Oran le …… /...../…….. *ENSO N°……*

CHARTE DE SECURITE INFORMATIQUEDE L'ENSO

L'Ecole Normale Supérieur AMMOUR Ahmed d'Oran (ENSO) met à la disposition des utilisateurs (enseignants – ATS) des moyens informatiques afin de leur permettre d'accomplir les missions qui leurs sont assignées. Une mauvaise utilisation de ces moyens augmente les risques d'atteinte à la sécurité des systèmes d'information de notre établissement.

Dans le cadre de la mise en place du référentiel national de sécurité de l'information, il a été décidé d'élaborer une charte de sécurité informatique afin de garantir un seuil minimal de sécurité.

Article 1 : Objet

La présente charte a pour objet de définir les conditions et modalités d'utilisation des ressources informatiques de ***« l'ENSO ».*** Elle définit également les règles de sécurité que les utilisateurs doivent respecter.

Article 2 : Champ d'application

La présente charte s'applique à toute personne ayant accès, de manière permanente ou temporaire, aux ressources informatiques de ***« l'ENSO »***.

Article 3 : de la propriété des ressources informatiques

- Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive de ***l'ENSO,*** il est donc strictement interdit de modifier ou supprimer ces ressource sans avertir le service informatique concerné ;
- Toutes les données hébergées (emmagasinées) dans les équipements (dispositifs) de ***L'ENSO*** ou transitant dans ses réseaux sont la propriété exclusive de ***l'ENSO***.

Article 4 : Conditions d'accès aux ressources et au réseau informatique

Tout accès aux ressources et réseaux informatiques de ***l'ENSO*** est soumis à uneprocédure d'authentification préalable.

Article 5 : responsabilité de l'utilisateur

L'utilisateur est seul responsable de toute utilisation des moyens d'authentification misà sa disposition par ***l'ENSO.***

Article 6 : protection des moyens d'authentification

Afin de préserver les moyens d'authentification mis à sa disposition, l'utilisateur doit :

- Veiller à la protection et à la préservation de ses informations secrètes d'authentification ;
- Changer périodiquement ses informations secrètes d'authentification ;

Il est strictement interdit de communiquer ses informations secrètes d'authentificationaux tiers (utilisateurs Enseignants et ATS).

Article 7 : Utilisation des ressources informatiques

- Les ressources informatiques de l'établissement ne peuvent être utilisées qu'à des fins professionnelles et ce après avis du service technique concerné ;
- L'utilisateur doit préserver les ressources et les moyens informatiques mis à sadisposition;
- L'utilisateur n'est pas autorisé à installer ou à déployer des applications ou des logiciels sur les moyens ou les ressources informatiques mis à sa disposition sans consulter le service technique concerné;
- En cas de défaillance de ces moyens ou de ces ressources, l'utilisateur doit informer immédiatement la structure en charge de la maintenance.

Article 8 : Obligations de l'ENSO vers les utilisateurs

L'Ecole Normale Supérieur AMMOUR Ahmed d'Oran(ENSO) doit :

- Mettre à la disposition de l'utilisateur les ressources informatiques nécessaires à l'exécution des missions qui lui incombent ;
- Garantir à l'utilisateur le bon fonctionnement et la disponibilité des ressources informatiques ;

- Maintenir la qualité du service fourni aux utilisateurs dans la limite des moyens alloués ;
- Tenir informer les utilisateurs des procédures et des politiques applicables en matière de
- ressources informatiques ;
- Mettre en œuvre les moyens nécessaires pour assurer la confidentialité et l'intégrité des documents et des échanges électroniques des utilisateurs ;
- Informer les utilisateurs que les activités sur le réseau et les systèmes font l'objet d'une surveillance automatisée ;
- Sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

Article 9 : Obligations de l'utilisateur

Respecter les lois et règlements en vigueur ;

- Respecter la présente charte ainsi que les différentes procédures et politiques de l'établissement ;
- Appliquer scrupuleusement les mesures et les directives de sécurité informatique de l'établissement ;
- Ne pas utiliser ou tenter d'utiliser les comptes d'autrui ;
- Signaler sans délai tout fonctionnement suspect ou incident de sécurité.

Article 10 : de la sécurité et de la protection du poste de travail

L'utilisateur doit respecter scrupuleusement les consignes de sécurité suivantes :

- Verrouiller l'accès au poste de travail en cas d'absence, même temporaire ;
- Alerter les services techniques en cas de découverte d'un nouvel équipement connectéau poste de travail ;
- S'assurer que son poste de travail dispose d'un antivirus, et informer le service concerné de toute alerte de sécurité (il est strictement interdit de désinstaller l'antivirus fournit par ENSO) ;
- Ne jamais connecté des équipements personnels au poste de travail ;
- Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser;
- Eteindre l'ordinateur pendant les périodes d'inactivité prolongée (nuit, weekend, vacances) ;

- Ne pas intervenir physiquement sur le matériel (entamer des opérations de maintenance auxquelles l'utilisateur n'est pas autorisé).

Article 11 : de l'utilisation de la messagerie électronique professionnelle

L'Ecole Normale Supérieur AMMOUR Ahmed d'Oran (ENSO) met à la disposition des utilisateurs des comptes de messageries électroniques (******@ens-oran.dz) qui leurspermettent d'émettre et de recevoir des courriers électroniques à caractère professionnel. La messagerie professionnelle ne peut être utilisée qu'à des fins professionnelles.

A cet effet, il est strictement interdit de :

- L'utiliser à des fins personnelles ou partisanes ;
- L'utiliser pour l'enregistrement sur les réseaux sociaux, les forums et les sites web ;
- Ouvrir les pièces jointes et/ou les liens hypertexte transmis à partir d'adresses mail inconnues ;
- Ouvrir la boite mail professionnelle à partir des espaces communautaires d'accès à internet notamment les cybers café ;

Lorsque les missions de l'utilisateur nécessitent son enregistrement sur les réseauxsociaux, les forums ou les sites web, une adresse mail dédiée à cet effet lui est attribuée après avis favorable de l'autorité habilitée.

L'utilisateur doit faire preuve de vigilance quant à l'utilisation des courriers électroniques et ceci en s'assurant que :

- L'adresse du destinataire est bien formulée ;
- Le destinataire est habilité à accéder au contenu transmis ;
- Les bonnes pièces jointes ont été rattachées au document.

Il est strictement interdit d'utiliser des adresses mails personnelles pour transmettre des documents professionnels.

Article 12 : de l'utilisation d'internet

Les utilisateurs ayant accès à internet s'engage à :

- Ne pas utiliser intentionnellement ce service à des fins malveillantes, obscènes, frauduleuses, haineuses, diffamatoires, pornographiques ou illégales ;
- Ne pas fournir des informations liées à leur fonction, grade ou responsabilité sur les réseaux sociaux
- Ne pas surcharger le réseau de l'établissement ;

Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de lesscanner par un antivirus.

Article 13 : des appareils mobiles et de supports de stockage

L'utilisateur doit :

- Signaler, à la hiérarchie dans l'immédiat, toute perte ou vol d'un appareil mobile ou support de stockage professionnel ;
- Verrouiller toujours les appareils mobiles lorsqu'ils ne sont pas utilisés ;
- Désactiver les fonctions Wifi et Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires ;
- Interdiction formelle pour toute personne étrangère à l'ENSO de transférer des documents par support amovible, tout échange de document doit se faire par courriel. Dans le cas où le volume de données exige le recours à un support amovible, ce dernier doit être analysé par les services compétents avant toute utilisation ;
- Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage ;
- Lors des déplacements professionnels, l'utilisateur doit garder ses appareils mobiles et supports de stockage amovible sur soi.

Article 14 : mesures de sécurité à appliquer lors des déplacements à l'étranger

- Il est interdit d'utiliser des terminaux (ordinateurs, tablettes, etc.) publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métier ;
- Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage ;

Le missionnaire doit désactiver de ses appareils, les fonctions de communication sans fil tel que le Wifi et le Bluetooth lorsque celle-ci ne sont pas nécessaires ;

- Le missionnaire doit supprimer toutes les données professionnelles sensibles, non nécessaire à la mission, de tous les supports amovibles avant tout déplacement à l'étranger ;
- Il doit informer la hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger ;

- Il est interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles ;
- Il doit mentionner dans les comptes rendus de la mission, la liste des objets connectés offerts lors du déplacement ;
- Il est formellement interdit qu'un transfert des documents par un étranger se fasse via des supports de stockage amovibles. Tout échange de document doit se faire exclusivement par courriel ;
- Le missionnaire doit changer les mots de passe utilisés pendant sa mission.

Article 15 : fin de la relation liant l'utilisateur à l'ENSO

- Lorsque la relation liant l'utilisateur à l'établissement prend fin, l'utilisateur doit restituer à l'ENSO toutes les ressources informatiques matérielles mises à sa disposition ;
- Le service technique concerné procédera à la suppression de l'ensemble des accès logiques de l'utilisateur aux ressources informatiques mises à sa disposition par l'ENSO.
- Le service technique concerné procédera à la restitution des accès aux différentes plateformes professionnelles (messagerie de l'école, plateforme Moodle, accès PROGRES, etc.)

Article 16 : gestion des incidents

En cas d'incident pouvant affecter la sécurité, l'ENSO peut :

- Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- Isoler ou neutraliser provisoirement toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information ;
- Prévenir le responsable hiérarchique.

Article 17 : du non-respect de la charte

Le non-respect des règles définies dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entrainer à son encontre des mesures disciplinaires proportionnelles à la gravité des faits constatés.

Sous réserve que soit informé le responsable hiérarchique, les responsables de la sécurité informatiques peuvent :

- Avertir un utilisateur ;
- Limiter ou retirer provisoirement les accès d'un utilisateur ;
- Effacer, comprimer ou isoler toute données ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information.

Sans préjudice des sanctions disciplinaire le contrevenant aux dispositions de laprésente charte peut faire l'objet de poursuites judiciaires.

Article 18 : entrée en vigueur

Cette Charte entre vigueur dès sa signature par l'utilisateur. Tout refus de signature interdira l'accès de l'utilisateur aux ressources informatiques de l'ENSO.

<table>
<tr><td colspan="2">L'utilisateur : ……</td><td rowspan="2">Signature (avec la mention « luet accepté)</td></tr>
<tr><td>Fonction :

……</td><td>Grade :

…….</td></tr>
</table>

Date et Visa du service administratif de rattachement