Charte régissant l'usage des ressources du système d'information de l'Université d'Orléans

Glossaire

Acronymes

DPD	Délégué à la Protection des Données
CIL	Correspondant Informatique et Liberté
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'Information

Définitions

Activité universitaire	L'activité universitaire est celle découlant des missions de l'université définies par la loi, à savoir : les activités de recherche, d'enseignement, de développement technique, de transfert de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant de ses activités.
Code ou logiciel malveillant	Code ou logiciel développé dans le but de nuire aux ressources d'un SI. Les virus, vers, chevaux de Troie ou bombes logiques constituent des exemples de *codes ou de logiciels malveillants*
Donnée à caractère personnel	Donnée qui permet d'identifier directement ou indirectement les personnes physiques. Il peut s'agir d'informations qui ne sont pas nécessairement associées au nom d'une personne mais qui permettent aisément de l'identifier et de connaître ses habitudes et ses goûts. Exemples : nom, lieu de résidence, profession, éléments biométriques.
Entité	Entité existante au sein de l'Université, de ses composantes, services communs et services centraux pour l'accomplissement de ses missions. Exemples : laboratoires, départements ou filières d'enseignement, services administratifs ou techniques.
Messagerie	La messagerie électronique comprend les systèmes de courrier électronique, de messagerie instantanée et messagerie texte (SMS).
Personne juridiquement responsable	Toute personne ayant la capacité de représenter l'Université (président, vice-président, directeur, etc.).
Responsable de la Sécurité des Systèmes d'information	Il est chargé avec son adjoint, par le Président de l'Université, d'assurer la sécurité des systèmes d'information de l'Université d'Orléans.

Responsable de l'utilisateur	Le responsable de l'utilisateur est : - Pour les agents titulaires ou non titulaires concourant à l'exécution des missions du service public de l'éducation et des stagiaires : le responsable hiérarchique ; - Pour les enseignants, chercheurs et enseignants chercheurs : le directeur de la composante ou de l'unité de recherche ; - Pour les étudiants : l'enseignant ; - Pour les prestataires : le responsable interne à l'université du contrat de prestation.
Ressources du Système d'information	Ensemble des ressources techniques, applicatives, organisationnelles, humaines et documentaires permettant de collecter, stocker, traiter, rechercher et/ou transmettre des données, en particulier : - Tout matériel informatique fixe : postes (dont les postes libre-service), serveurs, téléphones, périphériques (clavier, écran, imprimante, etc.), prises, câbles, … - Tout matériel informatique mobile : ordinateur, téléphone, etc. - Tout logiciel ou service réseau ou informatique : accès réseau, accès Internet, *messagerie* électronique, bureautique, etc. - Tout support de données : électronique, papier, etc.
Utilisateur	Toute personne / individu ayant accès ou utilisant les *ressources du système d'information* de l'Université d'Orléans, quel que soit son statut, en particulier : - Tout agent titulaire ou non-titulaire concourant à l'exécution des missions du service public de l'éducation ; - Tout enseignant, enseignant-chercheur ou chercheur utilisant les ressources de l'Université, y compris les locaux ; - Tout étudiant inscrit ou en cours d'inscription pour l'année en cours, ou ayant été inscrit à l'Université ; - Tout prestataire sous contrat avec l'Université ; - Tout stagiaire utilisant les ressources de l'Université, y compris les locaux ; - Tout lecteur autorisé qui dispose d'un accès aux ressources bibliographiques en ligne ; - Toute personne accédant à un service hébergé par l'Université, y compris le site internet ; - Toute personne accueillie temporairement au sein de l'Université et ayant de ce fait accès à un poste informatique de l'Université et/ou au réseau informatique (conférencier, chercheur invité, etc.).

Article 1 – Présentation

Section 1.1 - Objet

La présente charte définit les règles d'usage et de sécurité que l'*utilisateur* et l'Université s'engagent à respecter.

Elle a pour objet de définir les droits et les devoirs de chacun dans le cadre de l'utilisation des *ressources du système d'information*.

Elle est associée aux chartes des différents fournisseurs d'accès à Internet, notamment la charte RENATER, en ce qui concerne les modalités d'accès au réseau.

Section 1.2 - Domaine d'application

Les dispositions de la présente charte s'appliquent à l'Université ainsi qu'à l'ensemble des *utilisateurs*.

Section 1.3 - Engagements de l'Université

L'Université porte à la connaissance des *utilisateurs* 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 facilite l'accès des *utilisateurs* aux *ressources du système d'information*. Les ressources mises à leur disposition sont prioritairement à usage universitaire, mais l'Université est tenue de respecter l'utilisation du système d'information à titre privé, tel que défini dans la section 2.3.

Section 1.4 - Engagement de l'utilisateur

L'*utilisateur* est responsable, en tout lieu, de l'usage qu'il fait des *ressources du système d'information* de l'Université d'Orléans.

L'*utilisateur* s'engage à respecter les dispositions de la présente charte.

Article 2 – Conditions et règles d'utilisation des ressources du SI

Section 2.1 - Accès et utilisation des ressources du système d'information

L'utilisation des *ressources du système d'information* de l'Université et la connexion d'un équipement externe au système d'information sont soumises à autorisation. Chaque *entité* peut prévoir des restrictions d'accès (carte à puce d'accès, filtrage d'accès sécurisé, etc.) spécifiques à son organisation, sous réserve de validation.

L'*utilisateur* est informé que :

- Ses codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation abusive ou malveillante des *ressources du système d'information* ;
- Ses accès sont définis par l'Université en fonction de son statut ;
- Chaque *utilisateur* peut se voir attribuer un ou plusieurs codes d'accès aux *ressources du système d'information*. Ces codes d'accès peuvent être constitués d'un identifiant unique et nominatif attribué par l'Université et d'un mot de passe choisi par l'*utilisateur*.

Afin d'assurer la sécurité des accès aux *ressources du système d'information*, l'*utilisateur* doit :

- Garder strictement confidentiel(s) son (ses) code(s) d'accès et ne pas le(s) dévoiler à un tiers. L'*utilisateur* est responsable de l'utilisation qui est faite de ses codes d'accès, leur divulgation volontaire à un tiers engage sa responsabilité pénale et civile ;

  Le stockage des codes d'accès doit se faire via le coffre-fort de mots de passe mis à disposition par l'université d'Orléans
- Respecter les règles en vigueur au sein de l'Université concernant les mots de passe ;
- Respecter les consignes de sécurité et les règles relatives aux codes d'accès, en particulier :
  - Ne pas utiliser les codes d'accès d'un autre *utilisateur*, ni chercher à les connaître ;
  - S'interdire d'accéder ou de tenter d'accéder à des *ressources du système d'information* en contournant les droits attribués;
  - Ne pas connecter directement au système d'information des matériels autres que ceux confiés ou autorisés par l'Université.
- S'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des *ressources du système d'information*, que ce soit par des manipulations anormales du matériel (par exemple, débrancher un câble réseau), ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, logiciels d'écoute réseau, etc.

Afin d'assurer la sécurité des accès aux *ressources du système d'information*, l'Université est tenue de :

- Veiller à ce que les ressources ne soient accessibles qu'aux personnes habilitées
- Supprimer, désactiver ou modifier les codes d'accès dès que la situation le justifie : fin de l'activité de l'*utilisateur*, non-respect de la charte, etc.

Pour les accès distants aux *ressources du système d'information*, il est rappelé que les chartes des différents fournisseurs d'accès au réseau Internet empruntés par l'*utilisateur* s'appliquent.

Section 2.2 - Utilisation d'équipements (ordinateur, mobile, tablette) externes au système d'information de l'université (privés ou extérieurs) dans le cadre professionnel

De manière générale seuls les matériels fournis, configurés et gérés par l'université (ou le CNRS dans le cas de laboratoires mixtes) sont autorisés à être connectés au réseau filaire de l'université.

Toutefois, pour répondre à la nécessité de service, l'utilisation d'un équipement externe dans le cadre d'activités professionnelles pourra être autorisée sous conditions :

- L'utilisateur s'engage à utiliser cet équipement uniquement à but professionnel
- L'utilisateur doit avoir reçu l'autorisation du RSSI de l'université après demande motivée du responsable de son entité (service/laboratoire/composante). Le RSSI donnera à cette occasion les prérequis à l'utilisation de ce matériel.
- L'université ne peut être tenue responsable d'éventuels vols ou endommagements du matériel et ni en cas de pertes de données personnelles.

L'autorisation d'utilisation d'un équipement externe dans le cadre d'activités professionnelles fait entrer l'équipement dans les ressources informatiques de l'université et comme tel dans le périmètre de la SSI, ce qui implique que :

- Le propriétaire doit permettre au service informatique d'accéder sans restriction à sa machine, dans le respect du droit à la vie privée et des dispositions de la loi Informatique et Libertés
- L'ordinateur sera soumis aux mêmes règles que les matériels du parc informatique de l'université d'Orléans. (il devra notamment posséder un système d'exploitation à jour, un anti-virus à jour et validé par le RSSI, le proxy authentifié paramétré sur un navigateur)

Section 2.3 - Utilisation des ressources à titre privé

Les *ressources du système d'information* sont des outils mis à disposition pour une utilisation dans le cadre *d'activités universitaires*. L'utilisation de ces moyens peut également constituer le support d'une communication à titre privé dans les conditions décrites ci-après.

L'utilisation résiduelle des *ressources 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 universitaire 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 à cet effet nommé « PRIVE » ou « PERSO ». La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

L'*utilisateur*, lors de son départ de l'Université, est responsable de la destruction de son espace de données à caractère privé, la responsabilité de l'Université quant à la conservation de cet espace ne pouvant être engagée à cet effet.

Les données sont conservées conformément à la réglementation en vigueur.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur.

Section 2.4 - Utilisation des logiciels, données et applications

L'*utilisateur* est tenu de :

- Ne pas consulter, détenir, diffuser et importer des données à caractère pédopornographiques, d'incitation à la discrimination, à la haine ou à la violence ou présentant un caractère raciste ou discriminatoire ;
- Ne pas télécharger, reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, sons, musiques, vidéos ou autres créations protégées par le droit de propriété intellectuelle, en particulier le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- Ne pas consulter, diffuser, supprimer ou altérer des informations ou données détenues par l'Université d'Orléans ou d'autres *utilisateurs* sans leur autorisation, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type *messagerie* électronique dont l'*utilisateur* n'est le destinataire ni directement, ni en copie ;

- Ne pas installer, télécharger ou utiliser volontairement sur le système d'information :
  - Des logiciels non autorisés par l'Université ou non conformes aux missions de l'Université, en particulier des logiciels à caractère ludique ;
  - 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 l'Université ;
  - Des versions d'essai ou d'évaluation de logiciels ;
  - Des *codes ou logiciels malveillants*
- Ne pas désinstaller, modifier ou empêcher la bonne exécution des logiciels, applications et utilitaires installés sur son poste de travail par le service informatique
- Ne pas réaliser des copies de logiciels soumis à licence (exceptées les copies de sauvegarde) ou de mettre à disposition ces logiciels à une tierce personne par l'intermédiaire du réseau ;
- Ne pas contourner les restrictions d'utilisation d'un logiciel autorisé ;
- Informer le *DPD* préalablement à toute création de fichiers contenant des *données à caractère personnel* ou traitement sur ces même données, conformément aux dispositions de la loi Informatique et Libertés ;
- Signaler à tout responsable de l'application source tout constat concernant une donnée de gestion (ex : numéro de téléphone) qui nécessiterait une mise à jour ;
- Signaler rapidement au service informatique tout dysfonctionnement constaté de logiciel, application ou utilitaire installé sur le poste de travail par le service informatique ;
- Respecter la politique de sécurité de l'application ainsi que les règles et procédures en vigueur lors de toute manipulation de données extraites du système d'information.

Lors d'un changement de poste ou d'habilitations d'un *utilisateur*, le *responsable de l'utilisateur* concerné a pour obligation d'informer le service compétent conformément à la procédure en vigueur.

Section 2.4.1 – Données sensibles

Préambule : la « sensibilité » des données doit être appréhendée sous plusieurs angles pour l'établissement :

- Sensibilité au sens de la Sécurité des Systèmes d'Information (SSI)

L'instruction interministérielle relative à la protection des systèmes d'information sensibles (http://circulaire.legifrance.gouv.fr/pdf/2015/02/cir_39217.pdf) n°901/SGDSN/ANSSI définit une information sensible comme :

- « Information dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre,
- Information manipulée dans le cadre des « télétraitements » entre administration et particuliers soumises au Règlement Général de la Sécurité (systèmes d'information mentionnés dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives),
- Information couverte par le secret professionnel, ou constituant des correspondances privées. »

- Sensibilité au sens de la protection du potentiel scientifique et technique de la nation (PPST)

La circulaire interministérielle n° 3415/SGDSN/AIST/PST du 7 novembre 2012 relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation (PPST) identifie 4 risques liés à la captation de données, notamment dans le contexte d'un établissement universitaire :

- « « intérêts économiques de la Nation » : concerne les atteintes au potentiel scientifique et technique susceptibles de nuire aux intérêts économiques de la Nation,
- « arsenal militaire » : concerne le détournement du potentiel scientifique et technique susceptible de renforcer l'arsenal militaire (conventionnel) d'un autre pays ou d'affaiblir les capacités de défense de la Nation,
- « prolifération » : concerne la prolifération des armes de destruction massive et de leurs vecteurs, dans les domaines nucléaire, balistique, chimique ou biologique,
- « terrorisme » : concerne le détournement de savoirs susceptibles d'être utilisés à des fins d'activités terroristes, menées sur le territoire national ou à l'étranger »

- Sensibilité au sens du Règlement Général sur la Protection des Données

La CNIL apporte une définition officielle d'une donnée sensible (https://www.cnil.fr/fr/definition/donnee-sensible). Il s'agit d' »informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. »

Stockage des données sensibles

L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire.

Les données sensibles ne doivent pas être stockées sur du matériel autre que celui mis à disposition de l'utilisateur par l'Université.

Un répertoire chiffré, recommandé par l'université, pourra être utilisé pour sécuriser le stockage d'informations sensibles.

Traitement des données sensibles

Le traitement d'informations sensibles au sein des zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il doit rester ponctuel et exceptionnel.

Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité (en particulier dans les transports)

Transfert de données sensibles

Les données sensibles doivent transiter de préférence sur le réseau filaire de l'université et sur RENATER.

Dans le cas où elles doivent transiter sur un autre réseau, l'accès aux données sensibles devra se faire via le VPN de l'université d'Orléans

Section 2.5 - Utilisation d'Internet

Section 2.5.1 – Accès à Internet

L'utilisation d'Internet est soumise à la législation en vigueur. Pour l'accès à Internet depuis le système d'information, les chartes des différents fournisseurs d'accès à Internet s'appliquent.

L'*utilisateur* est informé que, si une utilisation résiduelle privée peut être tolérée, les connexions Internet établies grâces aux *ressources du système d'information* mises à disposition par l'Université sont réputées avoir un caractère universitaire. L'Université, ainsi que les différents fournisseurs d'accès à Internet, peuvent rechercher les connexions à internet établies aux fins de les identifier et de les contrôler conformément aux dispositions prévues par la loi.

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 et des durées d'accès correspondantes (ex : limitation de la bande passante vers des sites de téléchargements).

La consultation de l'historique de navigation d'un utilisateur nommé n'est autorisée que sur réquisition judiciaire.

L'accès à Internet n'est autorisé qu'au travers des dispositifs 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 l'*entité*.

L'*utilisateur* est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formation ou campagnes de sensibilisation.

Section 2.5.2 – Publications sur le site Internet de l'Université

Toute publication de contenu sur le site Internet de l'Université (page personnelle enseignants, chercheurs et enseignants chercheurs) relève de la responsabilité d'un publiant nommément désigné. Les publications doivent respecter les dispositions de la charte d'hébergement de l'Université.

Section 2.5.3 – Téléchargement ou transfert de fichiers

Tout téléchargement ou transfert de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de propriété intellectuelle.

L'université se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour les *ressources du système d'information* (virus susceptibles d'altérer le bon fonctionnement du SI de l'Université, *codes ou logiciels malveillants*, programmes espions, etc.).

Section 2.6 - Communication électronique

Section 2.6.1 – Adresses électroniques

L'université met à la disposition de certains *utilisateurs* une boite à lettres universitaire nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'*utilisateur*. Cette utilisation doit se faire en conformité avec la « charte d'utilisation des courriels » de l'établissement.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement des coordonnées administratives : il ne retire en rien le caractère universitaire de la *messagerie*.

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. Les adresses nominatives ne peuvent pas être partagées entre plusieurs *utilisateurs*.

La gestion des adresses électroniques correspondant à des listes de diffusion universitaires, désignant une catégorie ou un groupe d'*utilisateurs*, relève de la responsabilité de l'Université : ces listes ne peuvent être utilisées sans autorisation explicite. Leur création à l'initiative d'un *utilisateur* doit être validée par son responsable avant leur utilisation.

L'*utilisateur* est informé que l'Université pourra prendre des mesures de type conservatoire sur les comptes de *messagerie* lorsque la situation le justifie (exemple : blocage de compte en cas de suspicion de compromission, d'usage illicite ou contraire aux dispositions de la présente charte).

Section 2.6.2 – Contenu des messages électroniques

Tout message est réputé universitaire (en lien avec les activités de l'établissement) sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un répertoire privé de données. En ce sens, il appartient à l'utilisateur de procéder au stockage de ses messages électroniques à caractère privé dans un dossier prévu explicitement à cet effet nommé « PRIVE » ou « PERSO ».

Pour préserver le bon fonctionnement des services, l'Université se réserve le droit de mettre en place des limitations, dont les termes sont précisés et portés à la connaissance de l'*utilisateur* par l'Université.

Les messages comportant des contenus à caractère illicite sont interdits, quelle qu'en soit la nature. Il s'agit notamment des contenus contraires à la liberté d'expression ou portant atteinte à la vie privée d'autrui et plus généralement aux dispositions de l'article 2.4.

La consultation par un tiers des messages électroniques (non réputés privés) d'un utilisateur nommé n'est autorisée que sur réquisition judiciaire ou à des fins professionnelles liées à la continuité du service public (les conditions de consultation sont décrites à la section 2.7). La consultation est soumise au droit au respect de la vie privée.

Section 2.6.3 – Émission et réception de messages

L'*utilisateur* doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés, eux-mêmes en petit nombre, afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la *messagerie* ainsi qu'une dégradation du service.

Section 2.6.4 – Statut et valeur juridique des messages

Les messages électroniques échangés avec les 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.

Section 2.6.5 – Stockage et archivage des messages

Chaque *utilisateur* doit mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

Section 2.7 - Continuité de service

Afin d'assurer la continuité de service, les personnels de l'université doivent privilégier le dépôt de leurs fichiers de travail sur des espaces partagés avec l'ensemble du service ou de l'équipe.

Également, dans la mesure du possible, les personnels de l'université doivent favoriser l'usage des alias de messagerie fonctionnels (Exemple : secretariat.service@univ-orleans.fr).

Lors du départ programmé d'un agent, le responsable hiérarchique prévoit le transfert des données professionnelles de l'agent partant (documents et messagerie), en concertation avec celui-ci.

En tout état de cause les données non situées dans le répertoire « PRIVE » ou « PERSO » sont considérées comme des données appartenant à l'établissement qui pourra en disposer.

En cas d'absence, il est recommandé aux personnels de l'université de mettre en place en message d'absence associé à leur messagerie. Ce message d'absence pourra préciser une autre personne à contacter durant l'absence. En cas de besoin, pour répondre à la nécessité de service, un message d'absence pourra être mis en place par le service informatique, à la demande du responsable hiérarchique du personnel, avec l'accord du RSSI.

Dans le cas où il serait nécessaire d'accéder aux données professionnelles d'un personnel de l'université en son absence et afin d'assurer la continuité de service, seul le Président de l'université peut donner son accord, dans le respect du droit à la vie privée et des dispositions de la loi Informatique et Libertés. Le Président signifiera alors son accord au RSSI et au responsable du service dont dépend la personne, en précisant les données auxquelles il est nécessaire d'accéder.

Section 2.8 - Devoir de signalement et d'information

L'*utilisateur* doit avertir son responsable ou le *RSSI* de toute anomalie ou dysfonctionnement constaté. Il signale également à son responsable toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

L'*utilisateur* doit avertir son responsable et le RSSI en cas de doute concernant la divulgation possible de données sensibles.

Section 2.9 - Exploitation et contrôle des ressources du système d'information

L'*utilisateur* est informé:

- que 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 du système d'information* ;
- que toute action de prise en main à distance (principalement sur les postes de travail) doit obligatoirement être précédée d'un accord de l'*utilisateur* ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée et le cas échéant supprimée ;
- que les *ressources du système d'information* peuvent donner lieu à une surveillance et à un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'*utilisateur*.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article 40, alinéa 2 du code de procédure pénale.

Section 2.10 – Traçabilité

L'Université est dans l'obligation légale de mettre en place un système de journalisation de certains usages des *ressources du système d'information*, tels que les accès Internet, la *messagerie* et les données échangées.

Les conditions de collecte et d'utilisation des journaux sont décrites dans le document « Politique de gestion des journaux informatiques à l'Université d'Orléans », joint à la présente charte.

Article 3 – Lois et réglementations applicables

Section 3.1 - Propriété intellectuelle

L'Université rappelle que l'utilisation des *ressources du système d'information* implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tout tiers titulaire 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.

Section 3.2 - Respect des dispositions légales sur la protection des données personnelles

L'*utilisateur* est informé de l'obligation de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément au Règlement général sur la protection des données (RGPD –

2016/679) et à la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

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.

Les traitements de données à caractère personnel consistent en toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...). Tous les traitements de données à caractère personnel sont soumis aux obligations et formalités préalables prévues par la législation sur la protection des données.

Afin d'appliquer les mesures nécessaires au respect des dispositions légales, tout utilisateur souhaitant procéder à un traitement de données devra en informer, dès la phase de conception, le délégué à la protection des données (DPD-DPO) à cette adresse : dpo@univ-orleans.fr ou bien s'adresser à la direction des affaires juridiques.

Par ailleurs, conformément aux dispositions légales, chaque personne concernée par un traitement dispose des droits d'accès, de rectification, de limitation et de portabilité relatifs à l'ensemble des données la concernant, y compris les données portant sur l'utilisation des systèmes d'information. Dans certains cas, les droits d'opposition et d'effacement peuvent également s'exercer.

L'utilisateur est tenu de respecter la mise en œuvre de ces droits conformément aux dispositions légales.

Chaque personne concernée par un traitement de ses données personnelles peut demander l'exercice de ces droits, notamment en contactant le délégué à la protection des données (DPD-DPO) à cette adresse : dpo@univ-orleans.fr.

Section 3.3 – Politique de Sécurité des Systèmes d'Information de l'Etat

L'*utilisateur* et l'Université sont tenus de respecter les dispositions légales et réglementaires suivantes:

- Circulaire PM N°5725, signée le 17 juillet 2014, portant sur la mise en œuvre de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE)

Section 3.4 - Protection du potentiel scientifique et technique de la nation

L'*utilisateur* et l'Université sont tenus de respecter les dispositions légales et réglementaires suivantes:

- Décret n° 2011-1425 du 2 novembre 2011 portant application de 1' article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.
- Circulaire interministérielle de la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation du 7 novembre 2012.

Section 3.5 - Autres lois et réglementations applicables (liste non exhaustive)

L'*utilisateur* et l'Université sont tenus de respecter les dispositions légales et réglementaires suivantes:

- Référentiel Général de Sécurité ordonnance 2005-1516 du 8 décembre 2005
- la loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication ;
- le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ;
- les articles L.323-1 et suivants du Code Pénal, relatifs aux atteintes aux systèmes de traitement automatisé de données ;
- la loi n°2004-575 du 21 juin 2004 pour la confiance en l'économie numérique ;
- la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique ;
- l'article 9 du code civil relatif au droit à la vie privée ;
- les articles R226-1 et suivants, R623-4 et R625-9 du code pénal relatifs aux atteintes à la vie privée ;
- l'article 227-23 du Code Pénal, relatif à la sanction pénale de la consultation habituelle (sur Internet), de l'enregistrement, de la diffusion et de la détention d'images pédopornographiques ;
- les articles R625-7 et suivants relatifs du Code Pénal relatifs à la sanction pénale de l'incitation à la discrimination, à la haine ou à la violence ;
- les articles R624-3 et suivants du Code Pénal relatif à la sanction pénale de la diffamation ;
- les articles 1369-1 à 1369-11 du Code Civil relatifs aux contrats sous forme électronique ;
- la circulaire n'2004-035 DU 18-2-2004 relative à l'usage de l'Internet dans le cadre pédagogique et protection des mineurs
- articles 1241 et 1242 du nouveau Code Civil relatifs à la responsabilité ;

Article 4 - Sanctions

L'*utilisateur* est passible de sanctions dans les cas suivants:

- non-respect des règles précédemment définies dans la présente charte ainsi que des modalités définies dans les guides d'utilisation établis par l'Université ;
- abus dans l'utilisation du système d'information à des fins non universitaires. Dans ces cas de figure, les sanctions applicables à l'*utilisateur* sont:
- les poursuites disciplinaires et pénales prévues par les textes législatifs et réglementaires en vigueur;
- la suspension, suppression ou limitation des accès et droits d'utilisation du système d'information.

Par ailleurs, la *personne juridiquement responsable* pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Article 5 - Entrée en vigueur

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

Le comité technique a examiné les dispositions de cette charte lors de sa séance du 14/01/2020. Sa date d'entrée en vigueur est fixée au 3/02/2020.

Politique de gestion des journaux informatiques

On entend par « établissement » « l'Université d'Orléans»
On entend par « charte informatique » la charte régissant l'usage des ressources du système d'information de l'Université d'Orléans.

Entité	Entité existante au sein de l'Université, de ses composantes, services communs et services centraux pour l'accomplissement de ses missions. Exemples : laboratoires, départements ou filières d'enseignement, services administratifs ou techniques.
Utilisateur	Toute personne / individu ayant accès ou utilisant les *ressources du système* *d'information* de l'Université d'Orléans, quel que soit son statut, en particulier : - Tout agent titulaire ou non-titulaire concourant à l'exécution des missions du service public de l'éducation ; - Tout enseignant, enseignant-chercheur ou chercheur utilisant les ressources de l'Université, y compris les locaux ; - Tout étudiant inscrit ou en cours d'inscription pour l'année en cours, ou ayant été inscrit à l'Université ; - Tout prestataire sous contrat avec l'Université ; - Tout stagiaire utilisant les ressources de l'Université, y compris les locaux ; - Tout lecteur autorisé qui dispose d'un accès aux ressources bibliographiques en ligne ; - Toute personne accédant à un service hébergé par l'Université, y compris le site internet ; - Toute personne accueillie temporairement au sein de l'Université et ayant de ce fait accès à un poste informatique de l'Université et/ou au réseau informatique (conférencier, chercheur invité, etc.).
Ressources du Système d'information	Ensemble des ressources techniques, applicatives, organisationnelles, humaines et documentaires permettant de collecter, stocker, traiter, rechercher et/ou transmettre des données, en particulier : - Tout matériel informatique fixe : postes (dont les postes libre-service), serveurs, téléphones, périphériques (clavier, écran, imprimante, etc.), prises, câbles, … - Tout matériel informatique mobile : ordinateur, téléphone, etc. - Tout logiciel ou service réseau ou informatique : accès réseau, accès Internet, *messagerie* électronique, bureautique, etc. - Tout support de données : électronique, papier, etc.
Journaux informatiques	Informations qu'une ressource du système d'information enregistre sur l'activité ou l'identité de ses utilisateurs

2. Contexte

Le fonctionnement de l'établissement passe par l'utilisation de systèmes d'information et de moyens de communications qui s'appuient sur des réseaux connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une vulnérabilité intrinsèque, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que dans certaines situations celle de l'établissement qui met ces moyens à leur disposition en tant qu'outils de travail.

L'utilisation des nouvelles technologies de communication pose le problème de la protection d'une part de l'information sensible[1] gérée par les utilisateurs et d'autre part des systèmes d'information sous la responsabilité de l'établissement. Les mesures mises en œuvre doivent permettre à l'établissement de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, des réglementations sur la protection des données sensibles et la protection du patrimoine scientifique, des lois et règlements applicables (voir charte informatique) et en particulier de la loi sur la protection des données à caractère personnel (respect des droits de l'individu) et la sécurité des systèmes d'information.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des utilisateurs. L'établissement a mis en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens informatiques, et d'autre part a fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque utilisateur.

3. Principes de base

Une maîtrise de la fiabilité et de la sécurité du fonctionnement des systèmes d'information et une garantie de la légalité des transactions opérées nécessitent un contrôle s'appuyant nécessairement sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque transaction, appelées journaux informatiques (ou logues).

3.1 - Finalités des traitements

Les traitements de ces journaux informatiques ont pour finalités :

- de contrôler le volume d'utilisation de la ressource, de mesurer le trafic et de détecter des anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins (métrologie) ;
- de vérifier que les règles en matière de sécurité des systèmes d'information (SSI) sont correctement appliquées ;
- de détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- de détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité de l'établissement ;
- de détecter les utilisations des moyens informatiques contraires à la charte informatique de l'établissement.
- d'être à même de fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition de l'autorité judiciaire présentée dans les formes légales.

[1] Informations sensibles au sens où la confidentialité (contrat, données de recherche, information nominatives, ..), l'intégrité (informations de gestion,...) et la disponibilité nécessitent une protection particulière.

Les finalités précitées imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient de remonter à l'utilisateur.

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 dite loi "Informatique et libertés". Ils doivent avoir satisfait au principe d'information préalable et de transparence ainsi qu'au régime déclaratif en vigueur auprès de la CNIL.[2]

3.2 - Durée de conservation

La durée de conservation des journaux informatiques est de 1 an maximum. L'établissement s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme.

3.3 - Qualités des données collectées

Les informations journalisées doivent être factuelles et contextuelles, c'est à dire qu'elles doivent permettre de connaître l'environnement de la collecte, le système hôte, les logiciels mis en œuvre etc. L'heure relevée est une information importante parce qu'elle est souvent le premier élément utilisé pour rapprocher des journaux de différents serveurs. Il est donc indispensable que les machines produisant des logues soient synchronisées sur un serveur de temps.

D'éventuelles interruptions de la journalisation doivent être repérables par les destinataires de ces données.

3.4 - Sécurité et intégrité des données

Les journaux contenant des données à caractère personnel doivent être identifiés dans le but de garantir leur suppression au-delà d'une année.

Dans le cas d'une exploitation des journaux informatiques anonymisés, une copie anonymisée des logs est effectuée. L'anonymisation est réalisée dans le respect des règles de l'art, elle est irréversible. On se réfèrera en particulier à l'expertise[3] publiée par la Commission Nationale Informatiques et Libertés (CNIL) dans ce domaine.

[2] Voir la fiche pratique relative au contrôle de l'utilisation des moyens informatiques dans le *Guide pratique Informatique et Libertés" pour l'enseignement supérieur et la recherche* (ce guide est disponible sur le site de la CNIL et celui de l'AMUE)

[3] http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/index.html#/40/

4. Les intervenants

Les utilisateurs

Tous les utilisateurs, tel qu'ils sont définis en introduction de ce document, sont tenus de respecter la charte informatique en vigueur dans l'établissement.

4.1- La chaîne fonctionnelle SSI

En dehors des acteurs de la chaîne fonctionnelle rappelée ci-dessous, personne n'a de droit d'accès aux journaux informatiques comportant des données à caractère personnel, y compris la chaîne hiérarchique. Ils sont tenus au devoir de réserve ou de discrétion professionnelle, voire au secret professionnel.

4.1.1 - Les administrateurs systèmes et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et veillent au respect des règles de sécurité des systèmes d'information. À ce titre, ils gèrent les traces dans le respect des obligations générales de leur fonction.

Ils rapportent au RSSI (rssi@univ-orleans.fr) toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.

Ils acceptent d'exécuter des traitements ou de fournir des informations pouvant inclure des données à caractère personnel uniquement à la demande de la chaîne fonctionnelle de sécurité.

4.1.2 - Les autres acteurs de la chaîne fonctionnelle SSI :

- les correspondants de sécurité des systèmes d'information (c'est-à-dire les correspondants informatiques)
- le responsable de la sécurité des systèmes d'information (RSSI) et son adjoint
- l'autorité qualifiée de sécurité des systèmes d'information (AQSSI),
- le fonctionnaire de sécurité de défense (FSD).

Ils sont également tenus au devoir de discrétion professionnelle, et dans certains cas de secret professionnel en fonction de leur mission.

5. Les informations enregistrées

5.1 - Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'augmentation de ses droits, tout ou partie des informations suivantes peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :

- l'identifiant de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- les commandes passées.

Le choix d'une politique de centralisation des journaux informatiques des serveurs (hors messagerie et web) et des postes de travail pourra être mis en place.

5.2 - Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs hébergeant ces services mis en œuvre au sein de l'établissement enregistrent pour chaque message émis ou reçu tout ou partie des informations suivantes :

- l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
- l'adresse des destinataires ;
- la date et l'heure de la tentative ;
- les différentes machines traversées par le message ;
- le traitement « accepté ou rejeté » du message ;

- La taille du message ;
- Certaines en-têtes du message, tel que l'identifiant numérique de message ;
- Le résultat du traitement des courriers non sollicités (spam) ;
- Le résultat du traitement antiviral ;
- Les opérations de validation ou de rejet par les modérateurs quand cela s'applique.

Les éléments de contenu des messages ne sont pas journalisés, néanmoins, les applications peuvent inclure des archives qui ne relèvent pas des journaux informatiques (chrono départ et réception).

5.3 - Serveurs Web

On distingue les serveurs web exploités au sein de l'établissement de ceux situés en dehors de l'établissement

5.3.1 - Serveurs Web de l'établissement

Pour chaque connexion les serveurs Web enregistrent tout ou partie des informations suivantes en fonction des exigences de qualité de service et de sécurité de l'application web :

- les noms ou adresses IP source et destination ;
- les différentes données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
- l'URL de la page consultée et les informations fournies par le client ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;
- les différents paramètres passés.

5.3.2 - Serveurs Web hors établissement

Lorsque les utilisateurs sont des membres de l'établissement, pour chaque accès web via le réseau interne vers des serveurs externes peuvent être enregistrées tout ou partie des informations suivantes :

- les noms ou adresses IP source et destination et les différentes données d'authentification ;
- l'URL de la page consultée ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;

L'article L.34-1 du code des postes et des communications électroniques précise que les opérateurs de communications électroniques sont tenus à une obligation de conservation des données de connexion mais que celles-ci "ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ". Cette interdiction s'applique donc en particulier à l'URL des pages consultées dans le cas où l'établissement offre des accès internet à des personnes extérieures à l'établissement. En effet, il est alors possible d'assimiler le service réseau de l'établissement à celui d'un opérateur de communications électroniques.

5.4 - La téléphonie sur le réseau internet (ou téléphonie IP)

L'usage de la téléphonie sur IP peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux, mais bien entendu, les principes relatifs à la loi « Informatique et Libertés » s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie.

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. Cependant, l'établissement peut éditer des relevés contenant l'intégralité des numéros appelés dans le cas où il demande aux personnels le remboursement du coût des communications personnelles ou dans celui où il a été constaté une utilisation manifestement anormale.

Le régime déclaratif de ces journaux fait l'objet de la norme simplifiée n° 47 relative à l'utilisation de services de téléphonie fixe ou mobile sur les lieux de travail. En outre, la fiche pratique n°11 du guide « informatique et libertés » pour l'enseignement supérieur et la recherche [4] intitulée « Utilisation du téléphone sur le lieu de travail » détaille ce cas.

5.5 - Les équipements réseau

On appelle « équipements réseau » les routeurs, pare-feu, commutateurs, bornes d'accès, équipement de métrologie et d'administration de réseau, etc. Pour chaque paquet qui traverse l'équipement tout ou partie des informations suivantes peuvent être collectées :

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure de la tentative ;
- la façon dont le paquet a été traité par l'équipement ;
- le nombre de paquets et le nombre d'octets transférés ;
- les messages d'alerte.

5.6 - Les applications spécifiques

On entend par «applications spécifiques», toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation.

Parmi ces applications nous pouvons citer les exemples suivants :

- accès aux bases de données ;
- accès à l'ENT (espace numérique de travail) ;
- service d'authentification (SSO, radius, …) ;

Comme dans le cas des serveurs web internes, des journaux génériques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- l'identité de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative ;
- les volumes de données transférées ;
- les commandes passées ;

Le traitement des journaux décrit ici ne couvre pas l'ensemble des données conservées par ces applications qui de par leur nature peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations ont un caractère personnel, elles sont alors soumises aux obligations de la loi Informatique et Libertés (déclaration auprès du DPD de l'établissement).[5]

[4] http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_AMUE_2011.pdf

[5] Le Correspondant Informatique et Libertés a été introduit en 2004 avec la réforme de la loi informatique et libertés. Sa désignation permet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à

6. Finalités des traitements effectués et leurs destinataires

Les traitements effectués doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée.

6.1 - Résultats statistiques

Ceux-ci sont effectués automatiquement et permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en tant qu'outil de travail. Lors de l'exploitation de ces résultats on s'attachera à distinguer les résultats anonymes de ceux qui peuvent être rapprochés de l'identité d'une personne. Parmi tous ces traitements on trouvera :

- des traitements statistiques en anonyme, en volume transféré et en nombre de connexions ;
- des classements des services les plus utilisés en volume de données et en nombre de connexions ;

Les résultats « anonymes » peuvent être conservés au-delà des délais mentionnés au paragraphe 3.2 et être diffusés sur des sites Internet accessibles à tous. Par contre, les administrateurs systèmes et réseau limitent l'accès aux résultats contenant des données à caractère personnel à eux-mêmes et éventuellement à la chaîne fonctionnelle SSI. La durée de conservation de ces statistiques non anonymisées ne peut excéder celle des journaux utilisés pour produire ces statistiques.

6.2 - Résultats d'analyse

Une analyse systématique des traces peut être mise en place, avec l'autorisation du RSSI, afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d'incident, des analyses peuvent être faites par les administrateurs systèmes et réseau sur les traces disponibles. Les résultats ne peuvent être transmis qu'à la chaîne fonctionnelle SSI et au CERT-Renater ou CERTA pour les incidents de sécurité.

Dans ce cas, l'accès aux journaux est limité aux exploitants des systèmes en charge d'analyser l'incident et au RSSI. L'extraction de l'information et son utilisation sont strictement limitées à l'analyse de l'incident. Si l'incident n'est pas avéré les résultats sont non transmis et immédiatement détruits.

6.3 - Détection des usages abusifs

On entend ici par « usages abusifs » les usages du réseau qui sont contraires aux lois ou à la charte informatique.

Sont aussi visés les usages qui compromettent les services du réseau de l'établissement tels que :

- consommation excessive de bande passante
- introduction de faille dans la sécurité du réseau
- fichiers volumineux
- envoi massif de messages électroniques
- Etc.

Sont aussi visés les usages qui nuisent au bon fonctionnement de l'établissement, même provenant de l'extérieurs tels que

- Appels téléphonique malveillants
- Messages électroniques malveillants
- Etc.

Les journaux peuvent être exploités pour mettre en évidence ces abus. Par exemple, des classements des machines ayant consommé le plus de réseau en volume transféré et en nombre de connexions permettent souvent de détecter l'utilisation indésirable de protocoles de peer to peer ou la présence de serveurs pirates. Se référer à la fiche pratique « Contrôle de l'utilisation des moyens informatiques » du *guide pratique « Informatique et Libertés » pour l'enseignement supérieur et la recherche*. (Ce guide est disponible sur le site de la CNIL et celui de l'AMUE)

Quand ils sont mis en œuvre, ces traitements le sont de façon systématique (ils sont appliqués à toutes les machines du réseau de l'établissement ou d'une partie donnée du réseau) et ne ciblent aucune personne ou catégorie de personnes.

6.4 - Des journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête.

Dès l'apparition d'un incident, les journaux bruts pourront être requis par la chaîne fonctionnelle SSI.

Les administrateurs systèmes et réseau sont chargés de l'application de la requête, et ils sont, pour cette activité, soumis au secret professionnel.

Les journaux bruts sont remis, à sa requête à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

6.5 - Droit d'accès individuel

Chaque agent peut demander à consulter les traces qui le concernent. Les demandes doivent être faites par écrit auprès du DPD ou du président de l'Université. Conformément à l'article 39 de la loi

« informatique et libertés » du 6 janvier 1978 modifiée et à l'article 92 décret du 20 octobre 2005 modifié en 2007, pris pour l'application de la loi précitée, les personnes souhaitant exercer leur droit d'accès doivent justifier de leur identité.

La recherche est faite par l'administrateur, sur demande de sa hiérarchie, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un «courrier personnel».

7. Informations des utilisateurs sur la politique de gestion des journaux informatiques

L'établissement doit informer ses utilisateurs de la gestion qui est faite des traces qui les concernent.

A cet effet, le présent document sera joint à la charte informatique de l'établissement. Il sera rendu accessible à tout utilisateur par le réseau et notamment :

- via le site web de l'université
- via l'intranet de l'université
- via l'ENT

8. Entrée en vigueur

Le présent document annule et remplace tous les autres documents ou chartes relatifs à la gestion des journaux informatiques.

La présente politique de gestion des journaux informatiques à l'université d'Orléans a été validée par le conseil d'administration de l'Université d'Orléans le 29/01/2016 et est applicable à compter de ce jour.