

## Délibération n° 2024-13 relative à la charte informatique

*Vu le code rural et de la pêche maritime, notamment l'article R812-7,*

*Vu le décret n° 94-1225 du 30 décembre 1994 portant organisation de l'Ecole nationale supérieure de paysage de Versailles,*

*Vu l'avis du comité sociale d'administration du 31 octobre 2023,*

### Le conseil d'administration décide :

#### Article unique

La charte informatique portée en annexe de la présente délibération est adoptée.

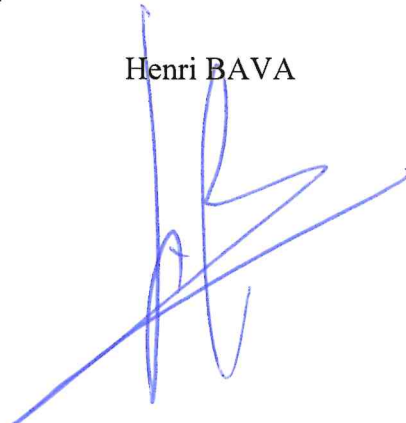
Favorables	25
Défavorables	
Abstentions	
Total votants	25

Fait à Versailles, le 14/03/2024

La délibération est approuvée / ~~rejetée~~

Le président du conseil d'administration

Henri BAVA



# Charte informatique

## Table des matières

---

<b>Préambule .....</b>	<b>3</b>
<b>Champ d'application .....</b>	<b>3</b>
Utilisateurs concernés .....	3
Système d'information .....	3
<b>Accès au système d'information .....</b>	<b>3</b>
Identifiants et droits d'accès .....	3
Politique des mots de passe.....	3
Usagers externes.....	4
Périphériques étrangers .....	4
Contrôle des accès.....	4
Procédure de contrôle manuel .....	4
<b>Poste de travail.....</b>	<b>4</b>
Généralités .....	4
Utilisation .....	5
Télétravail.....	5
Ordinateurs portables .....	5
Départ de l'agent .....	5
<b>Données.....</b>	<b>6</b>
Confidentialité et protection .....	6
Responsabilité .....	6
Accès aux documents .....	6
Espaces réseaux.....	6
Stockage sur internet.....	6
Documents personnels .....	6
Sauvegarde .....	7
Départ de l'agent .....	7
Collecte de données .....	7

<b>Messagerie .....</b>	<b>7</b>
Règles d'usage.....	7
Usage à des fins personnelles .....	7
Sécurité et filtrage.....	8
Accès suite au départ de l'agent .....	8
<b>Internet.....</b>	<b>8</b>
Règles d'usage.....	8
Usage à des fins personnelles .....	8
Contrôle.....	9
<b>Téléphonie .....</b>	<b>9</b>
Règles d'usage.....	9
Téléphones portables .....	9
<b>Reprographie .....</b>	<b>9</b>
<b>Cas particuliers .....</b>	<b>9</b>
Membres de la direction et chefs de service.....	9
Membres du service informatique .....	10
Représentants syndicaux.....	10
<b>Incidents .....</b>	<b>10</b>
Définition d'un incident de sécurité .....	10
Procédure .....	11
<b>Sanctions .....</b>	<b>11</b>
<b>Respect et législation .....</b>	<b>11</b>
Protection de la vie privée .....	11
Usage illicite de moyens .....	11
Protection des données à caractère personnel .....	11
Protection des données de santé .....	11
Protection des droits d'auteur et de la propriété industrielle.....	12
Protection des données statistiques.....	12
Cryptologie.....	12
Fraude et attaques informatiques .....	12
Numérique .....	12

# Préambule

---

Cette charte a pour objectif de définir le cadre d'utilisation du système d'information de l'ENSP. Elle définit les règles, droits et devoirs des utilisateurs (administratifs, enseignants et étudiants) dans l'exercice de leurs fonctions.

Elle définit un équilibre entre les impératifs de l'établissement et un usage responsable des ressources fournis aux usagers. L'ENSP s'engage à garantir la protection des informations, la sécurité et à respecter la vie privée des usagers.

Ce document s'applique en complément de la charte informatique du ministère de l'Agriculture et de la Souveraineté Alimentaire. Il peut être amené à évoluer en fonction du contexte législatif et réglementaire.

## Champ d'application

---

### Utilisateurs concernés

Sauf mention contraire, cette charte s'applique à l'ensemble des utilisateurs de l'établissement

- sans distinction de statut, grade, de fonction ou de rôle,
- quelle que soit son entité de rattachement et le statut de cette dernière,
- les prestataires doivent respecter la présente charte, et cette exigence doit être expressément prévue dans leurs contrats.

### Système d'information

Il est constitué

- des périphériques physiques permettant mis à disposition par l'établissement, qu'ils soient fixes ou mobiles,
- des informations véhiculées par le biais du réseau interne ou externe ainsi que le réseau téléphonique,
- des données stockées sur les serveurs ou contenues au sein des applications.

Cette définition s'applique quel que soit le lieu géographique où l'agent se trouve à partir du moment où il se connecte au réseau de l'établissement ou s'il utilise un périphérique fourni par l'ENSP.

## Accès au système d'information

---

### Identifiants et droits d'accès

Les identifiants permettant l'accès aux systèmes d'information de l'ENSP sont fournis à l'utilisateur par le service informatique lors de sa prise de poste.

Il est responsable de ces droits d'accès et doit assurer la protection des moyens d'authentification qui lui sont affectés

Cet accès est strictement personnel et incessible. Son propriétaire ne doit donc jamais :

- Communiquer son mot de passe à un tiers, y compris ses responsables hiérarchiques, ses collègues ou une personne du service informatique,
- Demander le mot de passe d'un tiers.

À ce titre, l'utilisateur est responsable de l'utilisation du système d'information réalisée avec ses droits d'accès.

L'utilisateur s'engage à ne pas tenter d'usurper l'identité d'autrui ni de cacher son identité dans le but d'accéder, modifier ou supprimer des données auxquelles il n'est pas habilité à accéder.

### Politique des mots de passe

Le choix d'un bon mot de passe est un élément essentiel dans la sécurité de l'ensemble du système d'information. Il assure à l'utilisateur la protection de ses informations :

- Il doit faire au moins 10 caractères,
- Il doit contenir au moins trois des différents types suivants :
  - Lettres en majuscule,
  - Lettres en minuscule,

- Chiffres,
- Caractères spéciaux.

Les mots de passe ne doivent pas être notés en clair sur une feuille, dans un cahier ou dans un fichier. Ils peuvent être stockés au sein de gestionnaire de mot de passes validés par le service informatique.

Les mots de passe auront une durée maximum de 6 mois.

Les 3 derniers mots de passe ne pourront être réutilisés.

## **Usagers externes**

Les usagers externes (visiteurs, intervenants, etc.) ont la possibilité de se connecter au réseau visiteur comme tout usager de l'établissement.

L'utilisateur s'engage à ne pas permettre à un prestataire d'intervenir sur ses outils de travail ou de connecter un périphérique extérieur sur le réseau administratif. Dans le cadre d'un besoin impératif, il contacte l'équipe informatique qui prendra les dispositions nécessaires dans le respect des procédures de sécurité.

## **Périphériques étrangers**

Seuls les équipements mis à disposition par l'établissement peuvent être connectés, de façon directe ou indirecte, au système d'information. L'utilisation de supports de stockage ou de périphériques USB de provenance inconnue est formellement interdite.

## **Contrôle des accès**

L'ENSP dispose de moyens permettant d'analyser et de contrôler de façon automatique et généralisée l'utilisation des ressources matérielles et logicielles ainsi que les échanges, quel que soit leur objet ou leur nature, effectués via les systèmes d'information de l'ENSP. Ainsi, les traces des actions des utilisateurs sont journalisées et conservées suivant les durées réglementaires sur des serveurs sécurisés.

Les contrôles mis en œuvre par l'ENSP sont réalisés :

- Dans l'objectif de garantir le bon fonctionnement technique et la sécurité des systèmes d'information,
- Dans le respect de la législation applicable, notamment la loi « Informatique et Libertés »,
- Exclusivement sous la responsabilité du responsable de la sécurité des systèmes d'information et des administrateurs des systèmes d'information qui gardent confidentielles les informations qu'ils pourraient être amenés à connaître.

Ces contrôles sont effectués afin de garantir le maintien en condition opérationnel, la sécurité du système d'information et détecter d'éventuelles anomalies.

### **Procédure de contrôle manuel**

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

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, les membres du service informatique ne peuvent ouvrir les fichiers identifiés par l'utilisateur comme personnels (contenus sur le disque dur de l'ordinateur mis à la disposition de l'utilisateur ou son dossier personnel stocké sur le serveur de fichiers du service) qu'en présence ou avec accord de ce dernier).

## **Poste de travail**

---

### **Généralités**

Le service informatique de l'ENSP configure le poste de travail avec un niveau de sécurité adapté. Il veille à installer les logiciels nécessaires à l'accomplissement des missions de l'agent auxquelles qui lui sont attribuées.

L'utilisateur devra utiliser les moyens de protection mis à sa disposition (câble antivol, rangements, etc.) pour garantir la protection des équipements qui lui sont attribués.

Aucun logiciel, hormis ceux installés dans le cadre de la réalisation des missions de l'agent ne devra être installé sur le poste de travail sans l'accord du service informatique.

L'utilisateur ne devra pas entraver l'installation de mise à jour sans quoi un processus les installera de façon automatique pouvant amener un redémarrage de l'ordinateur à des moments inopportuns.

## Utilisation

Pour garantir un maintien en condition opérationnelle de son poste de travail, l'utilisateur :

- ne doit pas modifier la configuration de son ordinateur,
- ne doit pas désactiver l'antivirus ou tout dispositif visant à le protéger,
- ne doit pas empêcher l'installation des mises à jours qui lui sont proposées,
- ne doit pas installer de logiciels non validés par le service informatique,
- doit éteindre son poste après son départ,
- doit se déconnecter des applications métiers lors des absences prolongées (repas...),
- devra verrouiller sa session lorsqu'il quitte son poste de travail, celle-ci sera automatiquement verrouillée dans le cas d'une inactivité supérieure à vingt minutes,
- doit ranger les périphériques éventuellement connectés.

Il est responsable de la protection des équipements mis à sa disposition et doit signaler le plus rapidement possible toute perte ou vol.

## Télétravail

L'utilisateur disposant d'un accès VPN veillera à ne se connecter à celui-ci que lorsque l'accès à une ressource est nécessaire. Lors de l'accès à une ressource tel qu'un logiciel métier avec un serveur interne à l'établissement ou un espace partagé.

Lorsque cette connexion est établie, l'utilisateur devra avoir une attention particulière sur ses usages.

L'usage du VPN est réservé aux ordinateurs administré par la DSI, il est interdit d'installer un client VPN sur un ordinateur personnel sans en demander l'accord au préalable.

Pour permettre des échanges fluides entre les agents en télétravail ou en présentiel, les outils mis à disposition pour les échanges (Softphone, application de visioconférence et de discussion instantannée – actuellement TEAMS, etc.) doivent être activés pendant les périodes de travail.

## Ordinateurs portables

L'utilisateur d'un ordinateur portable doit porter une attention particulière sur les risques de vol ou perte de son matériel entraînant une perte ou divulgation des données.

S'ajoute aux préconisations précédentes :

- l'interdiction de laisser un tiers utiliser son ordinateur,
- en dehors de l'établissement, veillera à utiliser au maximum la connexion partagée de son téléphone professionnel ou son réseau Wi-Fi personnel lors du télétravail,
- doit protéger son ordinateur d'un mot de passe à son allumage,
- doit chiffrer ses données,
- avoir une attention accrue sur le stockage de l'ordinateur en son absence.

Le réseau Wi-Fi de l'ordinateur devra être désactivé lorsque celui-ci sera relié au réseau de l'établissement afin de garantir un bon fonctionnement et une meilleure sécurité de son poste.

## Départ de l'agent

L'ensemble des équipements fournis par l'établissement doivent être restitués le dernier jour de l'agent auprès de la DSI.

Les données de l'agent se trouvant sur son poste de travail sont sauvegardées dans son espace réseau personnel suite à son départ (voir section Données). La session de l'utilisateur, ses données et ses paramètres sont alors effacés du poste.

# Données

---

## Confidentialité et protection

L'utilisateur doit adopter un niveau de protection en rapport avec la sensibilité de l'information (information non protégée, information en diffusion restreinte ou information confidentielle) et selon ses conditions de travail : dans son bureau, sur son poste de travail, hors de l'établissement avec des accès distants ou nomades.

## Responsabilité

L'utilisateur :

- assure la protection de ses informations, qu'elles soient sous forme numérique ou non, selon le devoir de réserve de tout agent au sein de la fonction publique,
- veille à ne pas mettre à la disposition de personnes non autorisées un accès aux systèmes d'information et à ne pas utiliser ou essayer d'utiliser des droits d'accès autres que les siens, en particulier l'accès physique au bureau. Une vigilance particulière doit s'exercer dans les entités accueillant du public ou partageant leurs locaux avec d'autres organismes,
- ne tente pas de lire, modifier, copier ou détruire des données ou documents autres que ceux qui lui appartiennent en propre ou pour lesquels il dispose du droit correspondant : lecture, modification ou suppression,
- garantit l'accès à ses données professionnelles, en cas d'empêchement ou de départ, en privilégiant systématiquement le stockage des fichiers d'intérêt général sur des répertoires partagés en réseau.

## Accès aux documents

### Espaces réseaux

Chaque utilisateur dispose :

- d'un espace réseau privatif dans lequel il peut stocker des données de travail sensibles ou temporaire qu'il estime ne pas devoir partager avec autrui. Il est interdit d'y stocker des données dont l'établissement peut avoir besoin en cas d'indisponibilité de l'agent..
- d'espaces réseaux collaboratifs dans lesquels les utilisateurs peuvent stocker et accéder aux données en fonctions des droits d'accès qui leurs sont accordés.

L'ensemble des documents produits dans le cadre de travail de l'agent doivent être stockés au sein du système d'information et doivent être accessible sur des ressources partagées si ces données comportent des informations pouvant être nécessaires au bon déroulement des missions de l'établissement dans le cas d'une absence.

Les documents stockés sur les espaces réseaux collaboratifs doivent être classés suivant une nomenclature en accord avec l'ensemble des utilisateurs ayant accès à cet espace.

Le cycle de vie des données, notamment l'archivage, doit être respecté afin de limiter le stockage de données obsolètes.

### Stockage sur internet

L'utilisation d'espaces de stockage en ligne de type Dropbox, One Drive, Google Drive, etc. est strictement interdit.

## Documents personnels

L'ensemble des documents se trouvant dans le système d'information sont présumés avoir un caractère professionnel.

Il appartient à ce dernier d'identifier les données personnelles en les stockant dans un répertoire intitulé "privé" ou "personnel".

En cas de circonstances exceptionnelles et d'absolue nécessité, il pourra être demandé à la Direction des Systèmes d'Information (DSI) d'accéder aux données d'un utilisateur en son absence. Une telle demande doit être écrite et signée d'un membre de la direction. L'objet de la recherche doit être précisé. A DSI accède aux données de l'utilisateur se fait en présence du chef de service demandeur et d'une personne tierce, à titre d'observateur. Cette mesure sera mise en œuvre conformément aux lois et réglementations en vigueur concernant la protection des données et la vie privée, et dans le respect des droits de l'utilisateur.

## Sauvegarde

Les espaces réseaux sont sauvegardés quotidiennement. Il est interdit de stocker des fichiers multimédias non professionnels.

Aucune sauvegarde du poste de travail n'est assurée, c'est pourquoi il est conseillé de stocker l'ensemble des données produites sur les espaces réseaux dédiés à cet effet.

## Départ de l'agent

Avant leur départ, les agents sont tenus d'effacer leurs données personnelles de leur espaces de travail.

Les données, donc professionnelles, de l'agent sont archivées durant trois ans mois après son départ. Après ce délai, celles-ci seront définitivement supprimées.

## Collecte de données

L'utilisateur ne collecte aucune donnée personnelle d'utilisateurs ou de toute autre personne hors de son cadre de travail.

La collecte de données personnelles ne peut se faire qu'après une déclaration du traitement auprès du Délégué à la Protection des Données (DPD) conformément au Règlement général sur la protection des données (RGPD) qui vérifiera la conformité du traitement.

Les données collectées sont traitées pour les besoins d'exécution des opérations sur les contenus du service. Cette utilisation repose sur l'un des fondements juridiques prévus par la loi soit :

- La protection des intérêts légitimes de l'ENSP,
- L'exécution d'un contrat conclu ou d'un engagement,
- Le respect d'une obligation légale ou réglementaire,
- La préservation de l'intérêt public.

Les données sont stockées et conservées pour la durée nécessaire à la réalisation des finalités visées.

## Messagerie

---

La messagerie électronique est l'un des moyens principaux de compromission du système d'information. De ce fait, il est indispensable pour les utilisateurs de porter une attention particulière à l'ensemble des emails qu'ils reçoivent.

## Règles d'usage

L'utilisateur :

- est responsable des messages émis avec son adresse,
- veille à ce que le message émis ne porte pas atteinte à la personnalité, à la vie privée ou à l'activité professionnelle d'aucune personne ou de l'établissement, qu'elle que soit son statut,
- ne stocke ni ne diffuse de messages ou de documents dont le contenu est réprimé par la loi,
- s'abstient de faire suivre des messages canulars,
- fait preuve de vigilance vis-à-vis de l'identité des auteurs des messages reçus,
- veille à la protection des informations diffusées par messagerie,
- ne doit pas transférer ses courriels vers une messagerie externe,
- n'utilise pas de messagerie personnelle à des fins professionnelles.

En cas de doute sur le contenu ou la provenance d'un courriel, l'utilisateur doit prévenir le service informatique qui se chargera de l'accompagner dans la vérification de la validité du courriel.

## Usage à des fins personnelles

La solution de messagerie fournie par l'ENSP est un outil de communication professionnelle. L'usage à des fins personnelles, ponctuelles et raisonnables est autorisé dans le respect de la loi.

L'ensemble des emails sont présumés avoir un caractère professionnel, par conséquent, une demande pourra être formulée auprès du supérieur hiérarchique de l'utilisateur pour obtenir un accès à certains éléments d'une boîte aux lettres. Cette intervention ne pourra avoir lieu que dans des situations exceptionnelles, en cas d'absence ou d'incapacité de l'utilisateur.



Il appartient à ce dernier d'identifier les données personnelles en les stockant dans un répertoire intitulé "privé" ou "personnel".

## **Sécurité et filtrage**

Les messages contenant des pièces jointes volumineuses sont susceptible d'être rejetés. Il vous appartient de les partager sur les espaces réseaux pour une diffusion en interne ou d'utiliser l'outil FILESENDER du service PARTAGE (Courriers électroniques gérés par le réseau RENATER). L'usage des autres services de transfert de données, tels que wetransfert, grosfichier.com ou autres sont interdits.

Les fichiers susceptibles d'exécuter du code potentiellement risqué (par les fichiers .exe ne sont pas autorisés à transiter par la messagerie, ils seront donc rejetés et un courriel d'information sera envoyé à l'émetteur.

Le service PARTAGE met en œuvre un système de filtrage limitant l'envoi et la réception de courrier indésirables. Une attention doit être apportée sur l'utilisation des termes sensibles employés pour éviter un filtrage aussi bien sur les dispositifs de protection du système d'information ainsi que sur celui du destinataire.

## **Accès suite au départ de l'agent**

L'accès à la messagerie de l'agent sera coupé 2 jours ouvrés après son départ. Toutefois, une dérogation peut être demandée au chef d'établissement. Si celle-ci est acceptée, alors l'utilisateur pourra continuer à utiliser la messagerie durant la durée définie, devra être attentif à toujours respecter les termes de cette charte et ne devra pas utiliser la messagerie dans un cadre extra-professionnel.

Avec l'accord de l'usager, sa boîte aux lettres pourra également être maintenue pour traiter d'éventuels messages qui pourraient lui être envoyés.

L'ensemble des données de la messagerie seront supprimées 36 mois après le départ ou la dérogation.

## **Internet**

---

### **Règles d'usage**

Au sein des locaux de l'ENSP, l'utilisateur ne doit accéder à internet que par une connexion fournie par l'établissement.

L'utilisateur :

- Ne doit pas communiquer ses informations professionnelles, sur des sites sans rapport avec son activité professionnelle,
- Ne doit pas intervenir sur les forums, blogs ou réseaux sociaux en indiquant son appartenance à un service de l'État sauf avec accord de sa hiérarchie ou dans le cadre de la communication de l'établissement,
- Ne doit pas faire usage de service de téléphonie par internet qui n'a pas été validé par le service informatique,
- Réserve la consultation de contenu vidéo et audio en temps réel (streaming) à un cadre professionnel.

### **Usage à des fins personnelles**

L'utilisation d'Internet à des fins personnelles est toléré dans le respect des règles mentionnées dans la présente charte.

Cette utilisation doit être raisonnable pour ne pas entraver l'utilisation professionnelle du système d'information et suivre les recommandations suivantes :

- l'utilisateur privilégie l'accès à Internet à des fins personnelles en dehors des plages à fort trafic sur le réseau, avant 9h00, de 12h30 à 14h, et après 17h30,
- il ne doit pas provoquer de surcharge réseau en téléchargeant des fichiers volumineux,
- il ne doit pas accéder à des sites illégaux et respecter la propriété intellectuelle en ne téléchargeant pas d'œuvres protégées par un droit de licence.

## Contrôle

L'ensemble du trafic est analysé par des procédures automatiques afin de protéger le système d'information contre d'éventuelles tentatives externes ou fuites d'informations.

Un système de filtrage bloque l'accès à des sites dont l'accès est prohibé (contenu illégal).

L'utilisateur ne doit pas essayer de contourner les protections mises en place par des systèmes de tunnel réseau ou proxy.

## Téléphonie

---

### Règles d'usage

Les personnes passant un appel depuis un téléphone appartenant à l'ENSP :

- sont responsables de tous les appels émis depuis celui-ci
- doivent le faire à des fins professionnelles,
- ne doivent pas appeler de numéros de téléphones entraînant un surcoût sauf en cas d'absolue nécessité,
- ne doivent pas prendre d'abonnement ou effectuer d'achat dont la facturation se fait sur facture téléphonique.

Le téléphone fourni par l'ENSP est un outil de communication professionnelle. L'usage à des fins personnelles, ponctuel et raisonnable est autorisé dans le respect de la loi.

### Téléphones portables

Les personnes dotées d'un téléphone portable devront :

- Sécuriser son accès par un mot de passe au minimum ainsi que son code PIN,
- Ne pas laisser à d'autres personnes l'usage du périphérique,
- Ne pas installer d'applications sans en informer le service informatique et sans en recevoir l'autorisation.
- Ne pas installer d'applications récréatives (TikTok, Instagram, Netflix...) selon les recommandations de l'ANSSI.
- Ne pas contourner le système de gestion des mobiles installés par la DSI.

L'utilisation de messageries instantanées, telles que WhatsApp, Messenger, ou tout autre service similaire, à des fins professionnelles est strictement interdite (car les données échangées ne sont pas sécurisées). Les communications professionnelles doivent être effectuées à travers les canaux de communication approuvés par l'ENSP.

## Reprographie

---

L'ENSP étant engagée dans une démarche de développement durable, l'utilisation des copieurs et imprimantes doit se faire de façon raisonnable et raisonnée.

Ainsi les impressions doivent se faire si possible en Recto/Verso en Noir et Blanc afin de limiter les déchets papier de l'établissement. L'impression ponctuelle à usage personnel est tolérée.

Les impressions contenant des données sensibles ou personnels doivent être protégées par un mot de passe.

## Cas particuliers

---

### Membres de la direction et chefs de service

Les membres de l'équipe de direction et chefs de service sont soumis aux mêmes règles que les autres utilisateurs.

Du fait de leurs responsabilités hiérarchiques, ils doivent :

- s'assurer que les droits d'accès attribués aux utilisateurs sous leur responsabilité correspondent à leurs missions,
- saisir leur autorité hiérarchique et avertir le service informatique en cas de manquement grave à cette charte informatique ou à un manquement grave des règles de sécurité,

- faciliter l'instauration de la culture de sécurité informatique et des bonnes pratiques par leur exemplarité.

En aucun cas, un supérieur hiérarchique n'est autorisé à consulter le contenu de la messagerie et les fichiers contenus sur les espaces dédiés à l'utilisateur sans accord explicite de l'utilisateur sauf cas particuliers définis par la loi ou urgence pouvant avoir des répercussions sur l'établissement ou un tiers.

## **Membres du service informatique**

Tous les membres du service informatique assurant des tâches d'administration sur le système d'information de l'ENSP sont tenus à un devoir strict de confidentialité et de discrétion.

- Les informations confidentielles auxquelles ils pourraient avoir accès au cours de leurs missions ne doivent être utilisées qu'à des fins de diagnostic ou d'administration du système dans le respect de la réglementation,
- Sauf cas particuliers définis par la loi ou urgence pouvant entraîner des répercussions sur l'établissement ou un tiers :
  - Ils ne doivent pas accéder ou tenter d'accéder à des documents ou messages personnels ne leur étant pas destinés sauf en présence de l'utilisateur propriétaire des données avec son autorisation explicite,
  - Ils n'autorisent aucun tiers à accéder à des données auxquelles il n'a pas accès,
  - Ils ne doivent pas chercher à accéder à une ressource à laquelle ils ne sont pas censés avoir accès sans l'autorisation expresse de l'utilisateur ou du chef de service responsable de la ressource.

Ils sont vigilants à ne pas abuser de leurs pouvoirs et privilèges sur les ressources informatiques de l'établissement.

Ils sont soumis à un devoir de discrétion quant aux données confidentielles ou personnelles dont ils pourraient avoir connaissance dans le cadre de leurs missions.

Ils ne doivent pas communiquer à des tiers des informations sensibles sur le système d'information sans l'autorisation du chef du service informatique.

## **Représentants syndicaux**

Les organisations syndicales et leurs représentants doivent préférer l'utilisation de leurs propres systèmes de communication lors de la diffusion de message.

Ils s'engagent à ne pas diffuser la liste des contacts des personnels de l'établissement.

Ils engagent leur responsabilité en cas de diffusion par l'intermédiaire des systèmes d'information de l'ENSP.

## **Incidents**

---

### **Définition d'un incident de sécurité**

- En cas de comportement anormal (au sens disponibilité, intégrité, confidentialité) du poste de travail ou d'une application utilisée,
- En constatant, la suppression ou la modification de fichiers,
- Une machine opère des actions non commandées, le système s'arrête et redémarre tout seul,
- En cas de constatation de comportements ou événements « suspects » : messagerie, vol ou perte de données, compromission de données personnelles ou confidentielles,
- Le logiciel antivirus ne répond plus, ou est désactivé,
- L'utilisateur a reçu un message d'un correspondant lui indiquant que ses emails étaient considérés comme indésirables par son système.

Tout individu peut être confronté à un incident. Il est important de souligner qu'un agent est vivement encouragé à signaler immédiatement et de manière explicite le problème au service informatique. Tout délai dans la notification pourrait engendrer des conséquences de plus en plus graves avec le temps.

## Procédure

L'utilisateur doit prévenir le plus rapidement possible le service informatique, idéalement par téléphone, par ticket au support ou par email à l'adresse [dsin@liste.ecole-paysage.fr](mailto:dsin@liste.ecole-paysage.fr).

L'utilisateur doit faire attention à ne pas mener d'action corrective afin de ne pas écraser certaines données ou informations permettant de déterminer la source de l'incident.

Le service informatique mettra en œuvre la procédure adaptée à la résolution du problème, pouvant aller de la restauration d'une sauvegarde à la déconnexion complète de l'infrastructure informatique de l'ENSP dans le cas d'une suspicion d'intrusion ou de propagation d'un programme malveillant.

## Sanctions

---

L'ENSP, représentée par sa Directrice, son secrétaire général et par son service informatique, se réserve le droit de vérifier, par tous les moyens dont il dispose, du bon usage fait de son réseau informatique en référence à toutes les recommandations édictées par les autorités ministérielles et la Commission Nationale Informatique et liberté (CNIL). Tout usager qui méconnaîtrait les règles définies par la présente charte, ainsi que celles relatives au code de la propriété intellectuelle ou aux recommandations émises par la CNIL, s'expose à des poursuites disciplinaires et judiciaires, en cas d'infractions pénales.

Le manquement aux règles et mesures de sécurité de 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 du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés. Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un utilisateur, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

## Respect et législation

---

Aux termes des articles L. 121-6 et L. 121-7 du code général de la fonction publique, « l'agent public est tenu au secret professionnel dans le respect des articles 226-13 et 226-14 du code pénal » et « doit faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions. En dehors des cas expressément prévus par les dispositions en vigueur, notamment en matière de liberté d'accès aux documents administratifs, il ne peut être délié de cette obligation que par décision expresse de l'autorité dont il dépend. »

### Protection de la vie privée

- Article 9 du code civil
- Article 226-1 et suivants du code pénal
- Article 226-15 du code pénal
- Article 432-9 du code pénal
- Article L. 34-1 et suivants du code des postes et des communications électroniques

### Usage illicite de moyens

- Article 227-24 du code pénal

### Protection des données à caractère personnel

- 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 (Règlement général sur la protection des données)
- Article 226-16 à 23 du code pénal
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

### Protection des données de santé

- Article L.1111-8 alinéas 1 et 2 du code de la santé publique
- Article L.1460-1 alinéa 1 du code de la santé publique

**Protection des droits d'auteur et de la propriété industrielle**

- Code de la propriété intellectuelle

**Protection des données statistiques**

- Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques

**Cryptologie**

- Loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique, article 29
- Article 230-1 du code de procédure pénale

**Fraude et attaques informatiques**

- Article 323-1 à 7 du code pénal
- Articles L. 2311-1 et R. 2311-1 et suivants du code de la défense (Protection des informations relevant du secret de la défense nationale)
- Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale
- Instruction interministérielle n°901 relative à la protection des systèmes d'informations sensibles
- Circulaire du Premier ministre du 17 juillet 2014 sur la politique de sécurité des systèmes d'information de l'Etat (PSSIE),
- Politique de sécurité des systèmes d'information du ministère chargé de l'agriculture
- Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité

**Numérique**

- Code des postes et des communications électroniques
- Code des relations entre le public et l'administration
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, notamment article 16