Charte Informatique de l'université Toulouse III - Paul Sabatier

Version adoptée par le Conseil d'Administration

de l'université du 03 avril 2017

Table des matières

Préambule

L'Université Toulouse III - Paul Sabatier met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Elle met ainsi à disposition de ses collaborateurs et usagers des outils informatiques et des moyens de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation de ces outils informatiques et des moyens de communication de l'Université. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'établissement.

La charte est diffusée à l'ensemble des utilisateurs par tout moyen et à chaque modification. A ce titre, elle est disponible sur le site Internet institutionnel de l'Université. Elle est systématiquement communiquée à tout nouvel arrivant. Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Définitions

Chargé·e de la sécurité des SI (CSSI) : Il (elle) est désigné·e par le·a responsable de structure. Il (elle) participe à la mise en œuvre de la sécurité du SI de l'établissement dans son périmètre, assiste et conseille le·a responsable de la structure en relation avec le·a RSSI.

Correspondant·e informatique et libertés (CIL) : Correspondant·e à la protection des données à caractère personnel.

Donnée à caractère personnel : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Une personne est identifiée lorsque son nom apparaît dans un fichier. Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification : adresses postale et électroniques (mail, IP *identification de la machine utilisée*) ; numéro d'immatriculation ou de compte bancaire, identifiants de connexion, numéro de téléphone, numéro de sécurité sociale ; photographie ; voix ; données de localisation...

Une donnée à caractère personnel peut donc aussi être une donnée professionnelle.

Équipements nomades : tous les moyens techniques mobiles (ordinateur portable, imprimante portable, tablette, téléphone mobile ou smartphone, objet connecté, CD ROM, clé USB, disque dur amovible etc…).

Informations d'authentification : identifiant, mot de passe, code pin, clés privées, etc.

Information professionnelle : information utilisée en contexte de travail. Sa sensibilité est qualifiée selon quatre critères (publique, interne, confidentielle, secrète).

Outils informatiques et de communication : tous les équipements informatiques, de télécommunications et de reprographie de l'Université.

Référent·e informatique et libertés (RIL) : Il (elle) est désigné(e) par le·a responsable de structure. Il (elle) participe à la mise en œuvre de la politique de protection des données de l'établissement dans son périmètre, assiste et conseille le·a responsable de la structure en relation avec le/la CIL.

Responsable de la sécurité des SI (RSSI) : Il (elle) est désigné·e par le·a président·e de l'Université Toulouse III. Il (elle) est Responsable de la sécurité des Systèmes d'Information.

Sécurité physique : concerne tous les aspects liés à l'environnement dans lequel les systèmes se trouvent.

Sécurité logique : la sécurité logique fait référence à la réalisation de mécanismes techniques de sécurité par logiciel.

Site malveillant : désigne tout site Web conçu pour faire accomplir à un utilisateur légitime des actions indésirables ou néfastes pour la sécurité du SI.

Structure : entité administrative ou d'enseignement ou de recherche rattachée à l'établissement (services centraux, communs ou inter-universitaires ; composantes ; instituts ; écoles doctorales ; unités de recherches propres ou mixtes dont la tutelle principale est l'Université Toulouse III - Paul Sabatier).

Système d'information (SI) : ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications mis à disposition par l'Université.

Tiers : une application, une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisés à traiter les données à caractère personnel - Règlement (UE) 2016/679 du 27 avril 2016.

Traitements de données : opérations informatisées portant sur des données telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Utilisateur : toute personne autorisée à accéder et à utiliser les outils informatiques et moyens de communication de l'Université (agents titulaires ou contractuels, étudiants, intervenants extérieurs, visiteurs, invités, etc.).

Article I. Champ d'application

La présente charte s'applique à tout utilisateur du système d'information et de communication de l'Université Toulouse III - Paul Sabatier quelles que soient ses activités.

Les usages relevant de l'activité des organisations syndicales sont régis par une charte conforme au décret n° 2014-1319 du 4 novembre 2014 et la décision ministérielle du 24 mai 2016[1].

Article II. Conditions d'utilisation du système d'information

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle ou universitaire dans les conditions définies par l'Université.

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 auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[2].

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

II.1. Utilisation professionnelle / privée

Le système d'information est composé d'outils de travail permettant la réalisation d'activités de recherche, d'enseignement, administratives ou de vie universitaire. Toute information traitée dans ce cadre 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 et à la sauvegarde des données dans un dossier intitulé *« Privé ».*

L'utilisation du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. L'espace utilisé ne doit pas occuper une part excessive des ressources. 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 de l'établissement.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur. Par exemple, le téléchargement illégal, la détention, diffusion et exportation d'images à caractère pédophile[3], ou la diffusion de contenus à caractère raciste ou antisémite[4] est interdite.

Cas particulier de l'utilisation de ressources informatiques personnelles :

L'utilisation de ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc… achetés sur des fonds personnels), lorsque celles-ci sont utilisées pour accéder localement ou à distance aux ressources de l'Université, ne doit pas remettre en cause ou affaiblir les politiques de sécurité en vigueur par une protection insuffisante ou une utilisation inappropriée. Ces ressources personnelles doivent être conformes aux règles de sécurité édictées dans la présente charte.

1 Décret n° 2014-1319 du 04-11-2014 relatif aux conditions d'accès aux technologies de l'information et de la communication et à l'utilisation de certaines données par les organisations syndicales dans la fonction publique de l'État ;
Décision (NOR : MENH1610318S) relative aux conditions et aux modalités d'utilisation des technologies de l'information et de la communication par les organisations syndicales.

2 Par exemple le secret médical dans le domaine de la santé.

3 Code pénal, articles L 323-1 et suivants.

4 Loi du 29 juillet 1881, articles 24 et 24 bis.

Les personnels qui souhaiteraient utiliser de tels matériels pour un usage professionnel demanderont préalablement l'autorisation au ou (à la) responsable de structure et prennent conseil auprès de leur service informatique de proximité. Les données professionnelles (qui sont la propriété de l'Université Toulouse III) ne doivent pas être enregistrées ou stockées sur les ressources informatiques personnelles.

II.2. Continuité de service : gestion des absences et des départs

Lors de son départ ou d'une absence prolongée, l'utilisateur doit remettre tous les documents professionnels (administratifs, recherche et pédagogiques…) à son (sa) responsable de structure ou lui permettre d'y accéder. En cas d'indisponibilité de l'utilisateur, son (sa) responsable de structure peut demander au service informatique de proximité d'accéder à tous les documents et informations professionnels (hors dossier « Privé »).

Les comptes et les données professionnelles, les dossiers spécifiquement nommés *« Privé »* de l'utilisateur sont supprimés dans un délai maximum d'un mois à compter de la date de son départ définitif.

L'utilisateur est responsable de la suppression des données stockées dans son dossier *« Privé ».* La responsabilité de l'établissement ne pouvant être engagée quant à la conservation de ces données.

L'utilisateur doit restituer au service de l'informatique de proximité, les matériels (ordinateurs portables, téléphones, disques durs externes, clés USB…) mis à sa disposition par l'établissement.

En cas de circonstances exceptionnelles (départ impromptu), le service informatique de proximité ne conservera que trois mois maximum les espaces de données à caractère privé présents sur les ressources informatiques, délai permettant à l'utilisateur ou ses ayants droit de récupérer les informations.

Article III. Principes de sécurité

Les principes suivants ont pour objectif de protéger les informations qui constituent le patrimoine immatériel de l'Université contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité des systèmes d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteintes au fonctionnement de l'organisme, au potentiel scientifique et technique ou à la vie privée).

III.1. Règles de sécurité applicables

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

L'utilisateur est informé que les informations d'authentification qui lui sont attribuées constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.

Les niveaux d'accès au système d'information ouverts à l'utilisateur sont définis en fonction de missions qui lui sont confiées. Il est responsable de l'utilisation des systèmes d'information auxquels il accède avec les droits qui lui sont conférés par son (sa) responsable de structure. En cas d'évolution de ses missions une nouvelle autorisation est délivrée par le·a responsable de structure.

La sécurité des ressources mises à la disposition de l'utilisateur lui impose le respect des règles suivantes :

de la part de l'Université **:**

- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément autorisé ;
- Garantir la disponibilité, l'intégrité et la confidentialité des données de l'utilisateur.

de la part de l'utilisateur :

- Se conformer aux directives de sécurité concernant les usages :
  - relatifs à la connexion :
    - appliquer la politique de gestion des mots de passe de l'Université Toulouse III ;
    - garder strictement confidentiel ses informations d'authentification ;
    - ne pas utiliser les informations d'authentification d'un autre utilisateur, ni chercher à les connaître ;
    - ne pas enregistrer ses informations d'authentification sur des applications ou espaces non maîtrisés par l'Université ;
    - ne pas masquer sa véritable identité, ne pas usurper l'identité d'autrui, ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas, s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'autorisation explicite ;
    - ne pas se connecter à des sites Internet malveillants ;
    - s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations du matériel ou du logiciel ;
    - verrouiller ou fermer toutes les sessions en cours sur son poste de travail, en cas d'absence, même momentanée ;
    - s'assurer que toute personne externe susceptible d'accéder au Système d'Information de l'Université y est autorisée par le·a responsable de structure. Cette autorisation comprend l'engagement de respecter la présente charte.

  - relatifs aux données et documents professionnels :
    - protéger les informations qu'il est habilité à manipuler dans le cadre de ses fonctions, selon leur sensibilité. Lorsqu'il crée un document, l'utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression, etc.) ;
    - n'opérer les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des sites hébergés ou faisant l'objet d'une convention signée par l'Université et dont la sécurité a été vérifiée par celle-ci ;
    - ne pas utiliser des supports de données tels que (ordinateur, clé USB, CDROM, DVD, cloud, etc…) sans respecter les règles de sécurité de l'Université et prendre les précautions nécessaires pour s'assurer de leur innocuité ;
    - respecter les règles définies par l'Université, obtenir l'autorisation de son (sa) responsable de structure pour tout traitement de données réalisé sur un support externe ;
    - mettre en œuvre un système de sauvegarde manuel lorsque des sauvegardes automatiques ne sont pas prévues ;
    - s'assurer que son poste de travail est verrouillé lorsqu'il s'absente de son bureau afin de se prémunir contre les risques de vol de documents sensibles. De la même manière s'assurer que les dispositions contractuelles avec des intervenants extérieurs comportent les clauses rappelant les rôles et les obligations des acteurs concernés.

- Respecter les consignes de sécurité concernant le matériel ou les logiciels :
    - ne pas modifier les paramétrages du poste de travail ;
    - ne pas installer, télécharger ou utiliser des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites de confiance, ou sans autorisation de son (sa) responsable de structure ;
    - ne pas copier, modifier, détruire les logiciels propriétés de l'Université ;
    - respecter les dispositifs mis en place par l'Université pour lutter contre les virus et les attaques par programmes informatiques ;
    - utiliser les moyens de protection mis à disposition contre le vol (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu'ils contiennent (ordinateur portable, disque dur, clé USB, smartphones, tablettes, etc.) ;
    - ne pas désactiver, ni altérer le fonctionnement ou désinstaller l'outil de cryptage lorsqu'il a été installé par l'Université ;
    - adapter la sécurité (physique et logique) des équipements nomades en fonction de la sensibilité de l'information qu'ils traitent et stockent.

- Signaler le plus rapidement possible au (à la) chargé·e de la sécurité des SI tout logiciel ou dispositif suspect ainsi que toute perte, tout vol ou toute compromission suspectée ou avérée :
    - d'un équipement stockant des données professionnelles ;
    - de ses informations d'authentification (identifiant, mot de passe, code pin, clés privées, etc.).

III.2. Mesures de contrôle de la sécurité

L'utilisateur est informé que :

- L'Université peut intervenir (y compris à distance) sur les ressources mises à sa disposition pour effectuer une maintenance corrective, curative ou évolutive ;
- La maintenance à distance de son poste de travail est réalisée avec information préalable ;
- Toute information bloquante ou générant une difficulté technique pour le système sera isolée et/ou supprimée ;
- Des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Ce filtrage peut être neutralisé sur autorisation du (de la) responsable de structure pour des raisons uniquement professionnelles ;
- Les services informatiques disposent d'outils techniques pour procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Article IV. Outils de communication

IV.1. Messagerie électronique

L'utilisation de la messagerie constitue un élément essentiel d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'Université.

Adresses électroniques

L'Université met à la disposition de l'utilisateur (sauf cas particulier) une adresse électronique professionnelle nominative lui permettant d'émettre et de recevoir des messages. L'utilisation de cette adresse électronique relève de la responsabilité de son détenteur. Son utilisation est interdite sur des sites sans rapport avec son activité professionnelle. 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 boite aux lettres électronique peut également être délivrée par une entité (laboratoire, institut...). Cette adresse doit aussi être utilisée dans un cadre strictement professionnel.
Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'Université.
La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'Université : ces listes ne peuvent être utilisées sans autorisation explicite.

Contenu des messages électroniques

Tout message est réputé professionnel. Les messages à caractère personnel sont tolérés, ils doivent être signalés par la mention « [Privé] » dans leur objet et être classés dès l'envoi dans un dossier nommé *« Privé »*. De même les messages reçus doivent être également classés dans un dossier nommé « Privé ». Il est recommandé d'utiliser sa messagerie personnelle pour l'envoi et la réception de messages présumés à caractère personnel.
Un message électronique à la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de limiter l'envoi de messages non sollicités afin de ne pas engager la responsabilité civile ou pénale de l'Université et/ou de l'utilisateur. 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 messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369-1 à 1369-11 du code civil. L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels. Le courriel est un document administratif reconnu en tant que preuve en cas de contentieux.

Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.
Les messages électroniques envoyés font l'objet d'un contrôle automatique antiviral. Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération lors d'envoi de correspondances importantes. Les messages importants sont envoyés avec une demande d'accusé de réception. La transmission de données confidentielles par messagerie électronique est interdite sauf utilisation d'un dispositif de cryptage agréé par l'ANSSI (Agence Nationale de la Sécurité du Système d'Information – https://www.ssi.gouv.fr/).

Les messages électroniques reçus font l'objet d'un contrôle automatique antiviral et anti-spam. L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage…).
Afin de préserver le bon fonctionnement du service de messagerie, la transmission de messages électroniques n'est possible que vers un nombre limité de destinataires. Cette limite peut être levée par l'utilisation de listes de diffusion ouvertes sur demande auprès de la Direction des systèmes d'information. De même, la taille, le nombre et/ou le type des pièces jointes peuvent être limités pour éviter l'engorgement ou la dégradation du système de messagerie.
La capacité de stockage des messages électroniques est limitée. Les services informatiques peuvent donc demander aux utilisateurs de supprimer des messages. Si l'utilisateur souhaite conserver ces messages, il lui appartient de les archiver.

IV.2. Internet

L'établissement est signataire de la charte RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche – https://www.renater.fr/IMG/pdf/charte_fr.pdf). Dans ce cadre il se doit de faire respecter les règles déontologiques qui y sont décrites. Par ailleurs, il est rappelé qu'Internet est soumis au respect de l'ensemble des règles de droit en vigueur.

L'outil Internet mis à disposition permet de consulter tous types de sites présentant un lien direct et nécessaire avec l'activité professionnelle de l'utilisateur. Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites Internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne mettant pas en cause l'intérêt et la réputation de l'établissement, est admise. En cas de suspicion d'atteinte à la sécurité du système d'information (SSI) et des données de l'Université, tous les flux chiffrés (ex : https, smtps, imaps…) peuvent être décryptés.

L'Université 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. Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Université. 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.
Les utilisateurs se doivent d'adopter un comportement loyal vis-à-vis de leur employeur lors de l'utilisation des réseaux sociaux, des blogs, qu'ils soient professionnels (Linkedin, Viadeo, autres sites) ou non professionnels (Facebook, Twitter, autres sites).
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.

Seuls les « clouds » dont les règles de sécurité sont maîtrisées et validées par l'Université peuvent être utilisés pour le dépôt de données professionnelles. Ceci exclut de facto les « clouds » de type Google Drive, Dropbox, iCloud, OneDrive etc.

IV.3. Téléchargements

Le téléchargement de logiciels ou d'œuvres protégées, doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VII, il doit être fait dans le cadre d'usages professionnels.
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…).

IV.4. Publication sur les sites Internet et intranet de l'Université

Le·a Président·e de l'Université, en tant que représentant·e légal·e, est le·a Directeur (directrice) de publication de l'établissement pour les sites Internet mis en œuvre par l'établissement. Toute publication de pages d'information sur les sites Internet ou intranet de l'Université doit être conforme à la politique Internet de l'établissement et validée par un·e responsable de publication désigné·e.

Préalablement à un projet de diffusion sur un site Internet, extranet, intranet d'informations relatives à des personnes, le service prendra attache auprès du (de la) correspondant·e informatique et libertés (cf. article VIII).
Aucune publication de pages d'information à caractère privé n'est autorisée sur les ressources du système d'information de l'Université, sauf cas particulier autorisé par le·a Président·e.
Chaque site rattaché au nom de domaine de l'établissement doit comporter les mentions légales obligatoires et pointer également sur la rubrique dédiée « mentions légales » du site de l'Université.
Toute publication devra respecter la réglementation en vigueur et notamment celle relative à l'accessibilité.
Les informations publiées sur les sites du domaine Université Toulouse III - Paul Sabatier doivent également être fiables et régulièrement mises à jour.

Article V. Traçabilité

L'Université informe l'utilisateur que le système d'information est surveillé et contrôlé dans le respect de la législation applicable, à des fins de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité, de détection des abus et fraudes (notamment fraude aux examens, détournement de finalité des applicatifs de gestion, etc.), ainsi qu'à des fins statistiques suivant la politique de gestion des traces de l'Université Toulouse III.
Les services informatiques de l'Université opèrent, sans avertissement, les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'un de ses composants. Ils s'appuient pour ce faire, sur des fichiers de journalisation (appelés également « traces », « journaux » ou « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent au minimum les données suivantes : date, identifiant et type d'événement.
Ces fichiers de journalisation sont conservés au minimum trois mois et au maximum douze mois selon la réglementation applicable au type de données conservées.

Article VI. Confidentialité

Tout utilisateur autorisé à accéder aux données du SI de l'Université s'engage à maintenir confidentielle l'information à laquelle il accède dans le cadre de ses fonctions. Les utilisateurs autorisés à accéder à l'information du SI de l'Université doivent être vigilants vis-à-vis des données auxquelles ils accèdent au sens de la politique de sécurité des systèmes d'information.
L'utilisateur est responsable des fichiers et répertoires qu'il constitue. Il est cependant interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas correctement protégées.
L'utilisateur ne doit pas tenter d'intercepter des communications entre tiers.
L'information collectée et contenue dans les fichiers et les bases de données exploitées par l'établissement a un caractère confidentiel. La manipulation et l'exploitation des données doivent être conformes aux dispositions consignées dans les déclarations CNIL.
La communication de données à caractère personnel doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées.
Tout projet de transmission interne ou externe de données doit être soumis à l'autorisation du (de la) responsable de structure et du (de la) correspondant·e à la protection des données à caractère personnel.
En cas d'absence d'un utilisateur, toute mesure indispensable à la continuité du service peut être mise en œuvre sous couvert de son responsable de structure.

Article VII. Respect de la propriété intellectuelle

L'université rappelle que l'utilisation de ses 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 protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Par ailleurs, l'usage des ressources documentaires doit être conforme au contrat de mise à disposition de l'éditeur validé par l'Université. Notamment, le téléchargement massif et systématique de ressources documentaires par l'intermédiaire d'un robot ou de tout autre logiciel est interdit.

Article VIII. Respect de la loi informatique et libertés

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite *« Informatique et Libertés »* modifiée.
Toute création de fichiers comprenant des informations à caractère personnel 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 » et au règlement européen référencé en annexe de la présente charte.
En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le·a référent·e informatique et libertés de sa structure qui prendra les mesures nécessaires au respect des dispositions légales. Par ailleurs, le·a correspondant·e à la protection des données à caractère personnel de l'Université doit être saisi·e préalablement à la mise en œuvre des traitements de données pour valider leur conformité légale.
En outre, 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 des systèmes d'information.
Ce droit s'exerce auprès du Cabinet du (de la) Président·e, 118 route de Narbonne 31062 TOULOUSE CEDEX 9, pour les étudiants et extérieurs et du (de la) responsable hiérarchique de la structure dont dépend l'agent souhaitant exercer ses droits, pour les personnels. Le·a correspondant·e à la protection des données à caractère personnel est informé·e par transmission d'une copie de toute demande d'accès, de rectification et d'opposition à l'utilisation des données personnelles.

Article IX. Limitation des usages et sanctions

L'utilisateur est tenu de respecter l'ensemble des règles définies dans la présente charte, ainsi que les textes de référence applicables annexés (cf. annexe).
Tout manquement à ces règles et mesures de sécurité et de confidentialité énoncées est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre :

- Des sanctions disciplinaires ou pénales en fonction de la gravité des faits constatés par les instances compétentes ;

- L'établissement pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre de l'utilisateur malveillant, délivrer un avertissement, limiter ou suspendre les usages, sans préavis par mesure conservatoire ;
- Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est également passible de sanctions.

Article X. Entrée en vigueur de la charte

La présente charte annule et remplace tous documents relatifs à l'utilisation des systèmes d'information de l'Université Toulouse III - Paul Sabatier.
Elle a été adoptée après information et consultation des représentants des personnels et des étudiants de l'établissement.
Elle est applicable à compter du 03 Avril 2017, date de son approbation par le Conseil d'Administration de l'Université Toulouse III - Paul Sabatier.
Elle est annexée au règlement intérieur de l'établissement.

Annexe - Principaux textes de référence applicables

- Règlement européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (abrogeant la directive 95/46/CE sur la protection des données) ;
- Loi du 29 juillet 1881 modifiée sur la liberté de la presse ;
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Charte déontologique RENATER https://www.renater.fr/IMG/pdf/charte_fr.pdf.
- Dispositions Pénales :
  - Code Pénal (partie législative) : art L.226-16 à 226-24, art L323-1 à 323-3 et art L.335-2
  - Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13
  - Loi n° 94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels ;
  - Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) ;
  - Code de la propriété intellectuelle relative à la propriété littéraire et artistique ;
  - Les dispositions relatives au respect de la vie privée, de l'ordre public, du secret professionnel ;
  - Les dispositions relatives à la Protection du Potentiel Scientifique et Technique de la Nation.