Charte régissant l'usage du Système d'Information

Adoptée par le conseil d'administration du 8 juillet 2022

Institut National
Universitaire
Champollion

Sommaire

Préambule

Afin de garantir la sécurité de son système d'information, l'établissement met en œuvre les principes de la politique de sécurité des systèmes d'information de l'État (circulaire du Premier ministre n° 5725/SG du 17 juillet 2014) : elle a pour objectif de définir un encadrement précis en matière de gestion de la sécurité des systèmes d'information des établissements, afin de permettre l'amélioration continue et de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des données contre les principaux risques pouvant impacter le système, tels que l'intrusion, l'altération des données, la divulgation ou les pertes des données et l'utilisation abusive des ressources informatiques.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte vient préciser les règles d'usage et de sécurité que l'établissement et l'utilisateur s'engagent à respecter : elle précise les droits et les devoirs de chacun.

Par l'intermédiaire du réseau de l'établissement, les utilisateurs ont accès à des réseaux extérieurs : réseau régional THD'OC[1], réseau national RENATER[2] et internet. L'utilisation du réseau RENATER est régie par une charte déontologique que l'Institut s'est engagé à respecter et à faire respecter par l'ensemble des utilisateurs.

Considérant les engagements de l'établissement :

L'établissement porte à la connaissance de l'utilisateur la présente charte. L'établissement met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'établissement facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'établissement est tenu de respecter l'utilisation résiduelle du système d'information à titre privé.

Considérant les engagements de l'utilisateur :

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents qu'il produit ou auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

L'utilisation des ressources qui sont mises à sa disposition doit être rationnelle et loyale afin d'en éviter la saturation ou le détournement à des fins personnelles.

Il est arrêté ce qui suit :

[1] **T**rès **H**aut **D**ébit en **OC**citanie

[2] **R**éseau **NA**tional de télécommunications pour la **T**echnologie l'**E**nseignement et la **R**echerche.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'établissement ainsi qu'à l'ensemble de ses utilisateurs.

Les usages relevant spécifiquement de l'activité des organisations syndicales ne sont pas régis par la présente charte mais font l'objet d'une charte spécifique.

Ces règles s'appliquent à toute personne autorisée à utiliser les moyens informatiques de l'établissement, y compris les moyens informatiques mutualisés ou externalisés, et s'étendent aux réseaux extérieurs accessibles par l'intermédiaire des réseaux de l'établissement.

Article II. Définitions

Système d'Information : s'entend de l'ensemble des ressources (réseaux, matériels, logiciels, données et processus) mis en œuvre par l'Institut pour collecter, stocker, traiter et diffuser l'information. L'ensemble des éléments nomades (ordinateurs et téléphones portables) sont également des éléments constitutifs du Système d'Information.

Utilisateur : Le terme « utilisateur » recouvre toute personne, quel que soit son statut, ayant accès dans le cadre de ses activités aux ressources du Système d'Information de l'Institut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire de l'Institut concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche ;
- tout étudiant inscrit à l'Institut ;
- tout personnel hébergé par l'Institut ;
- toute personne agissant dans le cadre d'une convention ou d'un contrat pour l'Institut, ainsi que les tiers qu'elle a sous sa responsabilité ;
- toute personne extérieure à l'Institut accédant une ressource publique sous le contrôle de l'Institut (sites web, helpdesk etc.).

Les exploitants et gestionnaires informatiques : le Système d'Information de l'Institut est géré par la Direction du Système d'Information et des Usages du Numérique (DSIUN).

La DSIUN gère l'infrastructure technique (réseaux et serveurs, bases de données) et est également en charge de la sécurité physique et logique de l'infrastructure (sécurité des accès, des données et des échanges).

Elle assure l'administration et le fonctionnement des applications et des bases de données administratives (scolarité, ressources humaines, finances) en garantissant leur confidentialité, leur l'intégrité et leur disponibilité.

Elle administre les comptes, les réseaux et serveurs locaux ainsi que les postes des utilisateurs. Elle n'intervient que sur les ordinateurs et matériels qui sont propriétés de l'Institut. Sa responsabilité est limitée à ces équipements. Elle assure un service de proximité aux utilisateurs dans le respect de la vie privée de chacun.

Article III. Protection des données

L'utilisateur est responsable de ses données professionnelles, ou de celles auxquelles il a accès dans le cadre de ses fonctions. Il doit en particulier s'assurer de la sauvegarde de ses données, et être vigilant sur les droits d'accès qu'il donne aux autres utilisateurs sur celles-ci.

L'utilisateur doit assurer la protection des informations sensibles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité) ; il doit notamment éviter de les communiquer ou les transporter sans protection (chiffrement) via des supports non fiabilisés (messagerie, clés USB, ordinateurs portables, disques externes, etc.) et ne pas les déposer sur un serveur externe ou ouvert au grand public.

Article IV. Conditions d'utilisation du Système d'Information

4.1 Autorisation d'accès

Toute utilisation du Système d'Information est soumise à une autorisation d'usage personnelle, temporaire et incessible, accordée par le Directeur de l'Institut. Cette autorisation est matérialisée par des identifiants ("login" et mot de passe).

Les utilisateurs sont responsables de toute utilisation faite à partir de leurs identifiants. Il leur appartient de veiller au choix, à la qualité et à la confidentialité de leur mot de passe.

L'autorisation d'accès sera retirée à l'utilisateur dès lors que sa qualité ne le justifie plus, dans un délai raisonnable lui permettant notamment d'effectuer la sauvegarde ou la destruction de ses données privées :

- Trois mois après la fin de l'inscription administrative d'un étudiant ;
- Deux mois après le départ d'un utilisateur géré ou hébergé par l'Institut (fin de contrat ou changement d'établissement par exemple) ;
- Le lendemain du départ d'un utilisateur non géré ou non hébergé par l'Institut (personne invitée, lecteur autorisé par exemple).

L'autorisation d'accès pourra être également retirée, par mesure conservatoire du Directeur de l'Institut, si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

4.2 Finalité d'utilisation

L'utilisation des ressources informatiques est limitée aux missions de l'établissement et aux besoins de l'activité qui en découle, soit :

- la formation initiale et continue, la recherche scientifique et technologique, la diffusion et la valorisation de ses résultats, l'orientation et l'insertion professionnelle, la diffusion de la culture et l'information scientifique et technique, la participation à la construction de l'Espace européen de l'enseignement supérieur et de la recherche et la coopération internationale (article L123-3 du code l'éducation) ;
- la vie universitaire et l'activité syndicale.

4.3 Utilisation professionnelle / privée

L'utilisation du système d'information de l'établissement a pour objet exclusif de mener des activités de recherche, d'enseignement, de documentation, d'administration ou de vie universitaire. Sauf autorisation, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'établissement ou des missions confiées aux utilisateurs. Ils peuvent néanmoins constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans son volume ou dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

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

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée, quel que soit le support (ordinateur, clé USB, téléphone…) ou le service (espace de stockage, messagerie…) utilisés.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource[3]. La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace. En cas de décès de l'utilisateur, ses espaces privés seront effacés.

L'utilisation du système d'information à titre privé doit respecter la réglementation en vigueur.

En particulier, la détention, diffusion et exportation d'images à caractère pédophile[4], ou la diffusion de contenus à caractère raciste ou antisémite[5] est totalement interdite.

Par ailleurs, eu égard à la mission de l'établissement, la consultation de sites de contenus à caractère pornographique depuis les locaux de l'établissement, hors contexte professionnel, est interdite.

4.4 Continuité de service - gestion des absences et des départs

Afin d'assurer la continuité de service, l'utilisateur doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe. En tout état de cause les données non situées dans un espace identifié comme privé, sont considérées comme appartenant à l'établissement qui pourra y accéder librement.

[3] Pour exemple, en indiquant "_privé_" dans le nom de l'espace ou de la ressource.
[4] Article L 323-1 et s. du Code pénal
[5] Article 24, 26bis, 32 et 33 de la Loi du 29 juillet 1881

En cas de départ, ou d'absence prolongée, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. Ces modalités respectent les règles de sécurité énoncées au paragraphe 5.1.

Article V. Principes de sécurité

5.1 Règles de sécurité applicables

L'Institut met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité du système d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ; chaque utilisateur est responsable de l'utilisation qui en est faite.
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.
- de veiller à ne pas laisser son poste de travail en libre accès.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

de la part de l'Institut :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de continuité du service mises en place par la hiérarchie;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

de la part de l'utilisateur :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'établissement ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance[6], ou sans autorisation de l'établissement ;

[6] Site de l'éditeur, ou plateformes reconnues de logiciels libres.

- se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les attaques par programmes informatiques ;
- s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou du logiciel ;
- veiller à protéger les matériels mis à sa disposition contre le vol et les dégradations ;
- appliquer les recommandations sécurité de l'établissement.

5.2 Devoirs de signalement et d'information

L'utilisateur doit avertir le responsable de la sécurité du système d'information (RSSI) dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il signale également à son responsable ou sa hiérarchie toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

Dans l'hypothèse d'une perte ou d'un vol des données d'identification (login et mot de passe) ; l'utilisateur doit en informer sans délai le RSSI et son supérieur hiérarchique.

5.3 Mesures de contrôle

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'établissement se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée ;
- que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que :

- ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ;
- elles ne mettent pas en cause le bon fonctionnement technique des applications ou leur sécurité ;
- elles ne tombent pas dans le champ de l'article[7] 40 alinéa 2 du code de procédure pénale.

Article VI. Communications électroniques

6.1 Messagerie électronique

[7] Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'établissement.

6.1.1 Adresses électroniques

L'établissement s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'établissement.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'établissement : ces listes ne peuvent être utilisées sans autorisation.

6.1.2 Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[8] ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus…) pourront être déployées.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques…).

Les échanges électroniques (courriers, forums de discussion, etc.) se doivent de respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées[9] est interdite sauf dispositif spécifique agrée et la transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée.

[8] Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message

[9] II s'agit des données classifiées de défense qui couvre le « confidentiel défense », le « secret défense » et le « très secret
défense »

6.1.3 Émission et réception des messages

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

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

L'utilisateur veillera également à n'utiliser que les outils fournis ou autorisés par l'établissement pour la gestion de sa messagerie. Tout recours à des prestataires extérieurs[10], notamment grand public, pour l'émission, la réception ou le stockage de message est interdit dans le cadre professionnel.

L'utilisateur envoie ses messages à destination de groupes de personnes grâce aux listes de diffusion institutionnelles dès lors qu'elles existent pour l'usage considéré ; il privilégie les adresses fonctionnelles aux adresses nominatives.

6.1.4 Statut et valeur juridique des messages

D'après le code civil[11], l'écrit électronique a la même force probante que l'écrit sur support papier, les messages électroniques échangés avec des tiers peuvent donc, au plan juridique, former un contrat[12].

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

6.1.5 Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte.

6.2 Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension Intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'établissement.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques ou de recherche). Si une utilisation résiduelle privée, telle que définie au paragraphe 4.3, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'établissement sont présumées avoir un caractère professionnel.

[10] Sauf les prestataires des partenaires institutionnels et les outils explicitement autorisés.
[11] Articles 1366 et 1367 du code civil
[12] Articles 1174 du code civil

6.2.1 Publication sur les sites Internet et Intranet de l'établissement

Tout site web doit préciser les mentions légales et en particulier le directeur de la publication et le respect des dispositions en matière de protection des données personnelles. Toute publication d'information sur les sites Internet ou Intranet de l'établissement doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé sur les ressources du système d'information ou de l'institution n'est autorisée, sauf disposition particulière précisée par l'établissement.

6.2.2 Sécurité

L'établissement 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 et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'établissement. L'établissement, son ministère de tutelle, ses fournisseurs d'accès ou ses partenaires techniques extérieurs se réservent le droit d'interdire certains accès, protocoles de communication, programmes ou modules pouvant porter atteinte à la sécurité.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions d'information ou de campagnes de sensibilisation.

6.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle.

L'Institut se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité du Système d'Information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'Institut, codes malveillants, programmes espions ...).

6.4 Traçabilité

L'Institut est dans l'obligation légale de mettre en place un système de journalisation[13] des accès Internet, de la messagerie et des données échangées.

L'Institut se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes informatiques.

L'Institut procédera, alors, à l'inscription à son registre des traitements, de la politique de gestion des journaux appliquées, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n 78-17 du 6 janvier 1978 modifiée et du Règlement général européen (UE) 2016/679 sur la protection des données (RGPD).

[13] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de.

Article VII. Respect de la législation concernant les données à caractère personnel

L'utilisateur a l'obligation de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 modifiée dite « Informatique et Libertés » et du Règlement général européen (UE) 2016/679 sur la protection des données (RGPD) du 27 avril 2016.

Les données à caractère personnel sont des informations susceptibles d'identifier directement ou indirectement et par quelque moyen que ce soit les personnes physiques auxquelles elles se rapportent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent d'extraction, de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux obligations légales et doivent avoir fait l'objet d'une instruction par le délégué à la protection des données (DPO) de l'établissement.

Par ailleurs, conformément aux dispositions légales, chaque utilisateur dispose de droits relatifs aux données le concernant, y compris les données portant sur l'utilisation des systèmes d'information : information, consentement, opposition, limitation, accès, rectification, portabilité, oubli, notification de violation de données, contestation d'une décision automatique, droit à réparation.

Ces droits peuvent s'exercer à tout moment auprès du délégué à la protection des données (DPO) de l'établissement : dpo@univ-jfc.fr.

Article VIII. Respect de la propriété intellectuelle

L'établissement rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier, télécharger ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations et contenus protégés par le droit d'auteur ou un droit privatif, de quelque nature que ce soit et sur toute forme de support, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ou s'être assuré du respect des droits de propriété intellectuelle, droit à l'image ou droit à la vie privée.

  Le fait de contrevenir à ces dispositions est susceptible d'engager la responsabilité pénale et civile de l'utilisateur ainsi que celle de l'établissement.

Article IX. Sanctions

En cas de non-respect de leurs obligations, et en dehors des poursuites pénales et/ou disciplinaires qui peuvent être engagées à leur encontre, les utilisateurs peuvent se voir appliquer :

- des mesures d'urgence

Les gestionnaires et exploitants peuvent, en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques ;
- prévenir le responsable hiérarchique ou pédagogique ;
- informer le directeur, par l'intermédiaire du responsable informatique.

- des mesures donnant lieu à information

Sous réserve que soit informé le Directeur ou le responsable hiérarchique ou pédagogique, les gestionnaires et exploitants peuvent :

- avertir un utilisateur ;
- à titre provisoire, limiter ou retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;
- effacer, comprimer ou isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité du Système d'Information.

Article X. Entrée en vigueur et révision de la charte

La présente charte annule et remplace tous les autres documents ou chartes relatifs à l'utilisation du système d'information de l'établissement.

Elle est annexée au règlement intérieur de l'Institut et entre en vigueur à la date de son approbation en conseil d'administration. Toute modification de la présente Charte devra suivre la procédure identique à son adoption. La dernière date de modification en conseil d'administration est inscrite sur la version publiée de la Charte.