Univ. Grenoble Alpes
Université de l'innovation

Charte d'usage du Système d'Information de l'EPE

Préambule

L'établissement s'est doté d'une **politique de sécurité des systèmes d'informations** (PSSI) en cohérence avec la PSSI de l'Etat (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.

Elle engage chaque structure et chaque utilisateur à son niveau de responsabilité.

La « Charte d'usage du système d'information » vient préciser les droits et devoirs de chacun des acteurs.

Par « **système d'information** » s'entend l'ensemble des données et des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition de l'« utilisateur ».

L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portable est également un des éléments constitutifs du système d'information.

Par « **utilisateur** » s'entend toute personne ayant vocation à détenir un compte informatique ou à avoir accès aux ressources du système d'information quel que soit son statut.

Il s'agit notamment de :

- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement et de la recherche ;
- tout étudiant inscrit dans l'établissement ;
- toute personne extérieure à l'établissement, visiteur, invité, prestataire ayant contracté avec l'établissement.

Par « données professionnelles » s'entend l'ensemble des données, des fichiers, des traitements gérés par l'établissement au sein de son activité qu'elle soit de recherche, d'enseignement, administrative ou culturelle.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation des données professionnelles.

La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

Considérant les engagements de l'UGA :

L'UGA 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[1].

L'utilisateur a une responsabilité particulière dans l'utilisation qu'il fait des ressources mises à sa disposition par l'établissement.

L'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

Il est arrêté ce qui suit :

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 des utilisateurs.

Les usages relevant spécifiquement de l'activité des organisations syndicales ou organisations représentatives du personnel ne sont pas régis par la présente charte.

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 DROITS D'ACCES AUX SYSTEMES D'INFORMATION

Le droit d'accès aux systèmes d'information est temporaire. Il est retiré si la qualité de l'utilisateur ne le justifie plus et, sauf demande expresse, au plus tard 3 mois après que celui-ci n'ait plus vocation à détenir un compte informatique.

Il peut également être retiré, par mesure conservatoire, si le comportement de l'utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Article III PROTECTION DES DONNEES

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.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'établissement.

Article IV CONDITIONS D'UTILISATION DES SYSTEMES D'INFORMATION

Section IV.1 UTILISATION ET VIE PRIVEE

Dans le cadre de son activité, les systèmes d'information sont mis à la disposition de l'utilisateur.

L'utilisation des systèmes 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.

1- Notamment le secret médical dans le domaine de la santé.

L'utilisation résiduelle des systèmes 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[2] 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 des systèmes 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 sexiste, homophobe, 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.

Section IV.2 CONTINUITE DE SERVICE : GESTION DES ABSENCES ET DES DEPARTS

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.

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 à la Section V.1

Article V PRINCIPE DE SECURITE

Section V.1 REGLES DE SECURITE APPLICABLES

L'établissement, son ministère de tutelle, ses fournisseurs d'accès et ses partenaires académiques extérieurs mettent en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les mots de passe (ou tout autre système d'authentification) constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère privé.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes 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. En cas de doute sur cette confidentialité, il incombe à l'utilisateur de changer immédiatement ses mots de passe.

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'établissement :
  - 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.
- 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, même si cet accès est techniquement possible.
  - Ne pas connecter directement aux réseaux des matériels non confiés ou non autorisés par l'établissement, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;
  - Ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, de logiciels ou progiciels sans autorisation explicite ; en cas d'autorisation le téléchargement et l'installation ne peut se faire qu'à partir de sites dignes de confiance[6]
  - Se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les différentes attaques pouvant nuire aux systèmes d'information.
  - Ne pas apporter des perturbations au bon fonctionnement des ressources informatiques et des réseaux 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.

Section V.2 DEVOIRS DE SIGNALEMENT ET D'INFORMATION

L'utilisateur doit avertir, par le biais de l'assistance informatique de l'établissement, le responsable de la sécurité du système d'information 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.

Section V.3 MESURES DE CONTROLE DE LA SECURITE

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 ;

2 Pour exemple, cet espace pourrait être dénommé "_privé_"

3 Pour exemple, "_privé_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.

4 Article L 323-1 et s. du Code pénal

5 Article 24, 26bis, 32 et 33 de la Loi du 29 juillet 1881

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

- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée, le cas échéant supprimée (information de type virus, logiciel espion, pourriel ou spam).
- 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 ELECTRONIQUES

Section VI.1 MESSAGERIE ELECTRONIQUE

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

a) *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 si elle est exploitée par un service ou un groupe d'utilisateurs.

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

b) *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.

c) *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.

d) *Statut et valeur juridique des messages*

D'après la loi[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.

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

e) *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.

Section VI.2 MESSAGERIE INSTANTANEE (CHAT)

L'emploi de la messagerie instantanée de l'établissement peut être recommandé par certains services notamment dans le cadre du télétravail

L'usage qui doit en être fait veille à respecter les mêmes principes que la messagerie, notamment sur la qualité et la teneur des contenus échangés.

Section VI.3 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 en section III.1, 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.

a) *Publication sur les sites Internet et Intranet de l'établissement*

Toute publication d'information sur les sites Internet ou Intranet de l'établissement[12] doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication d'information à caractère privé (pages privées …) sur les ressources du système d'information de l'établissement n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

b) *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. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou 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 de formations ou de campagnes de sensibilisation.

Section VI.4 TELECHARGEMENTS

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

La consultation, et a fortiori le téléchargement à partir de sites dont le contenu est contraire à la législation ou aux bonnes mœurs (sites à caractère pornographique, pédophile, xénophobe...) peut revêtir le caractère d'une infraction pénale. Cette activité est strictement interdite dans l'établissement pendant ou en dehors des heures de travail. Elle peut faire l'objet de sanctions pénales et/ou administratives

L'établissement se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'établissement, code malicieux, programmes espions …).

Article VII TRAÇABILITE

L'établissement 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'établissement se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

L'établissement s'est doté d'une « politique générale de gestion des journaux informatiques », inscrite au registre des traitements de l'établissement. Elle mentionne notamment les conditions et la durée de conservation des traces de connexions ou d'utilisation des services, et les modalités d'expression du droit d'accès dont disposent les utilisateurs, en application de la loi informatique et libertés du 6 janvier 1978 modifiée et du Règlement général européen (UE) 2016/679 sur la protection des données (RGPD).

Article VIII RESPECT DE LA LEGISLATION SUR LES DONNEES PERSONNELLES

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)

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 auprès du délégué à la protection des données (DPO) de l'établissement.

Article IX RESPECT DE LA PROPRIETE 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 ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Article X LIMITATION DES USAGES

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, la « personne juridiquement responsable » de l'établissement ou les responsables sécurité du système d'information pourront, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », il faut entendre toute personne ayant la capacité de représenter l'établissement (président d'université, directeur d'institut…).

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles, est passible de sanctions. Elles sont décidées par la section disciplinaire de L'UGA prévue à l'article L 712-4 du code de l'éducation. Les sanctions encourues sont fixées par le décret n° 92-657 du 13 juillet 1992 modifié fixant la procédure disciplinaire dans les Etablissements Publics à caractère Scientifique, Culturel et Professionnel (EPSCP).

Article XI ENTREE EN VIGUEUR DE LA CHARTE

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information de l'établissement.

Il entrera en vigueur dans chaque établissement à la date de son approbation par l'autorité compétente.

Il est annexé au règlement intérieur.

Prénom NOM : _____ Date de naissance : _____

Adresse électronique : _____

Mention à porter à la main : « Je soussigné(e) (Nom, Prénom) atteste avoir lu le présent règlement et m'engage à le respecter. »

Fait à Le Signature :

_____

[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.

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

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

[10] Sauf les prestataires des partenaires institutionnels et les outils explicitement autorisés.

[11] Articles 1366-1367 du code civil (Ordonnance n°2016-131 du 10 février 2016 - art. 4)

[12] A partir des ressources informatiques mises à la disposition de l'utilisateur.

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