REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

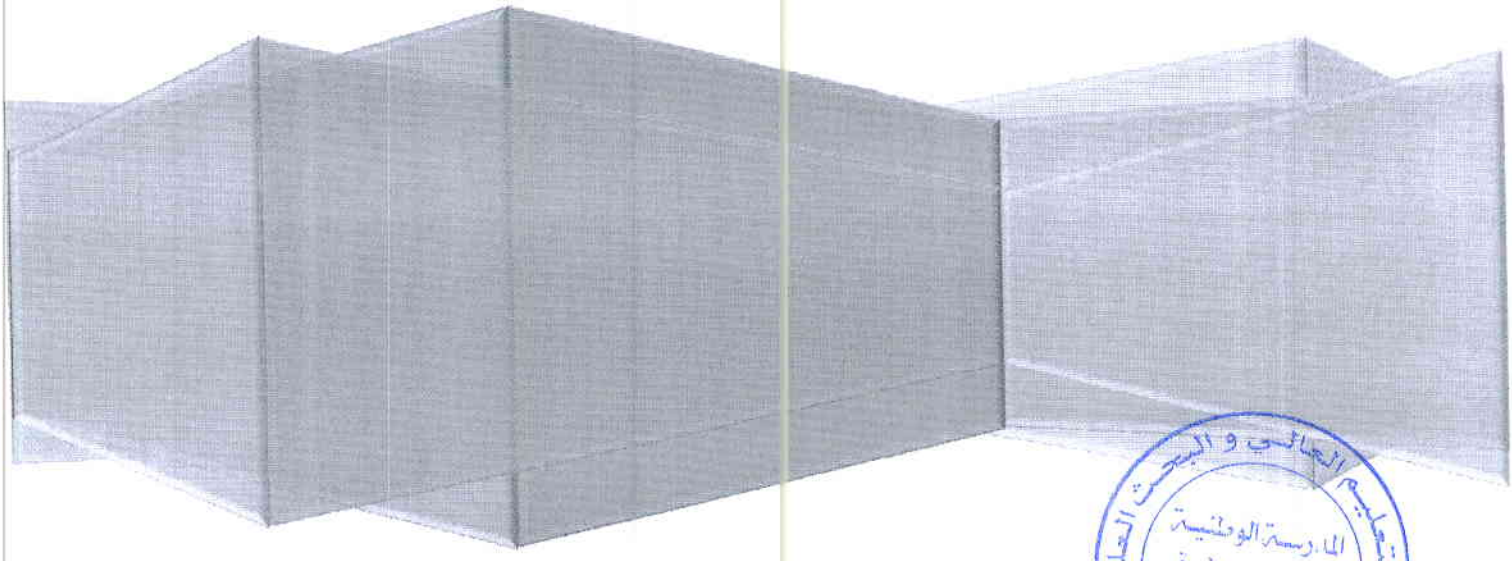
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE NATIONALE SUPERIEURE VETERINAIRE

Rabie BOUCHAMA

CHARTE INFORMATIQUE

Juin 2022



ENSV
ECOLE NATIONALE SUPERIEURE VETERINAIRE
ALGER

Charte informatique de l'Ecole Nationale Supérieure Vétérinaire

Table des matières

Introduction :

L'Ecole Nationale Supérieure Vétérinaire (ENSV) met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Elle met ainsi à disposition de ses collaborateurs et usagers des outils informatiques et des moyens de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation de ces outils informatiques et des moyens de communication de l'Ecole. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite.

L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'établissement. La charte est diffusée à l'ensemble des utilisateurs par tout moyen et à chaque modification. A ce titre, elle est disponible sur le site web de l'Ecole. Elle est systématiquement communiquée à tout nouvel arrivant.

Termes utilisés

- **Donnée à caractère personnel :** toute information relative à une personne identifiable sur un fichier qui comporte des informations permettant indirectement son identification : adresses postale et électroniques (mail, IP identification de la machine utilisée) ; numéro d'immatriculation identifiants de connexion, numéro de téléphone, numéro de sécurité sociale, photo, video, données de localisation... Une donnée à caractère personnel peut donc aussi être une donnée professionnelle.
- **Informations d'authentification :** identifiant, mot de passe … etc.
- **Information professionnelle :** information utilisée en contexte de travail. Repartie sur quatre types (publique, interne, confidentielle, secrète).

- **Équipements informatiques :** tous les équipements informatiques, de télécommunications et de reprographie de l'Ecole, statiques (Ordinateurs de bureau, imprimantes, scanners) ou mobiles (ordinateur portable, imprimante portable, tablette, téléphone mobile ou smartphone, objet connecté, CD ROM, clé USB, disque dur amovible etc…).
- **Site malveillant :** tout site Web conçu pour faire accomplir à un utilisateur légitime des actions indésirables ou néfastes pour la sécurité du SI.
- **Structure :** toutes les sous-directions, services, laboratoires de l'Ecole.
- **Système d'information (SI) :** ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications mis à disposition par l'Ecole.
- **Traitements de données :** opérations informatisées portant sur des données telles que l'ajout, modification et suppression des données.
- **Utilisateur :** toute personne autorisée à accéder et à utiliser les outils informatiques et moyens de communication de l'Ecole (enseignants, étudiants, ATS, intervenants extérieurs, visiteurs, invités, etc.).

Article I. Règles d'utilisation du système d'information

- Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès.
- L'utilisation de ces ressource doit être rationnelle, afin d'en éviter la saturation ou leur détournement à des fins personnelles;
- Tout utilisateur doit s'abstenir de nuire à l'image de marque de l'Ecole par une mauvaise utilisation des outils informatiques;
- Il doit suivre les règles en vigueur au sein de l'Ecole;
- Il doit choisir des mots de passe sûrs :
    - Ne pas les divulguer,

- Ne pas les écrire sur un document papier,
- Ne jamais les communiquer à un tiers,
- Ne jamais prêter son compte,

- Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité;
- Il doit protéger ses fichiers.
- Il lui appartient de protéger ses données et base de données en utilisant, régulièrement, les différents moyens de sauvegarde.
- Il ne doit pas laisser un document affiché sur l'écran de visualisation après exploitation.
- Il ne doit pas tenter de lire, modifié, copier ou détruire des données, sans qu'il n'y soit habilité.
- Il s'engage à ne pas mettre à la disposition d'utilisateur non autorisés un accès aux systèmes ou aux réseaux, à travers un matériel dont il a l'usage.
- Il doit respecter les modalités de raccordement du matériel au réseau de l'Ecole.
- Il ne doit, en aucun cas, déplacer le matériel et/ou modifier la configuration des systèmes, sauf s'il est habilité.
- Il ne doit pas quitter son poste de travail, sans fermer la session en laissant des ressources ou services accessibles.
- Il doit utiliser les guides utilisations du matériel informatique.

I.1. Utilisation professionnelle / privée

Il appartient à l'utilisateur de procéder au stockage et à la sauvegarde des données.

Les données privées de l'utilisateur ne doit pas occuper une part excessive des ressources.

L'utilisation de ces données ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement de l'établissement.

Cas particulier de l'utilisation de ressources informatiques personnelles :

L'utilisation de ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc… achetés sur des fonds personnels), au sein de l'école, ne doit pas affecter les politiques de sécurité de l'Ecole en raison d'une protection insuffisante ou une utilisation inappropriée.

I.2. Continuité de service : gestion des absences et des départs

Lors de son départ ou d'une absence prolongée, l'utilisateur doit remettre tous les documents professionnels (administratifs, recherche et pédagogiques…) à son responsable de structure ou lui permettre d'y accéder.

En cas d'indisponibilité de l'utilisateur, son responsable peut demander au service informatique de changer les paramètres d'accès au données de l'utilisateur en question afin d'accéder à tous les documents et informations professionnels (hors données privées).

L'utilisateur est responsable de la suppression des données privées.

Article II. Règles de sécurité

L'école met en œuvre les mécanismes de protection adaptés sur les systèmes d'information mis à la disposition des utilisateurs.

La sécurité des ressources mises à la disposition de l'utilisateur lui impose le respect des règles suivantes :

- appliquer la politique de gestion des mots de passe de l'ENSV ;
- garder strictement confidentiel ses informations d'authentification ;

- ne pas utiliser les informations d'authentification d'un autre utilisateur, ni chercher à les connaître ;
- ne pas enregistrer ses informations d'authentification sur des applications ou espaces non maîtrisés par l'école ;
- ne pas masquer sa véritable identité, ne pas usurper l'identité d'autrui
- ne pas accéder à des ressources du système d'information dont il n'a pas d'autorisation explicite ;
- ne pas se connecter à des sites Internet malveillants ;
- s'engager à ne pas apporter volontairement les perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations du matériel ou du logiciel ;
- verrouiller ou fermer toutes les sessions en cours sur son poste de travail, en cas d'absence, même momentanée ;
- s'assurer que toute personne externe susceptible d'accéder au Système d'Information de l'école y est autorisée par les responsables des services. Cette autorisation comprend l'engagement de respecter la présente charte.

- protéger les informations qu'il est habilité à manipuler dans le cadre de ses fonctions
- mettre en œuvre un système de sauvegarde manuel lorsque des sauvegardes automatiques ne sont pas prévues ;
- s'assurer que son poste de travail est verrouillé lorsqu'il s'absente de son bureau afin d'éviter les risques de vol de documents sensibles.

- ne pas modifier les paramétrages du poste de travail ;
- ne pas copier, modifier, détruire les logiciels propriétés de l'école ;
- respecter les dispositifs mis en place par l'école pour lutter contre les virus et les attaques par programmes informatiques ;

- ne pas désactiver, ni altérer le fonctionnement ou désinstaller l'outil de cryptage si il a été installé par l'école ;
- adapter la sécurité (physique et logique) des équipements mobiles en fonction de la sensibilité de l'information qu'ils traitent et stockent.
- Signaler le plus rapidement possible au service informatique tout logiciel ou dispositif suspect ainsi que toute perte, toute compromission suspectée ou avérée :
  - d'un équipement stockant des données professionnelles.
  - de ses informations d'authentification (identifiant, mot de passe, etc.).

L'utilisateur est informé que :

- l'école peut intervenir (y compris à distance) sur les ressources mises à sa disposition pour effectuer une maintenance corrective, curative ou évolutive.
- La maintenance à distance de son poste de travail est réalisée avec information préalable.

Article III. Outils de communication

III.1. Courrier électronique

La destination première du système de courrier électronique est exclusivement professionnelle. Il est toléré, toutefois, l'usage exceptionnel à des fins privées, à condition que cet usage soit occasionnel, n'entrave en rien la bonne conduite des affaires de l'institution ou la productivité.

- L'utilisation de cette adresse électronique relève de la responsabilité de son détenteur. Son utilisation est interdite sur des sites sans rapport avec son activité professionnelle.
- Une boite aux lettres électronique peut également être délivrée aux entités (laboratoire, services, directions...). Cette adresse doit aussi être utilisée dans un cadre strictement professionnel.

- Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'École.
- Un message électronique à la même portée qu'un courrier manuscrit. Il préférable de limiter l'envoi de messages non recommandés, afin de ne pas engager la responsabilité civile ou pénale de l'École et/ou de l'utilisateur.
- Les messages comportant des contenus à caractère illicite sont interdits (par exemple : les menaces, atteinte à l'honneur par la diffamation, par l'injure, …) quelle qu'en soit la nature sont .

En conséquence, l'utilisateur doit être vigilant sur la nature des messages électroniques qu'il échange. Le courriel est un document administratif reconnu en tant que preuve en cas de contentieux.

III.2. Internet

L'Ecole fournit aux travailleurs habilités l'accès à Internet à des fins professionnelles. Les règles suivantes doivent être, impérativement, respectées :

- L'utilisation d'Internet est limitée à des fins professionnelles. L'exploration d'Internet dans une optique d'apprentissage et de développement personnel est, toutefois, tolérée, mais ne doit en rien porter atteinte au bon fonctionnement du réseau ou à la productivité de l'employé.
- Si un système d'authentification pour l'accès à internet est mis en place, ce dernier ne peut se faire qu'en utilisant son propre compte (login / mot de passe). L'utilisation d'un autre compte n'est, par conséquent, pas autorisée.
- L'École se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités. Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'École.

- Les utilisateurs se doivent d'adopter un comportement loyal vis-à-vis de leur employeur lors de l'utilisation des réseaux sociaux, des blogs, (Facebook, Instagram, Twitter, Linkedin, autres sites).
- Le téléchargement doit être fait dans le cadre d'usages professionnels.
- L'École se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'École, codes malveillants, programmes espions…).

Article VI. Limitation des usages et sanctions

L'utilisateur est tenu de respecter l'ensemble des règles définies dans la présente charte.

Tout manquement à ces règles et mesures de sécurité et de confidentialité est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre :

- ❖ Des sanctions disciplinaires ou pénales en fonction de la gravité des faits constatés par les instances compétentes.
- ❖ Des poursuites ou procédures de sanctions peuvent être engagées à l'encontre de l'utilisateur malveillant.
- ❖ L'Ecole peut délivrer un avertissement, limiter ou suspendre les usages, sans préavis par mesure conservatoire..

Article V. Domaine d'Application

La présente charte s'applique à tout utilisateur du système d'information et de communication de l'Ecole Nationale Supérieure Vétérinaire quelles que soient ses activités.