Note Importante :

La charte de bon usage des ressources informatiques, est une version simplifiée de la Politique de la Sécurité de l'Information et de plusieurs autres directives, procédures et support de formation et de sensibilisation en matière de sécurité informatique au sein de l'ENISo. Ce document et ses directives doivent être suivis et appliqués par tous les utilisateurs du système d'information de l'ENISO afin d'assurer une meilleure sécurité durant leur travail quotidien.

La sécurité, la protection des données et le bon fonctionnement du Système d'Information résultent d'une action à la fois individuelle et collective.

I. INTRODUCTION

I.1 ÉTENDU

1. L'Information dans toutes ses formes : données stockées, traitées, transmises sur des supports informatiques et documents.
2. Toutes les applications informatiques, logiciels et systèmes informatiques.
3. Tout le matériel, serveurs, postes de travail, ordinateurs portables, composants du réseau, appareils de communication et périphériques propriétés de l'ENISo.
4. Cette charte de bon usage des moyens informatiques s'applique à tout le personnel de l'ENISo.

I.2 CONFORMITE

Toute déviation de cette charte et qui n'est pas formellement autorisée par le Comité de la Sécurité de l'Information de l'ENISo, est considérée comme une violation et non-conformité qui peuvent engendrer des sanctions disciplinaires.

I.3 CONTACT

1. Toutes les questions concernant cette charte devraient être adressées au service informatique de l'ENISo.
2. Cette charte exige à chaque employé la déclaration et le signalement immédiat des incidents liés à la sécurité de l'information. Pour déclarer un incident ou violation de la charte, contacter le service informatique de l'ENISo.

I.4 BUT

Le but de ce document est de s'assurer que tous les utilisateurs de l'ENISo sont sensibilisés et conscients de leurs devoirs et responsabilités lors de l'utilisation quotidienne des moyens informatiques. L'ENISo se réserve le droit pour modifier ses politiques et directives lorsque c'est nécessaire. Dans ce cas, les utilisateurs de la politique seront informés.

2. Sécurité de l'Internet

2.1 L'internet et le courrier électronique doivent être utilisés principalement pour des besoins professionnels.

2.2 L'utilisation des proxys pour contourner les règles de sécurité de l'ENISo est strictement interdite **(Utraasurf, Hotspot…).**

2.3 Le téléchargement des utilitaires et des exécutables est autorisé qu'après une permission de l'équipe technique de l'ENISo.

2.4 Tous les utilisateurs doivent signer la présente charte.

2.5 Eviter d'envoyer de l'information confidentielle par e-mail sans l'utilisation de la technologie des cryptages et de signature électronique.

2.6 Il est strictement interdit, sauf autorisation préalable, d'utiliser les Clés 3G, Flybox ou autres technologies pour s'interconnecter au réseau Internet au sein du réseau de l'ENISo.

2.7 *Consignes à respecter lors de la réception de courrier :*

2.14.1 Il ne faut pas ouvrir des courriers suspects car ils présentent des risques notamment d'infection virale. Un courrier suspect est un message qui n'a pas de rapport avec votre activité normale, ou provient d'un émetteur inconnu, et/ou comporte un titre inhabituel.

2.14.2. Il ne faut pas ouvrir, enregistrer ou exécuter les pièces jointes suspectes. Ces dernières doivent être détruites immédiatement.

2.14.3. Il est important d'éviter de faire suivre un courrier créant ou perpétuant une chaîne (les courriers demandant une transmission à un grand nombre de nouveaux destinataires)

3. Gestion des mots de passe

3.1 L'usage des mots de passe Admin et root doit être limité aux administrateurs des systèmes autorisés. Lorsqu'il est possible, un compte Admin équivalent doit être créé pour l'utilisation quotidienne de l'administrateur, au lieu d'utiliser le mot de passe par défaut d'administration.

3.2 Les mots de passe doivent contenir au minimum 7 caractères alphanumériques, et ne doivent pas être semblables aux cinq mots de passe antérieurs. Ils doivent également suivre au moins trois des quatre combinaisons suivantes : petite lettre, lettre capitale, chiffre, et un caractère du contrôle "Non-alphanumérique" (aucuns narres communs ou expressions).

3.3 Les mots de passe de domaine Windows doivent expirer et être renouvelés chaque 90 jours. Un compte devra automatiquement être désactivé et bloqué si un utilisateur entre trois fois de suite des mots de passe invalides.

3.4 Les mots de passe doivent être gardés privés, non partagés, ou codés dans des programmes et ne doivent pas être divulgués à un collègue ou personne de l'équipe support de l'ENISo.

3.5 Les mots de passe par défaut doivent être changés pendant le premier login.

4. Protection des données

4.1 Chaque utilisateur est responsable des données stockées dans son ordinateur.

5. Installations des utilitaires sur les ordinateurs utilisateurs

5.1 Le service informatique fournit les logiciels et les applications dont l'utilisateur a besoin dans l'exercice de ses fonctions.

5.2 L'utilisateur ne doit pas effectuer des copies de logiciels afin de respecter les obligations en matière de licence et de propriété intellectuelle. Il doit se conformer aux restrictions d'utilisation des logiciels.

5.3 Les utilisateurs ne sont pas autorisés à installer des utilitaires, programmes et applications sur leurs postes de travail, sans l'autorisation préalable écrite du responsable de la sécurité informatique.

6. Sécurité des postes de travail des utilisateurs et Responsabilités

6.1 Les utilisateurs sont autorisés uniquement à utiliser des logiciels légaux, d'une source prouvée et doivent être approuvés par le responsable de Sécurité informatique.

6.2 Les utilisateurs doivent s'assurer que leurs données critiques et sensibles sont sauvegardées avec le serveur de backup de l'ENISo.

6.3 Les utilisateurs doivent s'assurer que leur PC/Laptop sont fermés lorsqu'ils ne sont pas utilisés, que les mots de passe sont activés dans les différents modes veille.

7. Jeux et Programmes d'écrans de veille

7.1 Les jeux informatiques et les utilitaires d'écrans de veille et de bureau sont reconnus comme une source de virus informatiques et leur usage est strictement interdit.

8. Outils de communication Peer-To-Peer et réseaux sociaux (facebook, twitte ,…)

8.1 L'utilisation des outils peer-to-peer (partage de disques) est strictement interdite.

9. Authentification

9.1 Chaque utilisateur aura une identification unique sur le réseau et les Systèmes d'information de l'ENISo.

9.2 Les partages des identifiants (login/mot de passe) utilisateurs avec les autres employés sont strictement interdites.

9.3 Les comptes utilisateurs et mots de passe partagés entre un ou plusieurs départements peuvent être permis seulement après justification détaillée et une approbation obtenue par le responsable sécurité de l'ENISo.

10. Autorisation

10.1 L'accès aux ressources informatiques et Systèmes d'information de l'ENISo sera accordé sur la base des exigences d'activité de l'utilisateur.

10.2 Une révision des droits d'accès Utilisateurs doit être effectuée avec le propriétaire du système au moins semestriellement.

10.3 L'autorisation d'accès devrait être retirée de l'utilisateur quand celle-ci n'est plus exigée.

10.4 Toutes les activités, y compris l'administration du système, doivent être exécutées avec les autorisations minimales exigées pour conduire l'activité.

10.5 Les abus des niveaux d'autorité ou l'accès à des informations professionnelles, ainsi que l'assistance à des personnes malveillantes, ne sont pas permis et sont considérés comme des attaques et des manquements sérieux aux obligations professionnelles.

10.6 Lorsque les employés quittent leur lieu de travail, ils doivent s'assurer que leurs postes de travail ont été fermés, ou utiliser des mots de passe sur les écrans de veille.

11. Démission et fin de contrat de travail

11.1 En cas de démission, de mutation, de départ à la retraite ou de fin de contrat d'un employé, notifié par le département de ressources humaines, les responsables informatiques doivent supprimer les droits d'accès de cet employer.

12. Utilisation des média amovibles

12.1 Seulement le personnel autorisé à installer ou à modifier les logiciels, pourra utiliser les médias amovibles afin de transférer les données au réseau de l'ENISo. Toutes les autres personnes doivent avoir des autorisations spécifiques.

12.2 Tous les médias de stockage de l'ordinateur (CD, DVD, Bandes, etc.) contenant de l'information sensibles seront étiquetés, protégés dans des emplacements sûrs. Les utilisateurs

qui ont besoin d'échanger des informations stockées sur des médias amovibles sont responsables pour la sécurité de leurs données.

13. Signalement des incidents de la sécurité de l'information

13.1 Les incidents de la sécurité de l'information devraient être rapportés, le plutôt que possible, à travers des canaux appropriés avec le responsable et les correspondants locaux de la sécurité. Les événements de violation des directives et politiques de sécurité doivent également être rapportés. Dans le cas où les directeurs ou les correspondants de sécurité ne seraient pas disponibles au temps de l'événement, les utilisateurs doivent rapporter l'événement au responsable de sécurité SI de l'ENISo.

13.2 Il existe un processus de réponse aux incidents, documenté afin de fournir l'assistance nécessaire et éviter les perturbations des activités de l'ENISo. Pour de plus amples informations, prière de consulter le document "Processus de gestion des incidents de la sécurité" sur l'intranet de l'IRESA.

13.3 Tous les employés, contractants, prestataires externes de service et tiers devraient rapporter les faiblesses de sécurité et failles constatées au sein de l'IRESA.

13.4 Tout le personnel est responsable de rapporter tout incident, virus, vol, action malveillante d'une autre personne, fraude ou tout autre acte malveillant

14. La politique du bureau 'propre'

Il est crucial de protéger l'information sensible de la divulgation. L'espace du bureau est fréquenté par des visiteurs, consultants, fournisseurs, personnel de nettoyage et d'entretien. Prière de garder votre lieu de travail propre. S'il y'a désordre, vous ne pouvez pas remarquer les documents manquants.

14.1 Préserver les documents sensibles et médias dans des coffres et armoires fermées à clé.

14.2 Les pcs portables doivent être de préférence attachés physiquement par des câbles sécurisés.

14.3 Sécuriser votre poste de travail en tapant : (Ctrl+Alt+Delete)

14.4 A la fin de la journée, prenez un moment pour ranger les biens sensibles et onéreux.

Fin des clauses de la charte

Date/ Signature de l'employé,