



# Charte régissant l'usage du Système d'Information

Adoptée par le conseil d'administration du 7 juillet 2017



Institut National  
Universitaire  
**Champollion**

## Préambule

La présente charte définit les règles d'usage et de sécurité liées au Système d'Information de l'Institut.

### Article 1 : Champ d'application

La charte s'applique à l'ensemble du Système d'Information de l'établissement et à l'ensemble de ses utilisateurs.

L'établissement, par sa signature de la charte du Réseau RENATER<sup>1</sup>, est lui-même soumis aux règles d'utilisation des moyens informatiques et, à ce titre, se doit de faire respecter les règles déontologiques, ainsi que les dispositions législatives et réglementaires.

### Article 2 : 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 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 3 : Conditions d'utilisation du Système d'Information

#### 3-1 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).

---

<sup>1</sup> Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche.

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.

### 3-2 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.

### 3-3 Utilisation résiduelle à titre privé

Une utilisation à titre privé est tolérée. Elle doit rester raisonnable, tant dans sa fréquence que dans sa durée, et ne pas nuire à la qualité du travail ou au bon fonctionnement du service.

Les données privées, et leurs traitements associés ne doivent pas occasionner de surcoût pour l'Institut. A ce titre, leur volume doit rester raisonnable et les sauvegardes incombent à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Il lui appartient de le gérer, sauvegarder, détruire, notamment lors de son départ de l'Institut. L'établissement ne saurait en aucun cas être tenu pour responsable de la conservation ou de la destruction de cet espace.

### 3-4 Caractère des données

Toute communication et toute information sont réputées professionnelles (données et échanges mails) sauf à avoir été clairement identifiées comme privée par la mention du terme « Privé » dans l'objet du mail, le nom du répertoire, nom du fichier... Il appartient à l'utilisateur de stocker et, éventuellement, de sauvegarder ces communications, données et informations dans un espace dédié en mentionnant explicitement leur caractère privé.

### 3-5 Continuité de service

Dans l'hypothèse d'une absence prolongée ou d'un départ, et aux seules fins d'assurer la continuité du service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises à sa disposition dans le cadre de ses missions.

En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès au Système d'Information, il doit procéder, dès que possible, au changement de ces derniers ou en demander la modification au responsable de la DSIUN.

## Article 4 : Obligations des utilisateurs

Les utilisateurs doivent notamment :

- respecter les règles d'éthique professionnelle et de déontologie, et ne pas porter atteinte à la réputation ou à l'image de l'Institut ;
- respecter la présente charte ainsi que les différentes chartes dont l'Institut est signataire (charte RENATER) ;
- se conformer aux dispositifs mis en place par les gestionnaires et exploitants pour lutter contre les codes malveillants et les attaques par programmes informatiques ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître, ne pas utiliser ou tenter d'utiliser le compte d'un tiers ;
- veiller à la confidentialité des codes, mots de passe ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel ;

- respecter le droit d'auteur et les licences d'utilisation ;
- avertir sa hiérarchie 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 la personne responsable du site toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

### **Article 5 : Obligations des gestionnaires et exploitants**

Les gestionnaires et exploitants informatiques doivent :

- assurer le fonctionnement et la disponibilité des ressources informatiques ;
- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- veiller à la bonne utilisation du Système d'Information ;
- assurer la sécurité des ressources qu'ils exploitent ;
- garder les traces ("logs") en conformité avec législation : toute activité sur le réseau et les systèmes fait objet d'une surveillance automatisée ;
- porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

Les gestionnaires et exploitants peuvent, en cas d'urgence, prendre toutes mesures nécessaires pour assurer ou préserver le bon fonctionnement et la disponibilité normale des ressources informatiques dont ils ont la charge.

### **Article 6 : Respect de la législation concernant les données nominatives**

6-1 L'utilisateur est informé de la nécessité 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 dite « Informatique et Libertés » modifiée par la loi n°2004-801 du 6 août 2004.

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, [...] »<sup>2</sup>

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés ».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents qui prendront les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du Système d'Information.

Ce droit s'exerce auprès du Directeur de l'Institut ou auprès du service désigné selon les cas.

#### **6-2 Le correspondant informatique et libertés (CIL)**

Le CIL est un référent sur les questions de protection des données personnelles. Il conseille l'Institut sur les nouvelles manières d'exploiter les données.

Le CIL permet l'application des principes de la protection des données (finalité, pertinence des données, sécurité, droits des personnes, durée de conservation limitée), les rendant ainsi plus fiables.

<sup>2</sup> Article 2 de la loi n°78-17 du 6 janvier 1978

## Article 7 : Internet

Il est rappelé qu'Internet est soumis aux 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'Institut.

L'Institut met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques ou de recherche) : il peut constituer le support d'une communication privée dans le respect de la législation en vigueur.

En complément des dispositions légales en vigueur et au regard de la mission éducative de l'Institut, la consultation volontaire de sites à contenus de caractère pornographique depuis les locaux de l'Institut, est interdite.

### 7-1 Publications sur les sites internet et intranet de l'Institut

Toute publication de pages d'information sur les sites internet ou intranet de l'Institut doit être validée par un responsable de publication nommément désigné.

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

### 7-2 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 ...).

### 7-3 Traçabilité

L'Institut est dans l'obligation légale de mettre en place un système de journalisation<sup>3</sup> 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.

Préalablement à cette mise en place, l'Institut procédera, auprès de la Commission nationale de l'informatique et des libertés, à une déclaration, 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 par la loi n 2004-801 du 8 août 2004.

## Article 8 : Fin du statut d'utilisateur

Le compte d'accès sera retiré 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 :

- Deux mois après la fin de l'inscription administrative d'un étudiant ;

---

<sup>3</sup> La durée de conservation des journaux informatiques est de 1 an maximum. L'établissement s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme. Deux conteneurs de données sont donc définis, le premier reçoit les fichiers de logues vieux de moins de trois mois et les fichiers anonymisés quand ils existent. Le second reçoit les journaux contenant des données à caractère nominatif de plus de trois mois.

- 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.

## **Article 9 : 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, compresser ou isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité du Système d'Information.

## **Article 10 : Entrée en vigueur et révision de la charte**

La présente charte est annexée au règlement intérieur de l'Institut et entre en vigueur après sa validation 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.