utilisateur, courriers électroniques et plus généralement à tous documents à caractère professionnel de l'utilisateur.

***2.6 Protection de la propriété intellectuelle***

L'utilisation des systèmes d'information de la Direction des Services Judiciaires implique le respect des droits de propriété intellectuelle.

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

- utiliser les logiciels et applications, dans les conditions de la licence souscrite par la Direction des Services Judiciaires et l'Etat ;

- ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, ne pas tenter d'installer des logiciels pour lesquels la Direction des Services Judiciaires ne possèderait pas un droit d'usage ;

- ne pas reproduire et utiliser les bases de données, pages web ou autres créations de la Direction des Services Judiciaires et de l'Etat 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 diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet ;

- ne pas copier et remettre à des tiers des créations appartenant à des tiers ou à la Direction des Services Judiciaires sans s'assurer de l'autorisation du titulaire des droits qui s'y rapportent.

***2.7 Protection des informations nominatives***

L'utilisation du Système d'Information de la Direction des Services Judiciaires peut donner lieu à la mise en œuvre par la Direction des Services Judiciaires de traitements d'informations nominatives dans le respect des dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée.

L'utilisateur doit, dans l'exercice de ses fonctions, respecter les finalités de ces traitements d'informations nominatives et s'abstenir de communiquer des informations nominatives à des tiers extérieurs à la Direction des Services Judiciaires, sauf autorisation de sa hiérarchie et dans le respect des dispositions légales et réglementaires en vigueur.

Le cas échéant, conformément à la loi sur la protection des informations nominatives, les utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification des informations les concernant pour les données contenues sur le Système d'Information de la Direction des Services Judiciaires.

***2.8 Confidentialité des données***

La sauvegarde des intérêts et de la sécurité de la Direction des Services Judiciaires nécessite le respect, par l'utilisateur, d'une obligation générale et permanente de confidentialité laquelle résulte des devoirs généraux des magistrats, greffiers, fonctionnaires et agents de l'Etat en matière de secret professionnel, de discrétion professionnelle et de réserve inhérents à leur statut, à l'égard des informations ou données dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions.

Le respect de cette obligation implique notamment de : veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ou données ;

- n'accéder qu'aux informations en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations ou données réservées à d'autres utilisateurs;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve, de devoir de discrétion, de confidentialité en usage au sein de la Direction des Services Judiciaires.

L'attention de l'utilisateur est attirée sur les risques liés à la diffusion de contenus d'information et de données sur internet, en particulier au sein des réseaux sociaux et sur les blogs. Il est donc strictement interdit de diffuser la moindre information nominative, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de confidentialité, sur internet.

La diffusion de toute donnée ne peut être réalisée que dans les conditions dans lesquelles le magistrat, greffier, fonctionnaire ou l'agent non titulaire de l'Etat peut être délié de son obligation de discrétion professionnelle.

***2.9 Utilisation non-professionnelle***

L'utilisation du Système d'Information de la Direction des Services Judiciaires à des fins non-professionnelles doit être évitée dans toute la mesure du possible. Si elle doit avoir lieu, elle ne devra ni perturber le bon fonctionnement du service ou du Système d'Information, ni entraver aux règles d'utilisation du système d'information, telles que mentionnées dans la présente charte informatique.

A cet égard la consultation de sites internet à titre privé est tolérée dans la mesure où cette navigation n'entrave pas l'accès professionnel et qu'elle ne gêne pas de façon significative la bonne marche du travail de l'Utilisateur.

Il est précisé que le téléchargement ou l'utilisation en lecture continue (« streaming ») de fichiers musicaux ou vidéo ne rentrant pas dans l'accès professionnel est strictement prohibé en raison de l'encombrement qu'il génère.

Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par l'Administrateur. Celui-ci est habilité à imposer des configurations du navigateur et à limiter le volume des fichiers téléchargeables. De même, la taille, le nombre et le type des pièces jointes peuvent être limités par l'Administrateur pour éviter l'engorgement du système de messagerie.

Toute utilisation du Système d'Information de la Direction des Services Judiciaires à des fins lucratives est interdite.

Il est possible de créer un répertoire privé au sein du disque dur de l'ordinateur, sous réserve qu'il soit identifié sous le terme « privé » (avec une limite d'espace de stockage définie par l'Administrateur).

Concernant le système de messagerie une tolérance est possible à condition que le nombre et la taille des messages demeurent raisonnables et exceptionnels, pour cela le libellé « privé » doit être spécifié en objet de toute correspondance personnelle.

En outre, un répertoire nominatif est mis à disposition de chaque utilisateur sur le réseau du Palais de Justice. Ce répertoire ne doit toutefois pas être utilisé pour le stockage de données personnelles.

L'utilisateur s'interdit de copier depuis tout support numérique, quelques données que ce soient à destination de l'infrastructure informatique de la Direction des Services Judiciaires, sans qu'une procédure de vérification anti-virale ou anti-malware ou anti-x ait été préalablement réalisée par ses soins.

En cas d'infection du système d'information, l'utilisateur pourra être tenu pour responsable de la situation qu'il aura générée.

En tout état de cause la Direction des Services Judiciaires se réserve le droit de limiter ou suspendre la tolérance en matière d'utilisation non professionnelle en cas d'abus.

### *2.10 Messagerie*

Le Système d'Information de la Direction des Services Judiciaires est paramétré pour bloquer automatiquement les messages susceptibles de présenter un contenu technique dommageable (virus, troyen, ransomware...).

L'utilisateur conserve la charge d'éliminer les messages indésirables qui lui parviendraient (pourriels).

Il peut demander la mise en place d'un filtrage automatique plus restrictif, étant précisé que dans ce cas le risque de non-transmission d'un message utile ne peut être exclu.

En cas de réception d'un courriel suspect, l'utilisateur ne doit surtout pas cliquer sur une pièce jointe ou un lien piégé comme l'y invite le courriel mais informer rapidement le service informatique de la Direction des Services Judiciaires.

Ce risque doit particulièrement être pris en compte avant, pendant et après un déplacement à l'étranger lié à un évènement planifié où l'utilisateur peut être l'objet d'attaques ciblées.

## 3. CONFIDENTIALITE

### *3.1 Accès par les utilisateurs*

L'accès par les utilisateurs aux informations et documents conservés sur le Système d'Information doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

### *3.2 Accès par l'Administrateur*

L'Administrateur est soumis au secret professionnel sur les informations qu'il est amené à connaître en raison de ses possibilités d'accès au Système d'Information. Il ne peut en particulier communiquer, diffuser ou reproduire, par quelque moyen que ce soit, les données saisies, stockées, générées ou émises par un utilisateur, sous réserve des seules exceptions prévues au § 4.2 ci-dessous.

### *3.3 Départs des Utilisateurs*

Lors de la cessation de ses fonctions, l'utilisateur doit restituer en bon état général de fonctionnement, les ressources informatiques et de communication électronique qui lui ont été remises (ordinateurs, périphériques, mobiles, PDA, carte d'accès, moyens d'authentification à distance, badges, supports de stockage...).

Le compte messagerie de l'utilisateur est supprimé le jour de son départ. Toutefois, en cas de nécessité liée à la continuité du service, le contenu de la messagerie peut faire l'objet d'une conservation pendant une durée maximum de trois mois.

Les identifiants de l'utilisateur sont désactivés. Si l'utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage à le restituer.

L'utilisateur pourra, avant son départ, demander à l'Administrateur que lui soit remise une copie de sauvegarde de son courrier électronique personnel.

Cette copie est soumise à des limitations techniques quant au format dans lequel elle pourra être fournie.

Les documents privés doivent être supprimés par l'utilisateur au plus tard la veille de la cessation de ses fonctions.

Ces documents sont automatiquement supprimés dans un délai maximal de trois mois à compter du jour de la cessation des fonctions de l'utilisateur.

L'utilisateur pourra demander à l'Administrateur qu'il soit procédé à la destruction totale de ses données sans possibilité de récupération. Ces opérations auront lieu en la présence de l'intéressé.

***3.4 Sécurité et vigilance***

L'utilisateur s'engage à utiliser le Système d'Information de la Direction des Services Judiciaires de façon loyale et digne et à être vigilant en signalant toute anomalie ou intrusion.

L'utilisateur est tenu d'informer, sans délai, son Référent Informatique ou l'Administrateur de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter le Système d'Information.

L'utilisateur pourra être invité à prendre des mesures d'urgence ou de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

***3.5 Cyber sécurité en déplacement à l'étranger***

Lors de déplacement à l'étranger, l'utilisateur devra être vigilant à ne pas perdre ou compromettre les informations stockées sur son téléphone portable et son ordinateur portable. Il devra éviter de rapporter des fichiers de données ou des dispositifs externes et de les intégrer au Système d'Information de la Direction des Services Judiciaires au risque de compromettre le Système d'Information.

Il est recommandé de prendre contact avec le service informatique de la Direction des Services Judiciaires avant et après le déplacement à l'étranger.

Les conseils qui suivent visent à se prémunir contre de telles menaces.

Pour l'usage des téléphones portables, des mesures de précaution devraient être prises en considération avant tout déplacement :

Activer un mot de passe sur le téléphone et le modifier avant le déplacement puis une fois le déplacement terminé ;

- Conserver en tout temps son téléphone avec soi. Si cela n'est pas possible, retirer la batterie, l'extension mémoire et la carte SIM, et les conserver avec soi ;

- Désactiver la fonction Bluetooth ;

- Eviter d'utiliser un accès sans fil (Wi-Fi) pour se connecter à Internet. Des points d'accès gratuits peuvent être établis à des fins malveillantes et sont nommés intentionnellement de manière à donner l'impression de points d'accès de confiance, en particulier dans les lieux de passage (aéroports, gares, hôtels, …) ;

- Eviter de charger son téléphone en le connectant au port USB d'un ordinateur ou d'une borne non connus ou non fiables.

Pour l'usage des ordinateurs portables, des mesures de précaution devraient être prises en considération avant tout déplacement :

- Modifier le mot de passe de l'ordinateur portable avant le déplacement puis une fois le déplacement terminé ;

- S'assurer auprès du service informatique de la Direction des Services Judiciaires que les mises à jour logicielles qui s'appliquent au système d'exploitation et aux applications de l'appareil ont bien été réalisées ;

- Désactiver les connexions sans fil (Wi-Fi et liaison infrarouge) lorsqu'elles ne servent pas ;

- Eviter de connecter à l'ordinateur portable des appareils USB et des supports de stockage d'origine inconnue (exemple : clés USB remises à titre gratuit ou payées dans les frais de participation à un évènement) ;

- Eviter d'utiliser un accès sans fil (Wi-Fi) pour se connecter à Internet. Des points d'accès gratuits peuvent être établis à des fins malveillantes et sont nommés intentionnellement de manière à donner l'impression de points d'accès de confiance, en particulier dans les lieux de passage (aéroports, gares, hôtels, …) ;

- Utiliser le réseau opérateur pour toutes les connexions Internet depuis le téléphone mobile professionnel et établir, si nécessaire, un partage de connexion en faveur de l'ordinateur portable professionnel, plutôt que d'exploiter les moyens de communications locaux.

***3.6 Mesures d'urgences et plan de reprise d'activités***

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, la Direction des Services Judiciaires peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la reprise de son activité informatique et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené à la demande de la Direction des Services Judiciaires à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, le basculement sur un système informatique de relève, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information,

etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, déplacement sur des sites de secours tiers, etc.).

## 4. CONTRÔLE ET MAINTENANCE

### *4.1 Opérations de contrôle*

La mise à disposition et l'utilisation du Système d'Information de la Direction des Services Judiciaires impliquent nécessairement des opérations techniques de contrôle et de maintenance technique.

Le Système d'Information s'appuie sur des fichiers de relevés d'activités (" logs "), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Sont notamment journalisées et conservées les données relatives aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites internet ou le téléchargement de fichiers.

L'Administrateur est habilité à collecter, conserver et exploiter les informations nécessaires à la gestion du réseau (données de volumétrie, incidents, nature du trafic engendré) et à prendre toutes mesures en découlant pour la bonne marche des Ressources Informatiques.

Il est également habilité à communiquer ces informations aux tiers concernés, à l'exclusion de toute donnée nominative ou permettant une identification nominative, et du contenu de tout fichier et toute correspondance d'utilisateur.

### *4.2 Opérations de maintenance*

Les opérations de maintenance peuvent nécessiter l'intervention sur site, sous la responsabilité de l'Administrateur, des services techniques compétents.

Les opérations de maintenance sur site sont réalisées en présence de l'utilisateur.

Si celui-ci est empêché, il pourra donner autorisation expresse à l'Administrateur pour que les services compétents effectuent les opérations de maintenance hors sa présence, à charge pour l'Administrateur de prendre les précautions nécessaires pour assurer la confidentialité des données de l'utilisateur.

L'utilisateur devra être spécifiquement informé par l'Administrateur lorsque l'intervention est susceptible de donner lieu à modification des données lui appartenant ou à réalisation d'une copie de ces données sur un support extérieur aux terminaux en sa possession.

Les mêmes dispositions seront applicables en cas d'accès au répertoire nominatif mis à disposition de chaque utilisateur sur le réseau du Palais de Justice.

Aucune opération de « prise de main à distance» ou de consultation à distance d'un poste utilisateur ne pourra être effectuée autrement que pour des interventions d'aide et de support technique

***4.3 Mesures d'alerte***

Si à l'occasion des opérations de contrôle répertoriées au § 4.1, l'Administrateur constate une violation répétée des règles d'utilisation énoncées ci-dessus (§2.1 à 2.5 et 3.1), il alerte l'utilisateur concerné et lui seul sur les anomalies constatées. Le cas échéant, il l'informe de ce que ces agissements sont contraires à la présente charte et pour quelles raisons.

Dans le cas où les comportements perdureraient malgré cette mise en garde, l'Administrateur pourra, après en avoir averti l'utilisateur, limiter ou suspendre l'accès de celui-ci aux Ressources Informatiques, en informant de cette mesure les autorités hiérarchiques de l'intéressé.

Les présentes dispositions ne font pas préjudice aux règles pénales applicables dans le cas où serait constatée la présence d'un contenu illicite ou la commission manifeste d'une infraction.

Hormis ces deux cas de figure, aucune information personnelle ne sera communiquée, y compris aux autorités hiérarchiques de l'intéressé.

***4.4 Stockage et conservation des données***

Chaque utilisateur doit veiller à la conservation des documents électroniques en sa possession, en fonction des nécessités de son service.

Les données traitées par l'utilisateur doivent obligatoirement être stockées et/ou enregistrées sur les volumes réseaux mis à disposition par la Direction des Services Judiciaires. Ces espaces de stockage sont les seuls dispositifs techniques de stockage habilités à cette fin. Ceci afin que chaque collaborateur du Palais de Justice puisse disposer en temps réel et sans contrainte de dépendance d'un tiers, d'une information métier à un instant donnée.

D'autre part, seuls ces volumes seront éligibles à une procédure validée de sauvegarde et de restauration des données métiers.

Par ailleurs, la responsabilité de la conservation des données personnelles identifiées sous le libellé « privé » sur le système informatique de la Direction des Services Judiciaires, qui sont techniquement conservées sur le système d'information interne sous la seule et entière responsabilité de l'utilisateur, ne saurait être reportée sur l'Administrateur dans l'éventualité d'une perte de tout ou partie des fichiers personnels causée par un éventuel dysfonctionnement de l'infrastructure informatique de la Direction des Services Judiciaires.

***5 Entrée en vigueur***

La présente Charte figure en annexe de l'arrêté du Secrétaire d'Etat à la Justice Directeur des Services Judiciaires n°2022-07 et entre en vigueur à compter du lendemain de la publication au Journal de Monaco dudit arrêté.

*imprimé sur papier recyclé*

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO