Université Polytechnique
HAUTS-DE-FRANCE

Délibération 2022-33-CA P

Séance du 07 Juillet 2022

Extrait du recueil des actes du Conseil d'Administration

Règlement intérieur des systèmes d'information

Le Conseil d'Administration de l'UPHF s'est réuni en séance plénière dans l'amphithéâtre 150 du bâtiment Matisse sur le site du Mont Houy le jeudi 07 juillet 2022 sur la convocation et sous la présidence de Monsieur Abdelhakim Artiba, Président.

Le quorum étant atteint,

Vu le décret n° 219-942 du 09 septembre 2019 portant création de l'Université Polytechnique Hauts-de-France et de l'Institut National des Sciences Appliquées Hauts-de-France et approbation des statuts de l'établissement expérimental ;

Monsieur le Président donne la parole à M. Manuel Varago, Responsable du Service Juridique, qui présente aux membres, qui présente aux membres le règlement intérieur des systèmes d'information prenant compte des deux établissements notamment l'intégration de l'INSA Hauts-de-France.

Après en avoir délibéré,

Le conseil d'administration approuve à l'unanimité des voix le règlement intérieur des systèmes d'information selon le document joint à la présente délibération.

Pour : 23 voix
Contre : 0 voix
Abstention : 0 voix

Valenciennes, le 07 juillet 2022

Abdelhakim Artiba
Président

Annexe à la délibération 2022-33-CA P

Règlement intérieur relatif à l'usage du système d'information de l'Université Polytechnique Hauts-de-France

Document conseil d'administration 7 juillet 2022

Sommaire

Article I. Champ d'application 4

Article II. Conditions d'utilisation des systèmes d'information 4

Section II.1 Conditions d'utilisation professionnelle / privée 4

Section II.2 Conditions d'utilisation pour la continuité de service en cas d'absences et de départs 4

Article III. Principes de sécurité des systèmes d'information 5

Section III.1 Règles de sécurité applicables 5

Section III.2 Devoirs de signalement et d'information 6

Section III.3 Mesures de contrôle de la sécurité 6

Article IV. Communication électronique 7

Section IV.1 Messagerie électronique 7

Adresses électroniques 7

Contenu des messages électroniques 7

Émission et réception des messages 8

Statut et valeur juridique des messages 8

Gestion des mails et archivage 8

Liste de diffusion 8

Section IV.2 Internet 8

Publication sur les sites internet et intranet de l'université 9

Sécurité 9

Section IV.3 Échanges de fichiers 9

Section IV.4 Ressources numériques 9

Article V. Traçabilité 9

Article VI. Respect de la propriété intellectuelle 9

Article VII. Respect de la loi informatique et libertés 9

Article VIII. Limitation des usages 10

Article IX. Entrée en vigueur 10

Préambule

Le "système d'information" recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'Université Polytechnique Hauts-de-France .

L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables et tout équipement connecté sur le réseau, est également un des éléments constitutifs du système d'information.

Par «utilisateur» s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut. Il s'agit notamment de :

- tout étudiant en formation initiale ou en formation continue inscrit à l'université ou à l'INSA Hauts de France, ou étudiant invité ;
- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche en poste à l'université ou à l'INSA Hauts de France ;
- tout prestataire ou partenaire[1] ayant contracté avec l'université et conduit à devenir usager du système d'information ;
- tout stagiaire ayant contracté une convention de stage avec l'un des services ou l'une des composantes de l'université ou à l' INSA Hauts de France;
- toute personne « invitée » ou « hébergée » » autorisée à accéder à un service numérique.

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 ainsi que les consignes de la charte RENATER[2].

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

Engagements de l'université

L'université porte à la connaissance de l'utilisateur la présente charte.

L'université met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'université garantit l'accès des utilisateurs aux ressources du système d'information dans les meilleures conditions de sécurité et avec une haute disponibilité des services.

Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'université reconnaît l'utilisation résiduelle du système d'information à titre privé dans les conditions définies dans la présente charte.

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 confidentialité à l'égard des informations et documents 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.

---

1 Le contrat devra prévoir expressément l'obligation de respect de la charte.

2 http://www.renater.fr/IMG/pdf/charte_fr.pdf https://www.renater.fr/telechargement%2C1392

Article I. Champ d'application

En complément de la charte RENATER, les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'université ainsi qu'à l'ensemble des utilisateurs.

Les usages relevant de l'activité des organisations syndicales sont régis par une charte spécifique.

Article II. Conditions d'utilisation des systèmes d'information

Condition d'utilisation professionnelle / privée

L'Université a mis en place une démarche globale pour son système d'information s'appuyant sur un ensemble d'applications couvrant les différents domaines fonctionnels et sur un ensemble de services associés; parmi ces services et ressources liés au système d'information, certains services (messagerie, ENT, accès internet ...) sont des outils de travail ouverts à des usages professionnels administratifs, pédagogiques et de recherche et doivent s'inscrire dans un usage à caractère professionnel. Ils peuvent constituer d'une façon dérogatoire et contrôlée, le support d'une communication privée.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que 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.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement[3] à cet effet ou en mentionnant le caractère privé sur la ressource[4]. La sauvegarde régulière des données à caractère privé incombe à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'Université, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'université ne pouvant être engagée quant à la conservation de cet espace.

Les mesures de conservation des données professionnelles doivent être définies par le responsable concerné au sein de l'université. Les données professionnelles correspondent aux documents enregistrés, par exemple sous la forme de fichiers, de messages électroniques, d'événements dans le calendrier, de liste de contacts, de procédures....

De manière générale, la confidentialité et la sécurité des données sont assurées par l'université.

L'utilisation des systèmes d'information doit respecter les lois et règlement en vigueur.
Il est interdit :

- de diffuser des messages diffamatoires ou injurieux
- d'utiliser certaines formes d'apologie (crime, négationnisme, racisme ...)
- d'utiliser toute forme de provocation et de haine raciale

Conditions d'utilisation pour la continuité de service en cas d'absences et de départs

Afin d'assurer la continuité de service, plus particulièrement en cas de départ ou d'absence, 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. L'utilisation d'adresses mails fonctionnelles est autorisée, permettant ainsi de partager la réception des messages.

Pour les personnels, le responsable devra prévoir le transfert des données professionnelles de l'utilisateur qui part, en concertation avec celui-ci.

---

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

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

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant hors identifiant l'accès aux ressources mises spécifiquement à sa disposition.

En tout état de cause les données privées non classées dans un répertoire « PRIVE », ou identifiées comme telles, sont considérées comme des données appartenant à l'université qui pourra en disposer.

En cas d'atteinte à la continuité du service public causée par une absence de l'agent, le Président de l'université, sur demande motivée du chef de service, saisi le responsable de la sécurité des systèmes d'information (RSSI) pour qu'il restitue au chef de service les données à caractère professionnelles conservées sur le poste informatique de l'agent absent.

Les étudiants conservent des accès pendant six quatre mois après la fin de leur inscription. Ceux-ci seront fermés au delà de cette date et les données supprimées.

Les doctorants relèvent des règles relatives aux personnels dans la présente charte.

Les vacataires d'enseignement conservent leur compte pendant 6 mois après la fin de leur contrat.
Tout autre utilisateur conserve leur compte pendant 2 mois

Article III. Principes de sécurité des systèmes d'information

Règles de sécurité applicables

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

L'utilisateur est conscient que les codes d'accès au système d'information (par exemple accès à la messagerie électronique, au réseau sans fil, aux bases de données des étudiants ou des personnels constituent :

- une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive
- une protection des données à caractère personnel pour assurer le respect des droits des personnes fichées.

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 instructions relatives à la gestion des codes d'accès (le mot de passe ne doit pas être trouvé dans un dictionnaire, il doit contenir un mélange de caractère alphanumériques et spéciaux, il doit faire au moins 8 caractères, il faut le changer régulièrement, il ne faut pas l'écrire mais le mémoriser) ;
- de garder strictement confidentiels son (ou ses) codes d'accès et en aucun cas les communiquer à un tiers par quelque moyen que ce soit ;
- de respecter la gestion des accès, en particulier en ne cherchant pas à connaître les codes d'accès d'un tiers, et refuser de les utiliser.

Le non respect des règles de sécurité peut entraîner une détérioration de la qualité du système d'information, par mesure conservatoire les accès en défaut sont désactivés. L'utilisateur concerné doit contacter la DSI, ses codes d'accès sont rétablis après un délai de 3 jours, temps nécessaire pour le rétablissement du service.

La sécurité des ressources mises à la disposition de l'utilisateur nécessite des règles de prudentielles

1) De la part de l'université :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées. Par exemple les bases de données des étudiants et des personnels contiennent des données à caractère personnel accessibles uniquement par des agents qui ont une nécessité à les utiliser.
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

2) 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;
- ne pas installer, télécharger ou utiliser sur le matériel de l'université des logiciels ou progiciels sans respecter les droits de licence, ou en cas de logiciels libres, ne provenant pas de sites dignes de confiance;
- se conformer aux dispositifs mis en place par l'université pour lutter contre les virus et les attaques par programmes informatiques. Par exemple le poste de travail doit être protégé par un anti-virus, les postes de l'université doivent être munis de l'anti-virus proposé par la Direction du numérique de l'université. Les postes personnels doivent être protégés d'un anti-virus disposant d'une licence légale à la charge de l'utilisateur, l'utilisateur ne doit pas installer et utiliser des logiciels permettant des attaques sur des sites distants ;
- ne pas nuire au bon fonctionnement du système d'information, (par exemple en effectuant des téléchargements trop volumineux), et se conformer aux lois en vigueur ;
- 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 la propriété intellectuelle, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- ne pas déposer de données professionnelles ou des données de recherche confidentielles sur des sites extérieurs non conforme à la règlementation relative à la protection du potentiel scientifique de la Nation (par exemple dépôt de données sur des espaces de stockage Internet type DropBox ou autres, ou sur des sites Web de l'Internet)
- assurer la protection des données sensibles et à caractère personnel, veiller au respect des règles relatives à la protection des données personnelles avec l'aide du Délégué à la protection des données
- ne pas quitter son poste de travail en laissant les ressources ou services accessibles, verrouiller les accès (poste de travail, bureau ou salle).

Devoirs de signalement et d'information

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, suspicion d'une usurpation d'un code d'accès, etc. Le responsable hiérarchique doit en informer les RSSI[5] (responsables de la sécurité des systèmes d'information) de l'université.

Mesures de contrôle de la sécurité

L'utilisateur est informé et ne peut s'opposer :

- pour effectuer la maintenance corrective, curative ou évolutive, l'université se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- une maintenance à distance est précédée d'une information spécifique de l'utilisateur ;
- toute information bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste, le cas échéant à la suppression des éléments en cause ;
- l'ensemble du système d'information donne lieu, dans le respect de la législation applicable, à un suivi, un contrôle et à une surveillance, à des fins statistiques, de traçabilité réglementaire ou

5 Courriel : rssi@uphf.fr

fonctionnelle, d'optimisation, de sécurité ou de détection des abus.

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[6] 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.

Néanmoins, ces personnels sont soumis à l'obligation générale d'aviser le procureur de la République de tout crime ou délit dont ils acquièrent la connaissance à l'occasion de l'exercice de leur fonction[7].

Ils doivent se conformer aux réquisitions prévues par le code de procédure pénale, et en particulier aux réquisitions menées par des officiers de police judiciaire aux fins d'obtenir, notamment sous forme numérique, des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives[8].

Article IV. Communication électronique

Messagerie électronique

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'université.

Adresses électroniques

L'université s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative[9] lui permettant d'émettre et de recevoir des messages électroniques, dès lors : :

- pour un utilisateur étudiant, qu'il soit inscrit administrativement, -

pour un utilisateur personnel, qu'il soit identifié dans les bases de données de la de la Direction des Ressources Humaines.

L'utilisation de cette adresse nominative est de la responsabilité de l'utilisateur.

Cette adresse nominative doit être utilisée dans le cadre des communications professionnelles. L'université reconnaît l'utilisation résiduelle de la messagerie à usage privé.

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.

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[10] 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, ...) sont déployées.

Sont interdits les messages contraires aux lois et règlements en matière d'atteinte à la personne humaine et d'atteinte aux intérêts fondamentaux de la Nation, (par exemple les discriminations, l'atteinte à la vie privée, la dénonciation calomnieuse, la diffamation, l'intelligence avec une puissance étrangère, le terrorisme).

---

6 Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

7 Article 40 alinéa 2 du code de procédure pénale.

8 Article 60-1 du code de procédure pénale

9 Par exemple, l'adresse est de la forme prénom.nom@ @uphf.fr

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

Sont également interdits les messages contraires aux obligations de réserve, de neutralité et de loyauté des agents publics prévues par les lois et règlements.

Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. Il ne doit pas faire usage de message reçu par erreur.

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.

Statut et valeur juridique des messages

Dans le cadre de la réglementation relative au droit de saisine de l'administration par voie électronique, le message électronique est opposable aux administrés et à l'administration dans les mêmes conditions qu'un courrier en forme papier[11].

L'université a l'obligation de traiter une demande ou une information formulée par voie électronique, et d'en accuser réception. A défaut d'accusé, les délais de recours ne sont pas opposables à l'auteur de la demande.

Gestion des mails et archivage

Les utilisateurs privilégient les outils de transferts de fichiers mis à disposition par la Direction du numérique de l'université dans l'espace numérique de travail, veillent à structurer leurs dossiers et à épurer sa messagerie de manière à respecter le quota attribué, et vérifient la véracité des messages suspects (spams).

La boite aux lettres est personnelle, l'adresse mail garantit l'identité de l'utilisateur et engage sa responsabilité dans l'envoi des messages. L'abus dans l'envoi de messages (phishing) peut avoir un impact sur le bon fonctionnement du système d'information (mise en liste noire des serveurs de l'université), et par conséquent impacter l'ensemble des utilisateurs de l'université et dégrader notre image vis à vis des opérateurs Internet.

Liste de diffusion

Des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateurs » peuvent être mise en place par l'université. Elles peuvent avoir un caractère obligatoire (ex : listes institutionnelles) ou facultative (ex : liste de projet) à abonnement/désabonnement libre.

Chaque utilisateur est informé dans son environnement numérique de travail (ENT) de ses abonnements aux listes de diffusion et de leurs objets. Les listes institutionnelles ont un caractère obligatoire (par exemple pour l'administration, la pédagogie, la recherche), l'utilisateur ne peut pas se désabonner. Pour les listes spécifiques (syndicales, électorales, ...), l'abonnement et/ou le désabonnement sont libres.

Internet

Il est rappelé qu'Internet et l'intranet (réseau interne de l'université) sont soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet/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'université.

Internet/intranet est un outil de travail ouvert à des usages professionnels (administratifs, de recherche et pédagogiques). Si une utilisation résiduelle privée, telle que définie en section 2.01, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'université sont

---

11 La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

présumées avoir un caractère professionnel. La Direction du numérique de l'université pourra les rechercher aux fins de les identifier.

Publication sur les sites Internet et intranet de l'université

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

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

Sécurité

Afin de respecter les lois en vigueur, de protéger les utilisateurs, d'assurer le bon fonctionnement du système d'information, l'université peut filtrer ou interdire l'accès à certains sites Internet/intranet (par exemple site de « phishing » consistant à usurper des mots de passe), de procéder au contrôle à priori ou à posteriori des sites visités et des durées d'accès correspondantes.

Les accès Internet/intranet ne sont autorisés qu'au travers de dispositifs de sécurité mis en place par l'université. Des règles de sécurité spécifiques peuvent être précisées par la Direction du numérique de l'université.

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.

Échanges de fichiers

Tout téléchargement de fichiers, notamment de sons ou d'images doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI.

L'université 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'institution, codes malveillants, programmes espions ...).

Ressources numériques

L'usage des ressources est strictement professionnel, pour les activités de l'administration, de la recherche et de l'enseignement.

Les lecteurs autorisés ont le droit de visionner à l'écran et d'imprimer les informations ou bien de les télécharger dans les limites d'un usage raisonnable, non commercial, et strictement personnel.

Il est strictement interdit de distribuer ces copies (papier ou électroniques) à des personnes extérieures à l'université gratuitement ou à des fins lucratives.

Chaque personne est responsable de l'utilisation des ressources documentaires électroniques et s'engage à ne pas effectuer des opérations de téléchargements abusifs pouvant nuire à l'ensemble de la communauté et entraîner une interruption brutale de service du diffuseur ou du producteur de l'information.

Article V. Traçabilité

L'université est dans l'obligation légale de mettre en place un système de journalisation[12] des accès Internet,

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

de la messagerie et des données échangées.

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

Préalablement à cette mise en place, l'université procède à une mise en conformité du traitement des données, qui mentionne notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application du règlement européen relatif à la protection des données et à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée

Article VI. Respect de la propriété intellectuelle

L'université rappelle que l'utilisation des ressources 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 sans s'être préalablement assuré que les œuvres sont libres de droits de propriété intellectuelle ou sans avoir obtenu préalablement l'autorisation des titulaires ou des exploitants de ces droits.

Article VII. **Respect de la protection des données personnelles.**

Article VIII. Chaque utilisateur est tenu de respecter les dispositions légales en matière de protection des données à caractère personnel conformément au règlement général de l'Union Européenne 2016/679 du 27 avril 2016 sur la protection des données (RGPD) ainsi que la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.[13]

Article IX. Limitation des usages

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur est passible de sanctions[14] pénales et disciplinaires.

En cas de non-respect des règles définies dans le présent règlement, le Président de l'Université peut, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, suspendre temporairement les autorisations d'accès aux ressources informatiques. Sur demande écrite du Président, les personnels habilités de la DSI doivent fournir l'identité des usagers qui ne respectent pas la présente charte.

Article X. Entrée en vigueur

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

---

[13] https://www.uphf.fr/protection-des-donnees-personnelles

[14] Code pénal article 323-1 à 323-7 (fraudes informatiques) articles 226-16 à 226-24 (atteintes aux droits de la personne résultant des fichiers ou traitements informatiques)