Charte des usages numériques pour les utilisateurs des systèmes d'information de l'ENSOSP

Version 1.3	Octobre 2024
Rédaction	RSSI, DPO Acteam Conseil
Contributions	SG, SGA, DAAJ, DIP, DSIC Représentants des personnels
Validation	À faire valider en CSA du 05 novembre 2024

Table des matières

1 Préambule

L'Ensosp, en tant qu'établissement public national placé sous la tutelle du Ministère de l'Intérieur et des Outre-mer, emploie du personnel soumis à des statuts divers, et dans ses missions, accueille des stagiaires et intervenants.

Au travers des systèmes d'information et de communication de l'Ensosp, la sécurité et la prévention sont l'affaire de tous. La transformation digitale ayant accentué l'utilisation des services internet, des messageries électroniques, de la téléphonie et autres outils numériques, ces usages doivent faire l'objet d'un accord entre les différents acteurs.

L'objectif premier de cette charte d'utilisation des moyens numériques est de protéger les personnes et l'établissement des risques cyber qui peuvent se révéler dommageables pour les deux parties.
Les données professionnelles et personnelles ont une valeur monétaire sur des marchés parallèles et sont recherchées par des personnes mal intentionnées pour en faire le commerce. De plus, les attaques permettant de bloquer une institution contre, soit une rançon, soit l'aspiration de ses données, sont très répandues.

Cette charte représente un accord basé sur le bon sens entre l'Ensosp et les utilisateurs de son système d'information, pour que chacun puisse évoluer dans les meilleures conditions de vie au travail.

2 Contexte

L'Ensosp s'engage à fournir des moyens numériques fonctionnels et sécurisés. La mauvaise utilisation de ces moyens numériques génère des risques qui peuvent avoir une incidence sur le fonctionnement des services ou engager la responsabilité de l'établissement.

Ces risques peuvent être résumés ainsi :

- Atteintes aux droits de propriété intellectuelle ;
- Atteinte à la confidentialité, l'intégrité et à la disponibilité des informations ;
- Diffusion d'informations confidentielles ;
- Délits de presse (diffamation, propagation de fausses nouvelles, etc.) ;
- Atteinte au secret des correspondances ;
- Infractions au RGPD, notamment à l'obligation de sécurité des données ;
- Possession ou diffusion d'images à caractère pédophile ;
- Atteintes aux droits de la personne sur sa propre image ;
- Atteintes au droit au respect de la vie privée ;
- Utilisation des réseaux aux fins de réaliser le délit d'escroquerie, de menace.

L'Ensosp, en tant qu'employeur, peut être tenue pour responsable des actes des utilisateurs de ses systèmes d'information, quel que soit leur statut, dans le cadre de leurs attributions et de l'exécution de leur mission de service public.
L'établissement se doit d'informer les utilisateurs de ses systèmes d'information sur les conditions d'utilisation des moyens numériques mis à leur disposition.

De plus, la charte prévoit le contrôle par l'École nationale et par les personnes déléguées à ce contrôle : le plus souvent le (ou la) responsable de la sécurité des systèmes d'information (RSSI) et le (ou la) délégué(e) à la protection des données (DPO).

Les utilisateurs se doivent de respecter un code de bonne conduite basé sur la confiance et conforme à l'avis rendu par le comité social d'administration (CSA) : le respect de la présente charte, une fois adoptée, s'imposera à tous les utilisateurs quel que soit leur statut, dès lors que seront respectés les trois principes de base de la surveillance hiérarchique sur le lieu de travail : transparence, loyauté et mesure.

3 Champ d'application et dispositions

3.1 Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des personnels employés par l'Ensosp, incluant les élèves colonels, les stagiaires universitaires ou doctorants, les utilisateurs des systèmes d'information et de communication de l'établissement ayant une adresse@ensosp.fr. Nous les nommerons les « agents ».

Une partie de cette charte (paragraphe 8) s'applique spécifiquement aux agents de la division des systèmes d'information et de communication (DSIC) ayant des droits d'administration, en raison de leur rôle spécifique.

De même, cette charte s'applique à l'ensemble des prestataires du SI de l'École, quel que soit leur statut, et externes à l'École. Ainsi, cette charte doit être annexée aux contrats de prestations.

Les utilisateurs veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ilspermettraient d'accéder aux systèmes d'information et de communication.

3.2 Système d'information et de communication

Les systèmes d'information et de communication de l'Ensosp sont notamment constitués des éléments suivants : ordinateurs (fixes ou portables), périphériques (y compris clés USB), réseau informatique (VPN, serveurs, routeurs, connectique et Wi-Fi), copieurs, téléphones, smartphones, tablettes et clés 4/5G, logiciels, fichiers, données et bases de données, messagerie, connexion internet, intranet, systèmes de visioconférence…

Pour des raisons de sécurité, les matériels numériques personnels (smartphone, tablette, ordinateur portable…) ne sont pas autorisés à se connecter au réseau de l'Ensosp. Il est toutefois autorisé un accès à internet par un réseau Wi-Fi invité, une utilisation de la messagerie professionnelle ou de Microsoft Teams sur les smartphones personnels.

3.3 Généralités

L'utilisateur doit consacrer l'usage des ressources de l'Ensosp à son activité professionnelle. Conformément à la législation et à la jurisprudence, un usage personnel raisonnable, pour répondre à des nécessités de la vie courante et/ou familiale et restant conforme aux dispositions de la charte, est toutefois toléré.
Un outil professionnel se doit d'être utilisé de manière professionnelle. L'utilisation d'internet à des fins personnelles ne doit pas perturber le fonctionnement des ressources mises à disposition par l'Ensosp.

3.4 Condition d'accès aux ressources numériques

Le droit d'accès aux ressources informatiques, à la téléphonie et aux communications numériques est conditionné par le respect des termes de la charte. Ce droit est strictement personnel.

Chaque utilisateur accède aux différentes ressources par un système de compte nominatif offrant des droits d'accès individuels, composé d'un couple identifiant (ou login) mot de passe.

Chaque utilisateur est responsable de l'utilisation qui est faite de ses comptes d'accès aux différentes ressources numériques. Il est propriétaire de ses mots de passe qui sont personnels, uniques et confidentiels.
Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni personnel informatique sans engager la responsabilité du titulaire.
Dans la mesure du possible, ces informations doivent être mémorisées par l'utilisateur et ne pas être conservées, sous quelque forme que ce soit. En tout état de cause, elles ne doivent pas être transmises à des tiers ou aisément accessibles.

À l'exception des postes de travail en libre-service (salles de cours, de réunion, CRD), les utilisateurs devront utiliser uniquement les comptes qui leur auront été attribués. Ils ne doivent pas non plus déléguer à un tiers les droits d'utilisation qui leur ont été attribués.

Chaque utilisateur doit se conformer aux exigences de modification ou de mise à jour des mots de passe.
Automatiquement, il sera demandé à l'utilisateur de modifier son mot de passe à une fréquence régulière, avec application de règles de sécurité.

3.5 Verrouillage de sa session

En cas d'absence, même temporaire (quelques minutes), il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel. Pour mémoire, le poste se verrouille par la combinaison des touches suivantes : WINDOWS + L.

3.6 Installation de matériels et logiciels

Il est formellement interdit de copier les logiciels d'autres utilisateurs et d'utiliser des logiciels dont l'Ensosp n'aurait pas acquis les licences.
Seule la DSIC est habilitée à réaliser ou à déléguer toute installation de logiciel. L'utilisateur ne peut installer un logiciel (payant ou gratuit), que ce soit par copie ou téléchargement. En effet, l'installation d'un logiciel peut altérer le bon fonctionnement et/ou les performances du poste et/ou du réseau informatique. Son choix peut répondre à un besoin que la hiérarchie et la DSIC doivent pouvoir arbitrer en fonction des priorités ou des orientations de l'établissement.

Il est interdit de disposer sur ses outils professionnels de moyens de cryptographie ou de signature électronique à titre personnel.

3.7 Sécurité et usage des moyens de communication et des outils numériques

L'utilisation des ressources numériques est limitée aux activités professionnelles. Les usages personnels sont tolérés et sous la responsabilité de l'utilisateur.
Seules la DSIC et la direction de l'Ensosp sont habilitées à juger des écarts de conduite sur l'usage des ressources numériques et pourront le cas échéant limiter ou suspendre son usage personnel.

Chaque utilisateur doit personnellement contribuer à la sécurité des systèmes d'information de l'établissement. L'utilisateur doit signaler à la DSIC toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement.

3.8 Informations à caractère personnel

La création, l'utilisation ou le traitement de fichiers contenant des données à caractère personnel, faits en dehors d'un usage professionnel, sont proscrits. L'usage de données à caractère personnel doit se faire dans le cadre de la réglementation en vigueur (RGPD) et selon la démarche de conformité en vigueur à l'Ecole.

L'ensemble des données personnelles que l'utilisateur souhaite garder confidentielles, et dont il assume la pleine et entière responsabilité (notamment concernant les droits d'auteurs ou d'usages), doit être rassemblé dans des dossiers clairement identifiés comme personnels.

3.9 Déontologie - Éthique

Les règles d'éthique professionnelle, de déontologie, d'obligation de réserve, de devoir de discrétion en pratique dans les différentes activités exercées au sein de l'Ensosp s'appliquent à l'ensemble des ressources numériques mises à disposition ou produites par les utilisateurs. L'expression sur les médias et réseaux sociaux est soumise au devoir de réserve et de discrétion professionnelle.

Chaque utilisateur est personnellement responsable des ressources et données mises à sa disposition ou produites par lui-même dans le cadre de son activité professionnelle. Il doit respecter les dispositions légales, les dispositions de la présente charte et les procédures, consignes et contraintes techniques qui lui sont données, notamment par sa hiérarchie et la DSIC.

L'utilisateur doit mettre en œuvre toutes les mesures de protection qui lui sont préconisées, pour prévenir au mieux

des risques de vol, détérioration, déformation, dommage, indisponibilité des données et informations traitées.
L'utilisateur doit respecter les préconisations de cette charte afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord formel du supérieur hiérarchique et en respectant les règles de sécurité. En outre, l'utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Il doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils numériques, personnels ou appartenant à l'Ensosp, dans des lieux extérieurs à l'École nationale.
Pour plus de précision, voir l'engagement de confidentialité en annexe 1.

3.10 Télétravail

Le cadre de télétravail est défini par la charte spécifique en vigueur au sein de l'Ensosp.

- L'École fournit les moyens numériques à l'utilisateur en télétravail ainsi qu'une assistance technique si besoin
- En termes de logiciel, il n'y a pas de spécificité liée au télétravail
- Les télétravailleurs doivent utiliser leur équipement uniquement à des fins professionnelles
- Les télétravailleurs doivent respecter les bonnes pratiques de sécurité notifiées dans la présente charte

3.11 Absence

Les identifiants et mots de passe (session Windows, messagerie, Formaltis…) sont confidentiels et ne doivent pas être transmis ni à la hiérarchie, ni à des collègues. Par principe, l'École nationale respecte le secret des correspondances privées.
Toutefois, si un utilisateur absent détient sur son poste des informations indispensables à la poursuite de l'activité et en cas d'urgence, il sera mis en œuvre, avec son accord de préférence et celui de sa hiérarchie, les moyens permettant d'accéder à ces données.

3.12 Arrivée et départ d'un utilisateur

À son arrivée, tout utilisateur est informé des dispositions de la présente charte et se voit remettre les moyens et codes d'accès individuels nécessaires à l'accomplissement de ses fonctions. Il prend dès lors l'engagement, qu'à son départ de l'Ensosp, il rendra en ordre et en bon état l'ensemble des moyens mis à sa disposition.
À la discrétion de la direction, ces dispositions spécifiques de départ sont également prévues dans le cadre d'une absence longue prévisible ou programmée (congés parentaux, etc.) d'une durée à négocier au cas par cas.

3.13 Responsabilité de l'utilisateur

L'utilisateur est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler à la DSIC toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie. Sauf autorisation expresse du RSSI, l'accès au système d'information avec du matériel n'appartenant pas à l'École (smartphones ou ordinateurs personnels, supports amovibles…) est interdit.

Dans le cas où il a été autorisé, il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé.
En cas d'absence du bureau, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel.
L'utilisateur utilisera les supports de stockage sécurisés et sauvegardés proposés par le système d'information pour le stockage de ses données professionnelles. Il doit régulièrement supprimer les données devenues inutiles sur ces stockages réseau.
Les disques « locaux » d'un poste de travail (C:\ D:\...) ne sont pas sauvegardés, les données qui y seraient enregistrées ne relèvent pas de la responsabilité de la DSIC.

Les données anciennes mais qu'un utilisateur souhaite conserver doivent être archivées avec l'aide du service informatique et selon les préconisations d'archivage de l'Ecole.

L'utilisateur ne doit pas installer ou supprimer des logiciels, copier ou installer des fichiers susceptibles de créer des risques de sécurité au sein de l'Ensosp. Il ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre dans l'établissement.

3.14 Sécurité physique d'accès aux locaux

L'accès aux locaux techniques informatiques est soumis à autorisation (accès par badge ou clé). Si pour des raisons opérationnelles, un utilisateur doit avoir accès aux locaux techniques, celui-ci doit être accompagné par une personne habilitée de l'Ensosp (DSIC, DMGX ou agents de sécurité).
L'accompagnant de l'utilisateur doit s'assurer du bon déroulement de l'opération, rester à proximité et veiller à verrouiller le local après intervention.

3.15 Sanctions Applicables

Toute infraction aux règles présentées dans cette charte peut entraîner des sanctions disciplinaires et toute infraction à la loi peut entraîner des poursuites pénales et/ou civiles.

4 Dispositifs techniques particuliers

4.1 Internet

Accès aux sites web

L'utilisation d'internet à des fins personnelles est tolérée dans la limite du raisonnable et doit rester exceptionnelle. L'utilisation des médias et réseaux sociaux à des fins personnelles est à réduire au maximum.

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites web peut être limité ou prohibé par la DSIC qui est habilitée à imposer des restrictions et à installer des mécanismes de filtrage après validation du directeur de l'École ou de son représentant.

Seule la consultation de sites web ayant un rapport avec l'activité professionnelle est autorisée. En particulier, l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est aussi prohibé de créer ou mettre à jour au moyen de l'infrastructure de l'Ensosp tout site Internet, notamment des pages personnelles.

Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'Ensosp, ainsi qu'à ceux pouvant comporter un risque pour la sécurité des systèmes d'information de l'École ou engageant financièrement celle-ci.

Les utilisateurs doivent prendre connaissance que la plupart des sites internet conservent des traces des accès effectués.
Ces sites identifient précisément l'identité numérique du visiteur, ainsi que celle de l'Ensosp.

Sont notamment interdites les pratiques à des fins personnelles pendant les horaires de travail, comme :

- le téléchargement de logiciels,
- le téléchargement ou pratique des jeux,
- le téléchargement ou écoute de musique,
- le téléchargement ou visionnage de vidéos.

Sont également interdits : la consultation ou le téléchargement du contenu de sites à caractère pornographique, de même que de tout autre site portant atteinte ou contraire à l'ordre public et aux bonnes mœurs. L'accès à des sites illégaux revêt le caractère d'une infraction pénale.

Dans la mesure où des utilisations contrevenant aux règles ci-dessus énoncées, sont susceptibles d'engager la responsabilité administrative, civile et/ou pénale de l'Ensosp, outre bien évidemment celle de l'utilisateur, la direction

et la DSIC se réservent la possibilité d'exercer un droit de regard sur l'usage d'internet par les utilisateurs.

Autres utilisations

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs, réseaux sociaux n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie qui devra en informer la DSIC. Cela étant dit, la communication vers le public étant primordiale pour l'image de l'École, l'usage des réseaux sociaux ou tout autre moyen de toucher le cyberespace sont possibles. Tout cela reste soumis à cette charte et doit reposer sur le bon sens.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de l'établissement.

Ils sont informés que la DSIC enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de problématique de performance et de sécurité. La durée de conservation de ces traces, préconisée par la CNIL, est d'un an.

4.2 Usage de l'Intelligence Artificielle

4.2.1 Généralités

L'intelligence artificielle (IA) est un processus visant à simuler certains traitements de l'intelligence humaine : elle repose sur la création et l'application d'algorithmes exécutés dans un environnement informatique dynamique. Son but est de permettre à des ordinateurs d'imiter des raisonnements en se basant sur de l'apprentissage et en exploitant une grande quantité de données.

Des principes directeurs sont définis afin que l'emploi de Systèmes d'Intelligence Artificielle (SIA) à l'Ensosp respecte des usages sécurisés techniquement, juridiquement et d'un point de vue éthique.

L'Ensosp s'engage à respecter un ensemble de principes dans l'usage de ces technologies : la transparence vis-à-vis des utilisateurs, l'équité, la maîtrise humaine, la durabilité et la sûreté.

Les utilisateurs doivent également s'engager à utiliser les outils numériques mis à disposition par l'École, en respectant des consignes visant à favoriser des usages pertinents et sécurisés.

Ces principes directeurs seront détaillés dans une politique de gestion globale des SIA.

4.2.2 Mesures ENSOSP

4.2.2.1 Un cadre de confiance

Transparence :

L'École informera les parties prenantes à l'École (agents Ensosp, intervenants, stagiaires, etc.), dans un langage clair, de l'utilisation d'outils intégrant des processus d'IA (SIA).

Un document fera la synthèse des solutions et/ou des modèles d'IA employés, de leurs sources de données, des méthodologies utilisées et la manière dont elles peuvent intervenir dans les usages liés au fonctionnement de l'ENSOSP selon les orientations définies dans la politique évoquée ci-dessus.

Collaboration :

L'École favorisera, tout au long du cycle de vie d'un SIA la collaboration entre les diverses parties prenantes du processus pédagogique, en invitant, si nécessaire, des experts de diverses disciplines (droit, philosophie, sociologie, informatique, statistique notamment), pour partager les meilleures pratiques et promouvoir une gouvernance éthique de l'IA.

Formation :

L'École s'investira dans la formation et le développement des compétences de ses personnels afin qu'ils s'approprient les principes d'emploi d'une IA éthique et puissent travailler efficacement avec ces technologies.

Acteurs :
La DSIC, le RSSI, le DAAJ, la DPO et la DERE seront mobilisés pour une mise en œuvre dans le respect du cadre juridique applicable à l'École.

4.2.2.2 Une gouvernance adaptée à l'usage de SIA

Respect de la vie privée et des droits fondamentaux :

La DPO et le RSSI sont garants de la protection des données personnelles et sensibles en s'assurant que les SIA respectent la confidentialité et l'intégrité des informations traitées. De manière générale, et selon les contextes, la mise en œuvre d'un SIA doit respecter la dignité des individus et l'autonomie des utilisateurs.

Sécurité et fiabilité :

Le RSSI et la DPO sont garants de la suffisante sécurisation des SIA, de la fiabilité et robustesse face aux erreurs, aux manipulations et aux cyberattaques.

Durabilité et minimisation :

La future politique de gestion globale des SIA veillera à promouvoir une utilisation éthique des ressources dans le développement et l'exploitation des SIA, en tenant compte de leur impact environnemental. L'avantage du recours à un SIA par rapport à un algorithme classique ou une exécution humaine doit pouvoir être justifié.

4.2.3 Mesures utilisateurs

4.2.3.1 Utiliser un SIA pour un usage pertinent

Chaque utilisateur s'engage à ne pas utiliser des outils tiers (grand public ou non maitrisés par l'école nationale) basés sur de l'IA exfiltrant des données de l'école nationale. En effet ces outils peuvent s'approprier ces données et les conditions de leur réutilisation ne sont pas connues ni garanties. Il est interdit notamment de demander à ces moteurs d'IA d'analyser des données professionnelles ou de préparer des analyses en les contextualisant avec des éléments du domaine professionnel. Ces actions peuvent engendrés de la fuite de données

Le mode de communication de certaines IA prête à confusion, la conversation qui s'instaure avec la machine tendant à faire oublier qu'il n'y a pas d'interaction humaine. Il faut donc garder à l'esprit qu'une IA ne peut pas tout faire, et qu'elle ne sera performante que sur un périmètre défini de tâches :

- la traduction de textes (par exemple de l'anglais au français et vice versa),
- la production de textes, d'images ou de sons cohérents (mais pas nécessairement vrais),
- le résumé automatique de textes,
- l'amélioration de la qualité de rédaction d'un texte,
- la détection d'anomalies dans un texte (fraude par exemple),
- une assistance à l'idéation,
- l'analyse sémantique et la détection d'opinions,
- l'exploration de texte et l'accès au contenu.

4.2.3.2 Contextualiser au maximum son usage

En cas d'utilisation d'un SIA et afin de tirer parti au maximum d'un modèle de langage naturel, il est nécessaire d'échanger avec l'outil pour préciser au maximum ses instructions et ne laisser aucune zone d'ombre qui pourrait constituer une source d'erreur.
Il est généralement convenu que l'utilisateur doit :

- Donner un contexte à la machine,
- Lui adresser une tâche définie,
- Lui demander si elle a des questions complémentaires avant l'exécution de la tâche,
- Vérifier la bonne compréhension des consignes (par reformulation par la machine par exemple).

4.2.3.3 *Vérifier les résultats fournis*

Une intelligence artificielle n'est pas un moteur de recherche

Les IA peuvent générer un texte à la syntaxe et grammaire cohérentes sur la base d'interactions avec les utilisateurs. Les premières versions rendues publiques de ChatGPT n'effectuaient pas de recherche sur le web, mais, depuis la version 4, l'interface peut adresser une requête au moteur de recherche Bing si une question s'y prête.

Même si cette hybridation a probablement vocation à s'accentuer et à être de plus en plus invisible vu de l'utilisateur, les deux fonctionnalités conservent en leur cœur des modes de fonctionnement très différents. Les modèles de langage génèrent des réponses probables en composant des enchaînements de mots. Un moteur de recherche est conçu pour indexer des pages web et les hiérarchiser en fonction d'une requête. C'est ainsi qu'un modèle de langage peut produire des informations vraisemblables mais factuellement erronées, en « inventant » par exemple des sources scientifiques. Le moteur de recherche quant à lui affichera des liens vers des sources existantes, immédiatement accessibles et vérifiables par les utilisateurs.

La réponse apportée n'est pas issue d'une base de connaissance à proprement parler mais correspond à une production statistique. Il est possible qu'il y ait donc des biais orientant la perception de l'utilisateur.

4.2.3.4 *Protéger ses données personnelles*

Lors de l'utilisation d'outils SIA, les utilisateurs doivent veiller à ne pas divulguer de données personnelles à caractère sensible ou confidentiel, que ce soit dans les contenus générés ou dans les paramètres de configuration des outils.

4.3 Stockage, transport, sauvegarde et devoir d'archivage

Stockage et conservation

L'utilisateur doit conserver les fichiers et données nécessaires à son activité dans les espaces alloués à leur stockage et adaptés à leur sensibilité (lecteurs réseau prévus à cet effet, cloud, etc.). Des espaces de stockage sauvegardés sont mis à disposition des usagers par la DSIC.
L'utilisation de supports « physiques » autres (clé USB, disque externe...) doit être limitée au maximum, sauf nécessité et pour une durée limitée. Leur bon fonctionnement n'est pas garanti par la DSIC, leur contenu n'est pas sécurisé.

Déplacement

L'utilisateur qui transporte des fichiers et données professionnelles sur tout support de stockage (clé USB, ordinateur portable, disque dur externe, téléphone, etc.) doit particulièrement porter attention à la perte ou au vol de ce support, pouvant entraîner la communication à des tiers non autorisés de fichiers et données appartenant à l'Ensosp.

En cas de perte ou de vol, et dès constatation, l'utilisateur doit en informer rapidement et formellement sa hiérarchie et suivre cela d'un dépôt de plainte et d'une déclaration à la DSIC et au RSSI.

Sauvegarde et archivage

Les données professionnelles stockées aux emplacements alloués pour les utilisateurs sont sauvegardées automatiquement selon la politique de sauvegarde en application.
L'utilisateur doit également veiller à opérer un travail de tri et de classement de ses fichiers, notamment pour détruire les documents et données obsolètes qui surchargent inutilement les espaces serveurs.

Ce nettoyage s'applique aussi aux mails et fichiers attachés stockés dans la messagerie professionnelle, il revêt un caractère crucial en termes de développement durable.

4.4 Messagerie électronique

Usage de la messagerie

L'utilisateur peut disposer, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique

normalisée attribuée par l'Ensosp**.** Une liste des principales règles à respecter est rappelée et concerne : le comportement dans la communication, les actes illicites, l'engagement vis-à-vis des tiers, la conservation des courriels, la sécurité.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer la DSIC des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

Il est interdit d'utiliser la messagerie professionnelle pour s'enregistrer sur des plateformes de :

- Licences de logiciels non professionnels ou sortant du cadre de l'activité de l'Ensosp
- Inscription à des réseaux sociaux, forums et tout site sans lien direct avec l'activité professionnelle de l'utilisateur

Un guide d'utilisation de la messagerie électronique est en vigueur à l'Ensosp (voté en CHSCT du 18 mai 2021). Les utilisateurs se doivent de respecter son contenu dans l'usage quotidien de la messagerie.

Conseils généraux

L'attention des utilisateurs est attirée sur le fait que *« l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »* (Cf. article 1366 du Code Civil).
Un message électronique obéit donc aux mêmes règles qu'un courrier postal, en particulier en matière d'organisation hiérarchique.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants.
La forme de la signature professionnelle doit respecter les règles définies par la DSIC et le service communication.
En cas d'absence, l'utilisateur doit mettre en place un message de réponse automatique. En cas d'impossibilité, les administrateurs de la DSIC pourront être mandatés par les responsables de service pour mettre en place cette règle.
Pour des raisons de bon usage, l'envoi de messages électroniques vers un grand nombre de destinataires doit être réduit au maximum.
De même, la DSIC limite la taille des pièces jointes pour éviter l'engorgement du système de messagerie.

Utilisation personnelle de la messagerie

L'utilisation de la messagerie professionnelle à des fins personnelles est tolérée, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.
Les messages personnels envoyés doivent être signalés par la mention "Privé" ou "Personnel" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages personnels reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Personnel".
En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.
Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser une messagerie personnelle via une solution en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'Ensosp.

De plus, il est convenu de ne pas utiliser de messageries externes (Gmail par exemple) pour un usage professionnel.

Utilisation de la messagerie par les représentants du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention explicite (« RP » ou « OS ») dans leur objet à l'émission et dans le dossier où ils doivent être classés. Cela dit, les représentants des personnels doivent utiliser de manière privilégiée l'adresse générique fournie pour leur activité syndicale.

Départ

Lors du départ d'un utilisateur, la messagerie est conservée pendant une durée de 3 mois, sans que l'utilisateur ait accès à sa messagerie. À l'issue des trois mois, la boite est supprimée.

4.5 Les outils collaboratifs

L'Ensosp a mis en place Microsoft 365, dont l'outil collaboratif le plus utilisé est Microsoft Teams.
Teams est un espace de travail qui vise à faciliter la collaboration et la communication au sein d'une équipe, d'un projet, d'un établissement ou de tout autre groupe de personnes. Teams est un point d'accès unique pour les conversations, les visioconférences, les fichiers, les notes et les tâches.

L'utilisation de Teams, comme d'autres outils collaboratifs (Trello, Slack…), doit faire l'objet d'une attention particulière toujours basée sur le bon sens. En effet, le stockage des données n'est pas systématiquement localisé en France et peut parfois échapper à la réglementation sur les données à caractère personnel.

Les utilisateurs s'engagent à ne pas enregistrer et/ou diffuser les conversations avec ou sans vidéo sans l'accord préalable de toutes les personnes concernées.

L'Ensosp ne pourrait pas empêcher ces principes sans limiter les fonctionnalités de ces outils.
Il a été choisi de faire appel à la confiance et au bon sens des utilisateurs afin qu'ils soient vigilants lors de sessions collaboratives.

4.6 Téléphonie

Responsabilités

L'utilisateur qui se voit attribuer un téléphone professionnel doit répondre aux appels et consulter sa messagerie sur son temps de travail (activité normale, garde ou astreinte).

Analyse et contrôle de l'utilisation des ressources téléphoniques

Pour des nécessités de maintenance et de gestion technique des installations, l'utilisation des ressources téléphoniques peut être analysée et contrôlée selon le dispositif ci-dessous.
Les utilisateurs sont informés de l'enregistrement des informations suivantes :

- identité de l'utilisateur du poste : nom, prénom, numéro de poste
- communications téléphoniques : numéro de téléphone appelé, nature de l'appel (local, national, international), durée, date et heure de début et de fin de l'appel, nombre de taxes. Le traitement des informations collectées a pour finalité la maîtrise des dépenses téléphoniques, et l'établissement de tableaux de bord.

Dans la limite de leurs attributions respectives, ces informations peuvent être communiquées aux supérieurs hiérarchiques.

Les utilisateurs sont informés que la DSIC peut enregistrer leur utilisation de la téléphonie (hors conversation, données personnelles), aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi.

Toutefois, seule la DSIC pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur. En cas de différend, l'Ensosp pourra avoir recours au service « facturation détaillée » délivré par les différents opérateurs de télécommunication.
En cas d'usage abusif, l'employeur pourra exiger de l'utilisateur le remboursement du coût d'une ou plusieurs communications téléphoniques appréciées comme personnelles ou non conformes à son activité.

Il est également précisé que la dotation d'équipement mobile est adossée à la fonction occupée par l'utilisateur.

Chaque téléphone mobile affecté est configuré par la DSIC. L'utilisation de ces terminaux est prévue pour un usage professionnel. Ils peuvent être utilisés à des fins personnelles de manière raisonnée et avec bon sens. En cas d'usage ne respectant le cadre, la DSIC n'est pas responsable des dysfonctionnements.

Continuité de service

En cas d'absence d'un utilisateur, du fait du caractère professionnel présumé, un autre utilisateur peut répondre aux appels reçus et éventuellement traiter ceux-ci dans le cadre de ses attributions.

Utilisation personnelle de la téléphonie

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites des forfaits en termes de temps passé ou du type d'appels. Il s'agit tout particulièrement des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.
Les applications des différents « store » Android ou IOS pourront être installées sur le téléphone fourni (dans la mesure du raisonnable et de la légalité).

4.7 Les outils réseaux

Chaque utilisateur s'engage à :

- ne pas modifier la configuration des ressources (matériel, réseaux, etc.) mises à sa disposition,
- ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, chevaux de Troie, etc.),
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés,
- informer immédiatement la DSIC de toute perte, anomalie ou tentative de violation de ses codes d'accès personnels,
- effectuer une utilisation rationnelle et loyale des services et notamment du réseau, afin d'en éviter la saturation ou l'abus de leur usage à des fins personnelles,
- récupérer sur les matériels d'impression (imprimantes, matériels d'impression divers) les documents sensibles imprimés ou photocopiés.
- Ne pas jeter à la corbeille les documents professionnels confidentiels et utiliser les broyeurs papier.

5 Protection des données à caractère personnel

La notion de « données à caractère personnel » correspond à « toute information se rapportant à une personne physique identifiée ou identifiable ».

Un « traitement de données à caractère personnel » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement).
À chaque traitement de données doit être assigné un but, une finalité, qui doit bien évidemment être légale et légitime au regard de l'activité professionnelle de l'utilisateur.

Dans ce cadre, la législation en vigueur est le règlement général sur la protection des données (RGPD). Il existe au sein de l'ENSOSP une démarche globale qui permet de veiller au respect du RGPD, notamment par la désignation d'un DPO, qu'il est possible de contacter pour tout conseil à ce sujet (Cf. annexe 2).

Règlement général sur la protection des données 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.

6 Contrôle des activités

6.1 Contrôles automatisés

Les systèmes d'information et de communication de l'Ensosp s'appuient sur des fichiers journaux (logs), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques, sur les serveurs et le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'établissement, en détectant des dysfonctionnements et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant aux systèmes d'information.
La durée maximum de conservation de ces données est d'un an.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité des systèmes d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- 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 ou le téléchargement de fichiers ;
- aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activité et détecter des dysfonctionnements.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

6.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par la DSIC**,** il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de l'Ensosp, sur des systèmes collaboratifs ou sur sa messagerie.
Alors, sauf risque ou événement particulier, la DSIC ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à l'activité syndicale conformément à la présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé et éventuellement représenté par un représentant du personnel.

7 Comportement en cas d'incident

7.1 Vol ou perte d'une ressource

En cas de vol ou perte d'équipement informatique (ordinateur, téléphone, smartphone) fourni par l'École, l'utilisateur doit informer au plus vite son responsable hiérarchique et la DSIC (cf. annexe 2) puis leur communiquer :

- Les circonstances de la perte ou du vol, pour permettre à l'École de décider de porter plainte. Attention : l'utilisateur ne doit pas porter plainte en son nom ; seule une personne habilitée peut porter plainte au nom

de l'École,

- L'inventaire des données qui étaient présentes sur le matériel avec leur niveau de sensibilité et leur niveau de protection au moment de la perte ou du vol.

7.2 Infection ou intrusion sur le poste de travail

En cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité du SI de l'École (par exemple, une intrusion ou une infection par un code malveillant sur le poste de travail ou sur des ressources informatiques), l'utilisateur ne doit pas tenter de résoudre lui-même l'incident. Il doit prévenir la DSIC qui prendra les dispositions nécessaires pour confiner et traiter l'incident.

7.3 Dysfonctionnement d'un équipement

En cas de dysfonctionnement du matériel ou de non-respect des exigences précitées, une reconfiguration du système pourra être décidée. Le cas échéant, la DSIC réinitialisera l'équipement avec sa configuration initiale standard.

7.4 Respect du matériel

L'École fournit du matériel à l'utilisateur, pour l'exercice de ses fonctions. Il est de sa responsabilité de prendre soin du matériel qui lui a été confié.
De ce fait en cas de négligence flagrante ou de destruction volontaire du matériel, des sanctions pourront être prises par la direction de l'École à l'encontre de l'utilisateur.

8 Cadre du profil « agent DSIC »

Les utilisateurs sont informés qu'au sein de la DSIC, des agents formés ont accès en tant qu'administrateur à l'ensemble des systèmes d'information et de communication de l'Ensosp.

8.1 Champs d'intervention des administrateurs informatiques

Les administrateurs DSIC se distinguent des autres agents par les privilèges d'accès au sens informatique qui leur sont accordés sur les systèmes d'information et de communication. Ils disposent de droits d'administration nécessaires à la bonne réalisation d'actions d'administration. Un administrateur est une ressource critique investie de capacités techniques d'accès aux informations de l'entité.

Ils disposent d'outils permettant d'analyser et de contrôler l'utilisation des ressources numériques ainsi que les échanges via le réseau dans le strict cadre de leurs missions et dans le respect de la règlementation en vigueur.

Ainsi, en plus des obligations de confidentialité, les administrateurs informatiques sont soumis à des principes de loyauté, transparence et imputabilité.

8.2 Pouvoir d'alerte des administrateurs DSIC

Les agents DSIC ayant des droits « administrateur » sont tenus d'alerter formellement leur hiérarchie de tout problème pouvant affecter la sécurité des ressources numériques ou de l'École et en cas de constat de violation des dispositions de la présente charte.

8.3 Sécurité

L'Ensosp doit mettre en œuvre les moyens humains et techniques appropriés pour assurer la sécurité des systèmes d'information et de communication. À ce titre, il lui appartient d'identifier les limites d'accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle.
L'administrateur DSIC est responsable de la mise en œuvre et du contrôle du bon fonctionnement des systèmes d'information et de communication, il doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de sinistre majeur. Il veille à l'application des règles de la présente charte et à donner aux utilisateurs les moyens de respecter ces règles. Il est assujetti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

8.4 Engagement des administrateurs informatiques

Les administrateurs informatiques s'engagent à prendre toutes les précautions conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin de protéger la confidentialité des informations auxquelles ils ont accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.
Ils s'engagent en particulier à :

- Ne pas utiliser les données auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions,
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales,
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de leurs fonctions et traiter chaque copie avec le même degré de confidentialité que son original,
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données,
- Prendre toutes les précautions conformes aux usages et à l'état de l'art pour préserver la sécurité de ces données (notamment les journaux d'évènements),
- S'assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données,
- En cas de cessation de leurs fonctions, restituer intégralement les données, fichiers numériques et tout support d'information relatif à ces données,
- Alerter sans délai leur hiérarchie de toutes les anomalies mettant en jeu une problématique de sécurité (fuite de données par exemple).

9 Information et sanctions

La présente charte est annexée au règlement intérieur de l'ENSOSP, pour que chaque utilisateur en ait connaissance.

La DSIC est à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation des systèmes d'information et moyens numériques. Elle les informera régulièrement sur l'évolution des limites techniques des systèmes d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la DSIC dans le cadre de la présente charte.
En cas de besoin, les utilisateurs pourront être formés par la DSIC pour appliquer les règles d'utilisation des systèmes d'information et de communication prévues.

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie des systèmes d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits constatés. L'utilisation reconnue à des fins personnelles de certains services payants à travers les systèmes d'information de l'Ensosp donnera également lieu à remboursement de la part de la personne concernée.
Le directeur de l'Ensosp, ou son représentant légal, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

10 Entrée en vigueur

La présente charte est applicable à compter du moment où elle est remise à la personne, et que celle-ci signe l'accusé de réception.

Elle est adoptée après information aux Délégués du Personnel.

Annexe 1 : Engagement de confidentialité

Engagement de confidentialité pour les utilisateurs ayant vocation à manipuler des données à caractère personnel.

L'utilisateur s'engage, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

L'utilisateur s'engage en particulier à :

- Ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions,
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales,
- Ne faire aucune copie de ces données, sauf si ces copies sont nécessaires à l'exécution de ses fonctions,
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données,
- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données,
- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données,
- En cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de ses fonctions, demeurera effectif, sans limitation de durée après la cessation de ses fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

L'utilisateur a été informé que toute violation du présent engagement l'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Annexe 2 : Contacts DSIC (dont RSSI) et DPO

Comment contacter la DSIC ?

➔ Par téléphone

- En interne : 515
- De l'extérieur : 04 42 39 05 15

➔ Par mail

- assistance.dsic@ensosp.fr

➔ Accueil physique

- Bureau 0-41

  Du lundi au jeudi
  8h à 11h / 13h30 à 16h30

- Accueil de l'ENSOSP Aix

Comment contacter la DSIC pour les stagiaires ou prestataires externes ?

- Accueil de l'ENSOSP Aix

Comment contacter la DSIC pour les intervenants ?

- Service de la logistique et de la scolarité

Comment contacter le (ou la) DPO ?

➔ Par mail

- dpo@ensosp.fr

Annexe 3 : Dispositions légales applicables

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires.
Cette présente partie a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires dans le domaine de la sécurité du SI.

Textes législatifs

- **Code des relations entre le public et l'administration**
- **Code de la propriété intellectuelle**
- **Code de la sécurité intérieure**
- **Code pénal**
- **Code civil**

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.
Loi n°94-361 du 10 mai 1994 portant mise en œuvre de la directive (C. E. E.) n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle.
Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

Réglementation européenne

La convention européenne du 28/01/1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel.

- Elle définit les principes de base de la protection des données que les États doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les parties.
- Elle règle la coopération entre États pour la mise en œuvre de la Convention, en particulier l'assistance qu'un État partie doit prêter aux personnes concernées ayant leur résidence à l'étranger. Enfin, elle met en place un Comité consultatif chargé en particulier de faciliter et d'améliorer son application.

Le règlement (UE) 2016/679 du 27 avril 2016 dit règlement général sur la protection des données (RGPD), 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.