Charte des usages numériques

Janvier 2023

Nantes Université

Table des matières

Préambule

La présente charte a pour objet de définir les règles des usages numériques et du système d'information de Nantes Université.

Ces règles ont pour finalité de contribuer à la protection de l'utilisateur, à la préservation de la sécurité du système d'information de l'Etablissement et de garantir la disponibilité, l'intégrité et la confidentialité des données qui y sont hébergées.

Ce document a pour ambition de rendre visibles les bonnes pratiques d'utilisation des moyens numériques et d'accompagner l'évolution des usages numériques et de la réglementation.

1 Champ d'application

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

Les *utilisateurs* au sens de la présente charte, sont définis comme l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de Nantes Université.

Il s'agit notamment :

- des personnels, titulaires et non titulaires : enseignants, chercheurs, personnels administratifs et techniques ;
- des étudiants ;
- des prestataires et partenaires.

L'*Université* désigne dans la présente charte Nantes Université, l'ensemble de ses composantes, de ses pôles, de ses services ou de ses partenaires telles que les unités de recherche, dès lors qu'ils utilisent des moyens numériques de l'Université.

Les *usages numériques* recouvrent toute utilisation des moyens numériques mis à la disposition des utilisateurs. Ces moyens numériques représentent tous les dispositifs (outils, services, applications, logiciels, matériels, équipements…) informatiques, audiovisuels et de communication que Nantes Université met à disposition de ses utilisateurs. Il est précisé que les moyens numériques incluent les équipements mobiles, ordinateurs portables, téléphones portables, smartphones, tablettes…

Les dispositions de la présente charte précisent les droits et devoirs des utilisateurs de Nantes Université, quel que soit le lieu d'accès au système d'information (télétravail, accès à distance…).

Les usages relevant de l'activité des organisations syndicales[1] et de groupes d'élus au sein des instances centrales, ainsi que des administrateurs du système d'information sont régis par des documents spécifiques qui viennent compléter la présente charte.

Des procédures opérationnelles, guides pratiques, règles de sécurité viennent compléter et préciser la présente charte. L'ensemble de ces documents est accessible en ligne, notamment sur l'intranet[2] de l'Université.

2 Conditions d'utilisation des systèmes d'information et des moyens numériques

La présente charte précise que le respect par l'utilisateur d'obligations générales telles que la confidentialité, la discrétion, la loyauté ou la vigilance est un principe essentiel de l'utilisation des moyens numériques.

Il est rappelé que l'utilisateur joue un rôle déterminant dans la protection du système d'information de Nantes Université.

2.1 Utilisation professionnelle / privée

Nantes Université met à la disposition de ses utilisateurs un ensemble de moyens numériques à des fins professionnelles.

Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :

- dans le cadre des missions confiées par Nantes Université, pour les utilisateurs membres de son personnel : enseignants, chercheurs, personnels administratifs et techniques, mais également ses prestataires et partenaires ;
- dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Par opposition, l'utilisation à des fins privées doit être non lucrative et limitée, tant dans la fréquence que dans la durée. Elle ne doit nuire ni à la qualité du travail de l'utilisateur, ni au bon fonctionnement du service.

[1] https://intraperso.univ-nantes.fr/medias/fichier/charte-sur-les-modalites-d-utilisation-des-tic-pas-les-os-a-l-universite-de-nantes_1562572594268-pdf?ID_FICHE=1279280&INLINE=FALSE
[2] https://intraperso.univ-nantes.fr

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des moyens numériques doit demeurer négligeable au regard du coût global d'exploitation. L'utilisateur reste invité à bien séparer ses usages numériques privés de ses usages professionnels. En particulier, il est recommandé de ne pas utiliser les moyens numériques, notamment l'adresse mail de l'Université pour des activités privées et réciproquement.

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 prévu à cet effet et identifié sans ambiguïté comme tel.

Ainsi, tout utilisateur manifeste le caractère extra-professionnel d'une partie de ses données en adoptant, le terme «privé» ou «personnel», pour nommer le dossier de stockage de fichiers, le dossier de stockage de courrier électronique et pour identifier ses événements d'agenda et l'objet de ses communications.

La sauvegarde régulière des données à caractère privé incombe exclusivement à l'utilisateur.

2.2 Continuité de service : gestion des absences et des départs

Il appartient à tout membre du personnel, quittant à titre provisoire ou définitif Nantes Université, de respecter les obligations suivantes pour préparer son absence ou son départ :

2.2.1 Permettre l'accès à ses données professionnelles en vue de garantir la continuité de service

Les mesures de stockage et de conservation des données professionnelles sont définies par le responsable hiérarchique.

Lors d'un départ définitif ou d'une absence ponctuelle, l'utilisateur informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.

En cas d'absence ponctuelle, il convient également de :

- s'assurer de la mise en place d'un « répondeur » sur la messagerie électronique et le téléphone, orientant les demandeurs vers un autre contact.

En complément, en cas de départ définitif, il convient également de :

- demander la suppression des accès aux logiciels et applications de travail ;
- demander le retrait de son adresse électronique professionnelle des différentes listes de diffusion.

2.2.2 Procéder à la suppression des données privées stockées dans le système d'information

L'utilisateur est responsable de la gestion de ses données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de prendre en charge personnellement la récupération puis la suppression des données privées qu'il aurait stockées dans le système d'information de l'établissement.

En conséquence, Nantes Université ne peut être tenue responsable :

- de la perte des données qui n'auraient pas été récupérées par l'utilisateur avant son départ,
- de la divulgation ultérieure de données qu'il n'aurait pas supprimées.

2.2.3 Restituer le matériel fourni et les moyens d'accès aux locaux

L'utilisateur veille à restituer tous les matériels, équipements numériques et moyens d'accès aux locaux mis à sa disposition dans le cadre de ses missions et activités.

3 Principes de sécurité

Nantes Université met en œuvre des mesures de sécurité adaptées aux besoins de sécurité :

- de son système d'information ;
- des moyens numériques mis à la disposition des utilisateurs.

3.1 Moyens d'authentification

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

Les niveaux d'habilitation accordés à l'utilisateur sont définis en considération de la mission qui lui est confiée. La sécurité des ressources mises à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiels ses moyens d'authentification (comme les mots de passe) et de ne jamais les transmettre à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les moyens d'authentification d'un autre utilisateur, ni chercher à les connaître ;
- s'il ne bénéficie pas d'une habilitation explicite, de s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible.

3.2 Devoir de signalement

Il appartient à l'utilisateur d'avertir, sans délai, sa hiérarchie et le support informatique [3] de tout usage inapproprié ou malveillant des ressources numériques de Nantes Université, dont il aurait connaissance.

L'utilisateur doit avertir le support sans délai de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information. Il signale également toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

3.3 Maintenance et assistance à distance

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, Nantes Université se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les matériels mis à disposition ;
- qu'une prise de contrôle à distance du poste de travail de l'utilisateur est précédée d'une information de celui-ci ;
- que tout élément bloquant ou présentant un risque de sécurité ou une difficulté technique d'acheminement à son destinataire peut être isolé, le cas échéant supprimé.

3.4 Paramétrage et protection des postes de travail

Nantes Université met en œuvre une protection logicielle ainsi qu'un système de déploiement automatique des mises à jour sur les serveurs et sur les postes de travail des utilisateurs.

Par la présente charte, l'utilisateur :

- s'engage à ne pas apporter volontairement de perturbations au bon fonctionnement des ressources informatiques et des réseaux, par des manipulations anormales du matériel ou des logiciels ;
- n'installe pas, ne télécharge pas ou n'utilise pas des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou provenant de sites douteux ou signalés comme tels ;
- s'engage à ne jamais introduire volontairement sur le réseau de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, ransomwares, malwares, spywares, etc.
- reste vigilant vis-à-vis des supports de données amovibles (clé USB, disque externe, DVD, etc.) et prend les précautions nécessaires pour s'assurer de leur innocuité ;
- se conforme aux règles de sécurité de Nantes Université pour le maintien en conditions opérationnelles et de sécurité de l'ensemble du parc informatique. En particulier, l'utilisateur ne doit pas altérer le fonctionnement des outils de protection (antivirus) et de mise à jour des postes de travail et serveurs ;

[3] support-securite@univ-nantes.fr

Le poste de travail constitue une porte d'entrée sur le système d'information, qui doit être protégé des intrusions. À cet égard il est nécessaire :

- de paramétrer la mise en veille automatique de l'ordinateur avec demande du mot de passe pour sa réactivation après une période d'inactivité ;
- de systématiquement verrouiller la session ouverte sur le poste de travail lorsque l'utilisateur s'absente ;
- de déconnecter les sessions de travail ouvertes sur des serveurs distants lorsqu'elles ne sont plus requises ;
- d'éteindre complètement son poste de travail et ses écrans, a minima lorsque l'utilisateur quitte son lieu de travail, chaque soir.

3.5 Utilisation du poste de travail en mode administrateur

Un utilisateur, pour des besoins particuliers et sur demande explicite auprès de son équipe d'informaticiens de proximité, peut disposer d'un compte avec des droits d'administrateur local sur son poste de travail.

L'utilisation de ce compte doit être ponctuelle et réservée aux actions d'administration qui le nécessitent expressément. Pour tous les autres usages, au quotidien et particulièrement pour la navigation sur internet, il est obligatoire d'être connecté avec son compte standard, ne possédant pas les privilèges « administrateur ».

En effet, les comptes administrateurs sont les cibles privilégiées de nombreux programmes malveillants tentant d'accéder aux ressources du poste, avec des droits élevés.

En cas de doute, l'utilisateur se rapprochera de son équipe d'informaticiens de proximité.

3.6 Accès aux réseaux

La connexion d'un matériel personnel au réseau Wi-Fi est autorisée dans la mesure où elle a une finalité professionnelle. Une utilisation résiduelle privée, telle que définie au chapitre 2, est toutefois tolérée.

La présente charte rappelle à l'utilisateur l'importance de maintenir à jour son matériel personnel et de le doter d'une protection adaptée (antivirus, mises à jour de sécurité…) avant toute connexion au réseau Wi-Fi proposé par l'Université.

Les services offerts aux matériels personnels connectés en Wi-Fi peuvent être limités et ne pas permettre pas l'accès à certaines ressources comme par exemple des répertoires partagés ou certaines applications métiers de l'Université.

Seuls des matériels configurés et administrés par l'Université peuvent bénéficier d'une connexion filaire (c'est-à-dire sur une prise réseau).

De nombreux services, comme certaines applications métiers de l'Université, ne sont accessibles qu'à partir d'un poste fourni et administré par l'Université.

Besoins spécifiques

Si un service, une composante ou un chercheur de l'Université, dans le cadre de ses travaux, a des besoins spécifiques dérogeant aux règles ci-dessus, il doit s'adresser à son équipe d'informaticiens de proximité qui étudiera avec l'équipe réseaux de la Direction des Systèmes d'Information et du Numérique, une solution adaptée.

4 Matériel professionnel

Tout matériel financé par Nantes Université et mis à disposition dans le cadre professionnel est propriété de Nantes Université et inventorié en tant que tel.

4.1 Principes généraux

Lorsqu'un équipement, de type ordinateur fixe ou portable, téléphone, smartphone, tablette, appareil photo numérique, caméscope, dictaphone, vidéoprojecteur…est confié à un utilisateur de Nantes Université, cette mise à disposition :

- fait l'objet d'une consignation d'inventaire ;
- est réputée intervenir dans le cadre exclusif des activités professionnelles du bénéficiaire ;
- entraîne l'obligation pour le bénéficiaire d'apporter tous les soins nécessaires à la bonne conservation de ce matériel.

Le bénéficiaire doit veiller particulièrement à :

- sécuriser le matériel ;
- ne pas le laisser sans surveillance, ni l'exposer à convoitise ;
- ne pas le prêter à un tiers ;
- l'utiliser et le stocker en respectant les conditions prévues.

4.2 Vol / Perte / Détérioration

4.2.1 En cas de vol de l'équipement confié

- une déclaration doit être effectuée sans délai au commissariat de police ou à la gendarmerie le ou la plus proche.

Les informations (date, n° du dépôt de plainte…) doivent être reportées dans l'application Refmat (https://refmat-prod.intra.univ-nantes.fr/). Une copie de la déclaration est transmise au service juridique de Nantes Université.

4.2.2 En cas de perte de l'équipement confié

- une déclaration détaillée doit être effectuée sans délai au commissariat de police ou à la gendarmerie le ou

la plus proche.

Les informations (date, n° du dépôt de main-courante…) doivent être reportées dans l'application Refmat (https://refmat-prod.intra.univ-nantes.fr/). Une copie de la déclaration est transmise au service juridique de Nantes Université.

Toute fausse déclaration est passible de sanctions disciplinaires et/ou de poursuites pénales.

4.2.3 Détérioration

En cas de détérioration d'un matériel mis à disposition, celui-ci doit être restitué avec un descriptif des dommages constatés et un exposé des circonstances à l'origine de la détérioration.

5 Messagerie électronique

L'utilisation de la messagerie électronique constitue l'un des éléments essentiels d'optimisation du travail et de collaboration au sein de Nantes Université.

La messagerie est un outil de travail destiné à des usages professionnels, mais elle peut également constituer le support d'une communication privée telle que définie au chapitre 2.1.

5.1 Adresses électroniques

Nantes Université met à la disposition de l'utilisateur une boîte aux lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

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.

L'adresse électronique nominative est attribuée à un utilisateur qui peut autoriser, à son initiative et sous sa responsabilité, l'accès de tiers à sa boîte aux lettres.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en œuvre 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 catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de Nantes Université : ces adresses ne peuvent être utilisées sans autorisation explicite.

Par principe, l'adresse électronique attribuée par l'administration au personnel de Nantes Université prend, sous réserve des cas d'homonymie, la forme prenom.nom@univ-nantes.fr

L'adresse électronique attribuée par l'administration aux étudiants de Nantes Université prend, sous réserve des cas d'homonymie, la forme prenom.nom@etu.univ-nantes.fr

5.2 Charte du bon usage du courrier électronique

L'utilisateur s'engage à respecter la charte du bon usage du courrier électronique dont Nantes Université s'est dotée. Cette charte définit les conditions générales d'utilisation du service de messagerie électronique et rappelle des pratiques de bon sens, qui peuvent contribuer à améliorer la qualité de vie au travail, en veillant à la séparation vie professionnelle / vie privée.

Il en va aussi de la démarche éthique de l'Université, qui est de veiller au bien-être de ses personnels et d'accompagner au mieux ses étudiants durant leur parcours universitaire.

La charte du bon usage du courrier électronique de Nantes Université est accessible en ligne et notamment sur l'intranet[4].

5.3 Vigilance et sécurité

Caractère probant des courriels

Les informations échangées par voie électronique avec des tiers peuvent, au plan juridique, former un contrat sous certaines conditions ou encore être utilisées à des fins probatoires.

L'utilisateur doit, en conséquence, être prudent sur la nature des informations qu'il échange par voie électronique au même titre que pour les courriers traditionnels.

L'utilisateur est informé que le courriel est un document administratif pouvant être reconnu en tant que preuve en cas de contentieux.

Vigilance et sécurité

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

Par conséquent, l'utilisateur doit respecter les consignes suivantes :

- Ne jamais communiquer d'informations sensibles par messagerie ou téléphone
  Aucune administration ou société commerciale sérieuse ne demandera des données bancaires ou des mots de passe par message électronique (mail ou SMS) ou par téléphone.
- Avant de cliquer sur un lien douteux, positionner le curseur de la souris sur le lien (sans cliquer)
  L'adresse vers laquelle le lien pointe réellement sera alors affichée, il est ainsi possible d'en vérifier la vraisemblance. Il est souvent plus sûr d'aller directement sur le site officiel de l'organisme en question.
- Vérifier l'adresse du site qui s'affiche dans le navigateur
  Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois,

[4] https://intraperso.univ-nantes.fr/documents-procedures/documents-dsin/charte-du-courrier-electronique-le-bon-usage-de-le-mail-pour-eviter-les-maux

un seul caractère peut changer dans l'adresse du site pour tromper l'utilisateur. Au moindre doute, ne fournir aucune information et fermer immédiatement la page correspondante.

- Ne pas ouvrir de fichiers en provenance d'un expéditeur inconnu, en particulier les fichiers compressés ou exécutables dont l'ouverture peut déclencher l'activation de virus, de codes malveillants susceptibles d'entraîner des conséquences graves pour le système d'information de l'Université.

En cas de doute, contacter support-securite@univ-nantes.fr et/ou votre équipe informatique de proximité.
N'hésitez pas à transmettre tout mail suspect à l'adresse traitementspam@univ-nantes.fr

6 Internet

6.1 Dispositions générales

Il est rappelé que l'accès à Internet est soumis à l'ensemble des règles de droit en vigueur. En particulier, l'utilisation d'internet doit être conforme à la charte RENATER[5] (le réseau de Nantes Université est en effet raccordé à Internet via le réseau national RENATER).

Les ressources, services et applications accessibles sur Internet constituent un outil de travail ouvert à des usages professionnels. Si une utilisation résiduelle privée, telle que définie au chapitre 2, peut être tolérée, il est rappelé que l'utilisation d'internet depuis les outils numériques ou les réseaux mis à disposition par l'Université est présumée avoir un caractère professionnel.

Il est précisé qu'une consommation raisonnable de contenus multimédia, comme les vidéos en particulier, contribue aux enjeux de sobriété numérique.

6.2 Publication sur les sites Internet et intranet de l'institution

Toute publication de pages d'information sur les sites Internet ou intranet de l'Université 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 de l'Université n'est autorisée, sauf disposition particulière.

[5] https://www.renater.fr/IMG/pdf/charte_fr.pdf

6.3 Réseaux sociaux

Les réseaux sociaux permettent aujourd'hui une grande liberté d'expression. Ils peuvent par mégarde exposer au vu de tous des informations au départ destinées à un cercle restreint.

Au-delà d'une utilisation privée, les pages sur les réseaux sociaux qui se réclament de l'Université doivent faire l'objet d'une communication maîtrisée. L'Université reste garante en dernier ressort de la qualité éditoriale et de l'exactitude des contenus présents.

Ces pages ne doivent être publiées que par des personnes habilitées.

L'Université propose un guide d'utilisation des réseaux sociaux accessible en ligne et notamment sur l'intranet[6].

6.4 Règles de sécurité

Afin de maintenir son système d'information et l'accès à internet dans de bonnes conditions de sécurité et de fonctionnement, l'Université peut :

- filtrer ou interdire l'accès à certains sites ;
- limiter le téléchargement de certains fichiers trop volumineux ;
- bloquer le téléchargement de fichiers présentant un risque pour la sécurité des systèmes d'information, tels les virus, codes malveillants ou programmes espions.

L'accès à internet n'est autorisé qu'au travers des dispositifs mis en place par l'Université. Il est interdit de connecter au réseau de l'Université des bornes Wi-Fi, des box d'accès à internet ou des ordinateurs équipés d'une clé 3G/4G/5G en activité, qui créeraient ainsi une interconnexion non maîtrisée avec internet.

L'Université conduit régulièrement des campagnes de sensibilisation ou des actions de formation informant l'utilisateur des risques et limites inhérents à l'utilisation d'internet, et veille à donner les conseils de sécurité appropriés.

6.5 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 tels que rappelés au chapitre 7 de la présente charte.

[6] https://intraperso.univ-nantes.fr/documents-procedures/outils-de-communication/conseil-accompagnement-en-communication/charte-et-guide-des-reseaux-sociaux

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'Université, codes malveillants, programmes espions…).

7 Respect de la propriété intellectuelle

7.1 Principes généraux

Nantes Université rappelle que l'utilisation des moyens numériques 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 et les abonnements à des ressources en ligne dans le strict respect des licences souscrites ;
- S'abstenir de 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 autre droit privatif, sans avoir obtenu préalablement l'autorisation du ou des titulaires de ces droits.

7.2 Anti-plagiat

Nantes Université est engagée contre le plagiat, afin de garantir la qualité de ses diplômes et l'originalité des publications pédagogiques et scientifiques de ses personnels enseignants et/ou chercheurs. Les travaux quels qu'ils soient (devoirs, comptes rendus, mémoires, cours, articles, thèses), réalisés aussi bien par les étudiants que par les personnels universitaires, doivent toujours avoir pour ambition de produire un savoir inédit et d'offrir une lecture nouvelle et personnelle d'un sujet.

La Charte anti-plagiat de Nantes Université approuvée en Conseil d'Administration du 21 octobre 2011 définit les règles à respecter en la matière, par l'ensemble des étudiants et universitaires.

Dans le cadre de sa démarche de mise en place d'outils de prévention et de détection du plagiat, conformément à son règlement intérieur (section 2, articles 28 à 31), Nantes Université met à disposition de ses enseignants-chercheurs un logiciel de détection de similitudes.

La Charte anti-plagiat de Nantes Université et l'ensemble de ces documents est accessible en ligne et notamment sur l'intranet[7].

8 Protection des données à caractère personnel

8.1 Droit d'accès

Nantes Université a nommé un Délégué à la Protection des Données (anciennement Correspondant Informatique et Libertés ou CIL), chargé de s'assurer de la bonne application de la réglementation « Informatique et Libertés » en son sein.

Conformément aux dispositions de cette loi et du « Règlement Général sur la Protection des Données » européen, chaque utilisateur dispose d'un droit d'accès, de rectification, d'opposition, de limitation et de portabilité relatif à l'ensemble des données personnelles le concernant. Ce droit s'exerce[8] auprès du Délégué à la Protection des Données de l'établissement : dpo@univ-nantes.fr

8.2 Création de fichiers nominatifs

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.

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations, 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 » et le « Règlement Général sur la Protection des Données » européen.

[7] https://intraperso.univ-nantes.fr/dossier-plagiat-784821.kjsp?RH=1504693814319

[8] https://intraperso.univ-nantes.fr/documents-procedures/documents-juridiques-et-institutionnels/quand-contacter-le-dpo-et-que-declarer-quelques-exemples

Tout utilisateur souhaitant procéder à un tel traitement devra préalablement prendre contact avec le Délégué à la Protection des Données qui définira avec lui les mesures nécessaires au respect des dispositions légales.

9 Journalisation

Conformément à la législation, l'Université met en œuvre un système de « journalisation » des accès Internet, de la messagerie et des données échangées.

Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée, ce traitement de données est inscrit au registre des traitements de l'établissement.

Plus largement, l'Université informe l'utilisateur que le système d'information fait l'objet d'une surveillance de bon fonctionnement, incluant des mesures à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus. Ces mesures sont chaque fois que possible anonymisées. Les personnels chargés des opérations de contrôle sont soumis au secret professionnel, respectent la législation en vigueur et la charte des administrateurs du système d'information.

Les utilisateurs sont informés que la durée légale de conservation des fichiers de journalisation est d'une année à partir de la date d'enregistrement.

9.1 Demande de réquisition judiciaire

Dans le cas d'une réquisition judiciaire, l'Université sera tenue de communiquer, ou d'exploiter pour recherche, toutes les traces contenues dans ses journaux concernant la ou les personnes incriminées.

10 Limitations des usages

En cas de non-respect par un utilisateur des règles définies dans la présente Charte, la Direction des Systèmes d'Information et du Numérique pourra déconnecter l'utilisateur, avec ou sans préavis selon la gravité de la situation, et/ou limiter ses accès pour une durée déterminée.

La Direction Générale des Services ou la Présidence pourra, après en avoir averti l'intéressé et sans préjuger des poursuites ou procédures de sanction pouvant être engagées à son encontre, limiter les usages par mesure conservatoire, interdire à l'utilisateur l'accès à des ressources (par exemple l'accès à internet), ou retirer les droits ou autres dispositifs de contrôle d'accès et fermer les comptes.

11 Entrée en vigueur de la charte

La présente charte sera annexée au règlement intérieur de Nantes Université.

La présente charte s’articule avec tous les autres documents ou chartes relatifs à l’utilisation des moyens numériques.

Sont annexés à cette charte les documents suivants :

- Charte RENATER ;
- Charte du Courrier Electronique ;
- Charte Anti-plagiat ;
- Charte des administrateurs du système d’information ;
- Charte sur les modalités d'utilisation des technologies de l'information et de la communication par les organisations syndicales à l'Université de Nantes ;
- Annexe des principaux textes réglementaires.

La Directrice générale des services,

Direction des Systèmes d'Information et du Numérique

https://intraperso.univ-nantes.fr/