Charte Informatique

Les Amitiés d'Armor

Préambule

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de l'association Les Amitiés d'Armor, en particulier de préciser les responsabilités des utilisateurs salariés ou non de l'association. Elle vise à permettre un usage normal et optimal des ressources informatiques et des services internet.

Chaque nouveau membre du personnel de l'association se verra remettre un exemplaire de la présente charte contre émargement.

Cette charte sera annexée au règlement intérieur de l'établissement.

L'association met à la disposition de tout utilisateur des équipements informatiques, des moyens de communication, ainsi que des informations et données qui sont nécessaires à l'accomplissement de sa mission.
Le Directeur Général définit les conditions d'utilisation des systèmes informatiques de l'établissement et notamment les conditions d'utilisation des logiciels, d'internet et intranet.

Le Responsable des Systèmes d'Information (RSI) veille au respect et à la mise en œuvre de cette politique.

1. Définitions

On désignera sous le terme établissement, l'ensemble des établissements et services gérés par l'association.

On désignera sous le terme ressources informatiques :

- Les moyens informatiques matériels : serveurs, ordinateurs, imprimantes, et tout autre équipement informatique.
- Les logiciels, qu'ils soient sur l'ordinateur de l'utilisateur ou accessibles à distance sur les serveurs de l'association (Intranet, Osiris, EIG) ou autres serveurs externes (internet).

On désignera par services Internet, la mise à disposition de moyens d'échanges et d'informations diverses : Intranet, Web, messagerie.

On désignera sous le terme utilisateur, toute personne ayant accès ou utilisant les ressources informatiques.

On désignera par code utilisateur, tous les identifiants de connexion et les mots de passe (identifiant ordinateur et logiciel).

2. Respect de la confidentialité

1) Les utilisateurs ne doivent pas tenter de lire, de copier, de divulguer ou de modifier les fichiers d'un autre utilisateur sans y avoir été autorisés.
2) Les utilisateurs doivent s'interdire toute tentative d'interception de communications entre tiers.
3) Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne de l'Association qu'ils auraient pu obtenir en utilisant ces ressources informatiques.

3. Règles de sécurité

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et à celle de l'établissement.
L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier, l'utilisateur :

- s'engage à n'installer ni matériel, ni logiciel complémentaire sans l'accord **explicite du RSI.** Dans le cas contraire, ceux-ci pourront être désinstallés par ce dernier après information de l'utilisateur.
- s'engage à ne pas effectuer, de manière volontaire, des opérations pouvant nuire au fonctionnement du réseau de même qu'à l'intégrité des ressources informatiques.
  Toute clé USB introduite sur un système doit obligatoirement être vérifiée par l'antivirus installé sur le système.
- s'engage à ne pas modifier les paramètres matériels, systèmes ou applicatifs en dehors des procédures écrites par le RSI.
- ne doit pas enlever les étiquettes des équipements, procéder à des inscriptions ou coller des documents sur les équipements.
- doit choisir des mots de passe sûrs respectant les recommandations du RSI (cf. Annexe 2 : Choisir un bon mot de passe). Ces mots de passe doivent être gardés secrets, modifiés régulièrement et en aucun cas communiqués à qui que ce soit sauf autorisation expresse du directeur d'établissement.
- ne doit pas quitter son poste de travail sans verrouiller sa session utilisateur.
- doit signaler au service informatique ou à défaut le directeur de l'établissement ou son représentant toute tentative de violation de son compte, toute anomalie ou utilisation illicite qu'il peut constater.
- s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers les matériels dont il a l'usage.
- ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement.

4. Respect de la législation

L'utilisation des logiciels et plus généralement de tout document (fichier, image, son) doit se faire dans le respect de la propriété intellectuelle (loi 92-597 du 1er juillet 1992), des recommandations fixées par les détenteurs de droits et des engagements pris par l'Association.

En particulier, la reproduction de logiciels commerciaux est interdite. Une copie de sauvegarde pourra être autorisée par le RSI.

L'utilisateur doit s'imposer le respect de lois relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, ainsi que le respect des principes de neutralité religieuse, politique et commerciale.

Il est rappelé à ce titre, que la navigation sur des sites et/ou la sauvegarde de documents à caractère raciste ou pédophile est punissable par l'article 227-23 du code pénal.

5. Accès aux ressources informatiques et service internet

L'utilisation des ressources informatiques et l'usage des services internet ne sont autorisés que dans le cadre exclusif de l'activité professionnelle et sont soumis à autorisation préalable :

- Cette autorisation est concrétisée par l'attribution d'un identifiant ou d'un compte utilisateur. Ces accès sont précisés et accordés par le directeur de l'établissement.
- Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement, à un tiers et peuvent être retirées par les directeurs, notamment en cas de non-respect de la réglementation.

Est toléré l'utilisation privative des ordinateurs, notamment d'internet et des courriers électroniques, dans des limites raisonnables ne pouvant avoir des conséquences sur le travail et la bonne marche de l'association (Article 13, règlement intérieur).

<u>En particulier, l'utilisateur:</u>

- ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par le service informatique ou le directeur de l'établissement.
- doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier
- n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'association,
- ne doit pas télécharger des vidéos ou de la musique non autorisées.
- doit éviter toute activité fortement consommatrice en bande passante vers l'extérieur du réseau local pendant les heures de bureau (par exemple les transferts de gros fichiers et l'écoute de musique sur internet).

Le RSI pourra mettre en œuvre des moyens permettant :

- le filtrage de sites internet non autorisés par la Direction Générale
- l'interdiction de télécharger des logiciels
- le contrôle à postériori de données de connexion internet

6. Applications.

La présente charte s'applique à toutes les personnes amenées à utiliser des ressources informatiques mise à disposition par l'association (salariés, stagiaires, intervenant extérieurs).

L'Association ne pourra être tenue pour responsable des détériorations ou des manquements commis par un utilisateur qui ne sera pas conformé à ces règles. Tout manquement à ces stipulations engage la responsabilité personnelle de l'utilisateur, qui en assume les entières conséquences.

7. Consultation du Comité d'Entreprise.

Conformément à l'article 13 du règlement intérieur applicable au personnel de l'association, la présente charte a été soumise à la consultation du Comité d'Entreprise lors de sa séance du 20 mars 2015.

Annexe1 : Rappel des lois

Il est rappelé que toute personne sur le sol français doit respecter la législation française qui s'applique en particulier au domaine des technologies de l'information et de communication (TIC) :

- Le code du travail, le code civil
- La loi du 06/01/1978 dite *informatique et liberté modifiée par la loi du 06/08/2004* http://www.cnil.fr/
- La législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal) http://www.legifrance.gouv.fr
- La législation relative à la propriété intellectuelle http://www.legifrance.gouv.fr
- Les lois du 01/08/1986 et 01/08/2000 sur la communication Audiovisuelle et la liberté de communication
- La législation applicable en matière de cryptologie : http://www.telecom.gouv.fr
- La loi N°2002-303 du 04/03/2002 relative aux droits des malades et à la qualité du système de santé.
- L'article 227-23 du code pénal

Annexe2 : Choisir un bon mot de passe

Pourquoi choisir un bon mot de passe ?

Tout d'abord votre mot de passe est personnel et ne doit être divulgué à aucun tiers.
Il est aussi personnel que votre numéro de carte bancaire.
Pourquoi ? Parce qu'il permet de lire votre courrier électronique, d'envoyer des messages électroniques sous votre nom, d'y consulter vos informations personnelles, d'usurper votre identité sur le réseau informatique.

Retenez-le par cœur :

Votre mot de passe doit être difficile à trouver, mais facile à retenir :
Ne l'inscrivez nulle part. En particulier, ne le stockez pas dans un fichier électronique (fichier des paramètres de votre client de messagerie, fichier des préférences de votre navigateur favori), et n'activez pas l'option permettant d'enregistrer votre mot de passe.

Ce qu'il faut éviter :

Que votre mot de passe soit votre identifiant. Ça a l'air évident, mais ça arrive !
Le mot de passe ne doit pas être un mot concernant une donnée personnelle (votre nom, numéro de téléphone, votre code postal…) que l'on peut retrouver facilement. Le mot de passe ne doit pas figurer dans un dictionnaire (dictionnaire français, anglais, noms communs, nom propre…).

Choisir un bon mot de passe :

Un bon mot de passe doit faire au moins 8 caractères.
Il doit mixer un maximum de caractères différents : majuscules, minuscules, chiffres, caractères spéciaux (#{[\@%?...).
Il ne doit avoir une signification que pour celui qui l'a créé de façon à le retenir facilement.