# Charte informatique d'ANHIMA

Cette charte, annexée au règlement intérieur de l'unité ANHIMA/ UMR 8210, a pour objet d'informer les utilisateurs de leurs droits et de leurs responsabilités lors de l'usage des ressources informatiques et des services internet, en application de la Politique générale de sécurité de l'information (PGSI) du CNRS et de la législation.

Elle répond à la préoccupation d'ANHIMA de protéger les informations qui constituent son patrimoine immatériel contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité des systèmes d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique).

L'utilisateur contribue à son niveau à la sécurité des systèmes d'Information. À ce titre, il applique les règles de sécurité en vigueur au sein d'ANHIMA et signale tout dysfonctionnement ou événement lui apparaissant anormal.

ANHIMA met à la disposition de l'utilisateur les moyens nécessaires à l'application de la politique de sécurité des systèmes d'information.

À son niveau, le personnel d'encadrement favorise l'instauration d'une « culture sécurité » par son exemplarité dans le respect de cette charte et par un soutien actif du correspondant sécurité (CSSI) d'ANHIMA.

**Protection des moyens et droits d'accès aux informations**

L'utilisateur est responsable de l'utilisation des systèmes d'information réalisée avec ses droits d'accès.

À ce titre, il assure la protection des moyens d'authentification qui lui ont été affectés ou qu'il a générés (badges, mots de passe, clés privées, clés privées liées aux certificats, etc.).

L'utilisateur ne fait pas usage des moyens d'authentification ou des droits d'accès d'une tierce personne. De la même façon, il n'essaie pas de masquer sa propre identité.

L'utilisateur ne fait usage de ses droits d'accès que pour accéder à des informations ou des services nécessaires à l'exercice des missions qui lui ont été confiées et pour lesquels il est autorisé.

## Protection vis-à-vis des échanges sur les réseaux

L'accès au réseau se fait par le système informatique de l'INHA (voir charte informatique de l'INHA).

**Contenu des échanges sur les réseaux**

Les échanges électroniques (courriels, forums de discussion, messagerie instantanée, réseaux sociaux, partages de documents, voix, images, vidéos, etc.) respectent la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

**Vigilance**

L'utilisateur fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage, …).

**Protection vis-à-vis de l'accès aux services en ligne sur Internet**

L'utilisateur :

- évite de se connecter à des sites suspects ;
- évite de télécharger des logiciels dont l'innocuité n'est pas garantie (nature de l'éditeur, mode de téléchargement, etc.) ;
- n'opère les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des sites de confiance, mis à disposition par l'établissement et dont la sécurité a été vérifiée par l'établissement (via par exemple un audit de sécurité) ;

**Bibliothèque Gernet-Glotz**

Les usagers de la bibliothèque Gernet-Glotz devront respecter cette charte informatique. Celle-ci s'applique pour l'utilisation de tous les ordinateurs à disposition dans la salle de lecture.

**Services proposés par les tutelles**

Dans la mesure du possible les personnels utiliseront les services proposés par les tutelles tels que ceux-ci proposés par le CNRS :

- My Core pour le stockage et le partage de fichiers ;
- Une adresse de messagerie de son établissement de rattachement ;
- Hébergement de sites web.

**Hébergement**

Notre partenaire Huma-Num est l'hébergeur privilégié d'ANHIMA pour tous les projets numériques.

**Parc informatique – logiciels**

L'EHESS est en charge de la maintenance du parc des postes de travail d'ANHIMA sur le site de l'INHA.

Juin 2018