Charte du bon usage des outils numériques et emploi du système d'information UVSQ

Table des matières

I. Objet

La charte de l'Université de Versailles Saint-Quentin-en-Yvelines, ci-après dénommée UVSQ, définit les règles d'usages et de sécurité du système d'information de l'UVSQ. Elle précise les droits et devoirs de chacun.

L'UVSQ facilite l'accès des utilisateurs au système d'information et met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs. Elle tient compte notamment des recommandations de la Commission nationale de l'informatique et des libertés (CNIL) et de celles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ainsi que des dispositions de la charte du réseau RENATER.

Elle vise à informer que l'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès ; il est soumis au respect des obligations résultant de son statut ou de son contrat.

La présente charte, annexée au Règlement intérieur de l'Université, est portée à la connaissance de tout Utilisateur des systèmes d'information de l'Université de Versailles-Saint-Quentin-en-Yvelines. Elle est applicable de fait et produit, à ce titre, les mêmes effets.

Pour une meilleure compréhension de la charte, l'Utilisateur est invité à contacter le Responsable de la sécurité des systèmes d'information (RSSI) de l'Université rssi@uvsq.fr

II. Définitions

SI

On entend par Système d'Information (« SI ») l'ensemble des moyens matériels, des logiciels, des bases de données, des réseaux de communication et des données pouvant être mis à disposition des utilisateurs.

L'accès à cet ensemble à distance, par un poste fixe ou par l'informatique « nomade » (ordinateurs portables, tablettes, téléphones mobiles, ...) que ces matériels soient mis à disposition par l'université ou qu'il s'agisse de matériel personnel utilisé à des fins professionnelles, relève également de la présente charte, ainsi que toute nouvelle technologie de l'information ou de communication déployée par l'UVSQ.

Utilisateurs

On entend par Utilisateur toute personne physique ou morale qui a accès à tout ou partie des moyens informatiques et de communications électroniques de l'université, qu'il s'agisse des personnels titulaires ou non titulaires, stagiaires, étudiants, hébergés, personnels de sociétés prestataires de l'UVSQ, visiteurs occasionnels, unités et laboratoires de recherche, et toute autre structure de recherche.

Usage

La charte s'applique aux types d'usage, de moyens et de ressources informatiques et numériques sous mentionnés, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu :

- dans les locaux de l'Université, quelle que soit leur localisation ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès.

L'établissement étant raccordé au réseau national RENATER, tous les types d'usage des moyens et ressources informatiques et numériques doivent être conformes à la charte RENATER consultable sur le site de RENATER

https://www.renater.fr/documentation/chartes/

III. Principes Généraux

1. Respect des Lois et Réglementations

Tous les utilisateurs doivent se conformer aux lois et règlements en vigueur, notamment ceux relatifs à la protection des données personnelles (Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 - RGPD), aux droits d'auteur, à la propriété intellectuelle et à la cybersécurité.

S'agissant de l'application du RGPD, les utilisateurs sont informés que l'UVSQ se doit de respecter l'ensemble du corpus juridique applicable en matière de traitement automatisé de données à caractère personnel, au premier rang desquels les lois n° 7817 du 6 janvier 1978 et n° 2018-493 du 20 juin 2018 dites «Informatique et Libertés» et le règlement général (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 (RGPD).

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.

Ces données sont placées sous la responsabilité du Président de l'UVSQ, agissant en qualité de responsable de traitement, conformément au principe dit de l'accountability (article 24 du Règlement Général sur la Protection des Données).

Chaque utilisateur dispose d'un droit d'accès, de rectification et d'opposition à l'égard des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.

Ce droit s'exerce auprès du Délégué à la Protection des Données. (dpo@uvsq.fr)

Par ailleurs, tout traitement de données personnelles doit faire l'objet d'une déclaration auprès du délégué à la protection des données de l'UVSQ conformément à la procédure disponible sur l'intranet (https://www.personnels.uvsq.fr/rgpd).

2. Respect de la propriété intellectuelle

L'UVSQ rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits, notamment :

- les droits acquittés par l'Université pour permettre l'accès à des contenus numériques sous droits, couvrent l'accès à ces ressources hors l'enceinte de l'établissement pour les seuls étudiants et personnels de l'UVSQ. L'usage de ces ressources par tout autre Utilisateur est limité à la consultation sur les postes informatiques situés dans l'emprise de l'établissement ;
- il est formellement interdit de copier, même pour son usage privé, l'intégralité ou une partie substantielle des contenus numériques sous droits, mis à la disposition de ses Utilisateurs par l'UVSQ, sous réserve du droit des tiers et de l'application de la législation nationale et européenne en vigueur ;
- il est formellement interdit de diffuser à un tiers, même gratuitement, quelque contenu protégé que ce soit mis à la disposition de ses étudiants et personnels par l'UVSQ

3. Respect de la vie privée

Le droit à la vie privée, le droit à l'image, issus de l'article 9 du code civil, ainsi que le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans le consentement de la personne intéressée

4. Responsabilité

Chaque utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques mises à sa disposition. Toute utilisation abusive, frauduleuse ou contraire aux règles établies est interdite.

L'Utilisateur devra entre autres s'abstenir :

- de diffuser des messages diffamatoires ou injurieux (ces faits sont pénalement et/ou disciplinairement répréhensibles quel que soit leur mode de diffusion, public ou privé) ;
- d'utiliser certaines formes d'apologie (crime, racisme, négationnisme, crimes de guerre, ...) ;
- d'utiliser toute forme de provocation à la haine raciale ;
- de diffuser des informations confidentielles sans autorisation préalable d'une personne habilitée

5. Confidentialité

Les utilisateurs doivent préserver la confidentialité des informations auxquelles ils ont accès, notamment les données personnelles, les résultats de recherche, et les informations institutionnelles sensibles.

Les utilisateurs s'engagent à ne pas déposer des données professionnelles sur des serveurs externes et/ ouverts au grand public, sans avoir solliciter préalablement l'accord du RSSI de l'UVSQ.

IV. Usages du Systèmes d'Information

1. Usage professionnel ou étudiant

Les dispositifs de communications électroniques (utilisation des ressources informatiques, usage des services Internet, usage du réseau) sont mis à disposition des Utilisateurs pour l'exercice de leur activité professionnelle ou étudiante au sein de l'UVSQ. Cet usage ne doit pas être contraire à la loi, l'ordre public et ne doit pas mettre en cause l'intérêt et la réputation de l'établissement.

L'activité professionnelle doit être notamment entendue comme celle définie par les textes spécifiant les missions du service public de l'enseignement supérieur, à savoir :

- La formation initiale et continue ;
- La recherche scientifique et technologique, la diffusion et la valorisation de ses résultats ;
- L'orientation et l'insertion professionnelle ;
- La diffusion de la culture et l'information scientifique et technique ;
- La participation à la construction de l'Espace européen de l'enseignement supérieur et de la recherche ;
- La coopération internationale.

2. Usage à titre privé

L'utilisation à titre privé des Systèmes d'information et de communication est tolérée, mais doit être raisonnable, non lucrative, loyale et conforme aux règles et lois en vigueur. Elle ne doit pas nuire à la qualité du travail de l'Utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Les espaces de stockages intitulés « Mes documents », « perso », « personnel » ou identifiés par les initiales de l'Utilisateur sont réputés contenir des données professionnelles.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'Utilisateur comme relevant de sa vie privée. Ainsi, 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 en mentionnant le caractère privé sur la ressource. L'Utilisateur devra ainsi conserver ses informations privées dans un dossier intitulé « privé ».

Ce dossier peut éventuellement être consulté par la DSIN dans le cadre d'une remédiation à la suite d'une crise produite par une cyberattaque (cf. Politiques de Sécurité du Système d'Information).

3. Identification et Authentification

L'accès aux systèmes d'information repose sur l'utilisation d'un compte numérique et est soumis à une authentification stricte.

Chaque utilisateur se voit attribuer des identifiants personnels, confidentiels et incessibles à son arrivée, et qu'il doit protéger. Les identifiants et mots de passe personnels constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive par une tierce personne.

La « robustesse » de son mot de passe est contrainte par un outil mis à disposition par l'établissement, et reste de la responsabilité de l'Utilisateur. Le choix d'un mot de passe non trivial et son changement en cas de doute, notamment lorsqu'il a été utilisé à partir d'un poste connecté à un réseau extérieur non sécurisé, sont des mesures primordiales et fortement recommandées.

4. Droits d'Accès

Les droits d'accès sont accordés en fonction du statut de l'utilisateur (personnel, étudiant, vacataire, extérieur) et de ses besoins spécifiques. Toute demande d'accès doit être justifiée et validée par l'administration compétente.

5. Usages distants

Mobilité et accès distant

Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'Utilisateur assure la garde et la responsabilité des données et des outils du système d'information de l'établissement qu'il utilise.

Il se doit d'adopter une attitude responsable au regard des informations, données et ressources des systèmes d'information de l'établissement qu'il pourrait être amené à manipuler ou à échanger. En cas d'incident avéré ou de doute, l'Utilisateur doit immédiatement en aviser le RSSI de l'Université rssi@uvsq.fr

Télétravail

L'Université a mis en œuvre le télétravail. Une charte dédiée est accessible sur le portail : https://www.personnels.uvsq.fr/charte-sur-les-conditions-de-mise-en-oeuvre-du-teletravail-a-luvsq

V. Droit à la déconnexion

L'Université met à disposition une charte dédiée : https://www.personnels.uvsq.fr/charte-des-bonnes-pratiques-en-matiere-de-gestion-des-temps-et-du-droit-a-la-deconnexion

VI. Organisations syndicales

Les organisations syndicales représentatives ont la délégation sur la communication via les listes sympa à destination des populations de l'UVSQ.

VII. Unités mixtes de recherche

Dans le cas d'une UMR, celle-ci peut prévoir des restrictions d'accès spécifiques à son organisation.

Les Utilisateurs de ces unités sont notamment soumis au respect, quand elles existent, des Politiques de sécurité du système d'information de l'unité (PSSI) édictées par les tutelles correspondantes (Université, CNRS, INSERM, INRIA, ...).

La transmission des données classifiées de défense au sens de l'IGI1300 est interdite, sauf dispositif spécifique agréé par l'ANSSI. Par ailleurs, tout équipement traitant des données classifiées de défense doit être de même niveau que la donnée classifiée la plus haute (Secret ou Très Secret).

La transmission des données dites sensibles au sens de l'II n°901 (ie sensible pour l'organisation ou de niveau Diffusion Restreinte) doit être traitée via les moyens de chiffrement appropriés qualifiés par l'ANSSI. Des informations de niveau DR ne peuvent être traitées sur des équipements ne disposant pas de ce niveau de protection.

VIII. Utilisation des ressources informatiques

1. Configuration du poste de travail

L'UVSQ met à disposition des Utilisateurs un poste de travail doté des outils informatiques nécessaires à l'accomplissement de leurs fonctions. L'Utilisateur ne doit pas :

- modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle ;
- connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne ;
- déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade ») ;
- nuire au fonctionnement des outils informatiques et de communication.

2. Gestion des médias USB

Il est interdit de connecter à son poste de travail tout équipement non nécessaire à l'activité professionnelle.

A titre d'exemple sont interdits à la connexion sur le poste de travail les équipements suivants (liste non exhaustive) :

- Téléphone mobile personnel ou professionnel (ils sont vecteurs de nombreuses failles de sécurité). Il est toutefois autorisé de se servir des téléphones comme point d'accès internet via wifi ;
- Cigarettes électroniques ;
- Webcam personnelle ;
- …

Pour les usages des supports amovibles de stockage (clés USB ou disques durs), il est recommandé de vérifier l'innocuité de ces derniers avant de connecter ces médias sur un poste de travail professionnel.

Il est interdit de connecter un de ces supports si l'origine de ce dernier n'est pas maitrisée (ex : clé USB trouvée).

3. Messagerie électronique

a. Conditions d'utilisation

Tout Utilisateur doit utiliser l'adresse électronique professionnelle qui lui a été attribuée à sa prise de fonction.

La messagerie mise à disposition des Utilisateurs est destinée à un usage professionnel (administration, pédagogie, recherche). L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail du personnel ni la sécurité du réseau informatique de l'UVSQ. Toutefois, l'Université recommande plutôt l'utilisation d'une messagerie personnelle et de matériel personnel pour l'utilisation de la messagerie à des fins personnelles.

Tout message qui comportera la mention expresse de son caractère privé bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Pour lui conférer un caractère privé, l'objet du message doit contenir la mention « privé » ou le message doit être déposé dans un dossier intitulé « Privé ».

L'UVSQ s'interdit d'accéder aux dossiers et aux messages identifiés comme « privés » dans l'objet de la messagerie de l'agent.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies et validées par l'UVSQ :

- volumétrie de la messagerie ;
- taille maximale de l'envoi et de la réception d'un message ;
- nombre limité de destinataires simultanés lors de l'envoi d'un message ;
- respect de la confidentialité des données (aucune donnée sensible ne doit transiter via la messagerie sans les mesures de sécurité ad hoc cf. II n°901)
- gestion de l'archivage de la messagerie.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles désignant une catégorie d'utilisateurs, (listes sympas) relève de la responsabilité de l'UVSQ. Ces listes ne peuvent être utilisées pour un autre objet que celui pour lequel elles ont été mises en place. Tout besoin de listes de diffusions spécifiques peut être demandé auprès de la direction générale des services qui en appréciera l'opportunité.

b. Statut et valeur juridique des messages

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.

c. Stockage et archivage des messages

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

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte.

4. Téléphonie fixe et mobile

L'UVSQ met à disposition des Utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure marginale.

Des restrictions d'utilisation par les personnels de l'UVSQ des téléphones fixes et mobiles peuvent être mises en place en tenant compte de leurs missions.

A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

L'UVSQ s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications, sauf injonction réglementaire, atteinte à la sécurité ou sûreté. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

L'UVSQ s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, la DSIN, sur demande du Directeur Général des Services, se réserve le droit d'accéder aux numéros complets des relevés individuels.

5. Internet et Intranet

Les utilisateurs peuvent consulter les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

a. Publications sur les sites Internet et Intranet de l'UVSQ

Toute publication de pages professionnelles sur les sites Internet ou Intranet de l'Université, ou sur ses comptes institutionnels sur les réseaux sociaux, doit être validée par un responsable de site ou responsable de publication nommément désigné, sous réserve des libertés des universitaires.

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

b. Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle. L'UVSQ 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 des Systèmes d'information, code malicieux, programmes espions ...).

À l'inverse, l'utilisation du réseau pour l'offre d'un service disponible depuis l'Internet doit être rationnelle de manière à éviter toute consommation abusive ou pénalisante. L'offre de sons, d'images, de vidéos, de logiciels et tous autres documents doivent s'effectuer dans le respect des droits de la propriété intellectuelle et être en rapport avec les missions d'enseignement et de recherche de l'UVSQ.

IX. Règles de sécurité

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

En particulier, chaque utilisateur des systèmes d'information de l'UVSQ doit être répertorié dans les systèmes d'information de l'Université et avoir obtenu des codes d'accès personnels et confidentiels, comprenant un identifiant de connexion et un mot de passe associé.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité permettant de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive. Cette mesure ne confère pas pour autant un caractère personnel à ces données ou outils.

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.

Les niveaux d'accès ouverts à l'Utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des Systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre Utilisateur, ni chercher à les connaître ;
- de protéger son certificat électronique (s'il en dispose) par un mot de passe sûr gardé secret.

L'utilisateur s'engage à n'autoriser personne à faire usage d'un certificat électronique à sa place.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

(a) De la part de l'UVSQ :

- Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées ;
- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- Ne pas autoriser les redirections de messagerie pour les adresses de fonctions dans la mesure où le Système d'information est accessible (après authentification) tant du réseau de l'Université que de l'extérieur.

(b) De la part de l'Utilisateur :

Tout Utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler à la DSIN (securite@uvsq.fr) toute violation ou tentative de violation suspectée de son compte Utilisateur et de manière générale tout dysfonctionnement ;
- Ne jamais confier son identifiant/mot de passe à un tiers ;
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur ;
- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas modifier et/ou contourner les paramétrages de sécurité du poste de travail ;
- Ne pas copier, modifier, détruire les logiciels propriétés de l'UVSQ ;
- Verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- Ne pas accéder à, tenter d'accéder à, supprimer ou modifier des informations qui ne lui appartiennent pas ;
- Ne pas publier sur Internet ou Intranet des informations pouvant nuire aux personnels, aux étudiants ou à l'Université ;
- Veiller aux règlementations en vigueur visant à engager les Utilisateurs sur ce qu'ils publient avec le label de l'Université ;
- Toute copie de données appartenant à l'UVSQ sur un support externe est soumise à l'accord du supérieur hiérarchique ou fonctionnel et doit respecter les règles définies par l'UVSQ ;
- S'interdire d'accéder ou de tenter d'accéder à des ressources du Système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;

- Ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'UVSQ, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou par l'établissement. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle ou étudiante qui l'a justifiée ;
- Ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau de l'UVSQ, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
- Ne pas déposer des données sur un serveur interne ou ouvert au grand public (Free, Orange, ...) ou sur le poste de travail d'un autre Utilisateur sans y être autorisé par les responsables habilités ;
- Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques...). Tout travail de recherche ou autre, risquant de conduire à la violation de cette règle, ne pourra être accompli qu'avec l'autorisation du responsable de la sécurité du Système d'information de l'Université et dans le strict respect des règles qui auront alors été définies ;
- Se conformer aux dispositifs mis en place par l'Université pour lutter contre les virus et les attaques par programmes informatiques ;
- Assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles, y compris en utilisant différents moyens de sauvegarde individuels ou mis à sa disposition. En particulier, il ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiables tels que ordinateurs portables, clés USB, disques externes, etc. ;
- Ne pas quitter un poste informatique en libre-service en laissant des ressources ou services accessibles. Il doit notamment procéder à la fermeture de sa session en verrouillant son ordinateur ;
- L'Utilisateur assure la garde et la responsabilité des équipements fournis par l'Université. Il doit informer la direction compétente en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements ;
- Quand cela est techniquement possible, les équipements nomades doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

  Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, cet ordinateur doit être physiquement attaché à l'aide de l'antivol prévu à cet effet ou à défaut, de fermer son bureau à clef.

  L'utilisation de smartphones professionnels comporte des risques particuliers pour la confidentialité des données, notamment en cas de perte ou de vol de ces équipements.

Quand ces appareils ne sont pas utilisés pendant quelques secondes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre l'UVSQ et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

Devoirs de signalement et d'information

L'UVSQ doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du Système d'information.

L'Utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le Système d'information, etc. Il signale également au responsable de la sécurité des systèmes d'information à securite@uvsq.fr toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

X. Mesures de contrôle

La DSIN assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'UVSQ. Les personnels de cette direction disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'UVSQ se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- que pour préserver la sécurité, l'intégrité des systèmes d'information de l'université, la DSIN se réserve le droit d'isoler, bloquer, éteindre tout flux ou équipement qu'elle identifierait comme étant problématique (règlementation, sécurité, accès illicite, ...) ;
- qu'une maintenance est précédée d'une information de l'utilisateur sauf mesures urgentes.

L'UVSQ informe l'Utilisateur que les Systèmes d'information et postes de travail peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les personnels en charge des opérations de contrôle ont accès à l'ensemble des données techniques. Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Ils ne peuvent donc pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction dès lors que :

- ces informations sont couvertes par le secret des correspondances ou, qu'identifiées comme telles, elles relèvent de la vie privée de l'Utilisateur ;
- elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité ;
- elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale qui fait obligation à tout organe public de déférer des faits délictueux au procureur de la République.

1. Administration des systèmes d'information

Afin de surveiller le fonctionnement et de garantir la sécurité des Systèmes d'information de l'UVSQ, différents dispositifs sont mis en place (ex : administration à distance, centralisation des logs, ...).

Conformément au paragraphe ci-dessus, les logs des équipements (serveurs ou poste de travail notamment), ainsi que les logs applicatifs peuvent être récupérés à des fins de supervisions de sécurité (une durée de rétention sera appliquée entre 6 mois et un an en fonction des logs applicatifs concernés).

2. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'informations pour l'UVSQ et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles.

L'UVSQ se réserve le droit de filtrer ou d'interdire l'accès à certains sites internet, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'UVSQ. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par la DSIN ou l'établissement.

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

3. Les systèmes automatiques de traçabilité

La DSIN de l'UVSQ opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements des Systèmes d'information ou de l'une de ses composantes, qui mettent en péril leur fonctionnement ou leur intégrité.

Elle s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions aux Systèmes d'information. Ces fichiers peuvent comporter les données suivantes : date, identifiant de l'Utilisateur, adresse IP et objet de l'évènement.

Les personnes habilitées au sein de la DSIN seront les seuls utilisateurs autorisés à accéder à ces informations qui sont effacées périodiquement

XI. Sanctions

Toute violation de cette charte peut entraîner des sanctions disciplinaires, administratives et/ou judiciaires, en fonction de la gravité des faits constatés.

Des sanctions peuvent être prononcées selon l'échelle des sanctions réglementaires

XII. Mise à Jour de la Charte

Cette charte est susceptible d'être modifiée pour s'adapter aux évolutions technologiques et législatives. Les utilisateurs seront informés de toute modification.

XIII. Validation et Entrée en Vigueur

La présente charte a été adoptée après information et consultation du Comité Social d'Administration.

Elle entrera en vigueur un mois à compter de sa publication par l'Université et annexé au règlement intérieur.