Sorbonne Université

Charte d'utilisation des moyens et des ressources informatiques et numériques

14 juin 2018

1. Préambule

1. La présente charte[1] de Sorbonne Université a pour objet de fixer les règles d'utilisation des moyens et des ressources informatiques mises à la disposition des utilisateurs, ci-après définis à l'article 4.1, dans le cadre de leur activité professionnelle.
Elle a pour vocation d'être diffusée à l'ensemble des personnels ainsi qu'aux utilisateurs occasionnels du système d'information de l'établissement.

2. Les règles ainsi définies sont destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance d'usage des systèmes d'information et de communication, en conformité avec les dispositions légales et réglementaires applicables ainsi que la jurisprudence des Cours et Tribunaux.

3. 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).

4. La charte est rédigée dans le souci de concilier les intérêts de chaque utilisateur et ceux de l'établissement. Elle manifeste ainsi la volonté de l'établissement d'assurer un usage loyal, respectueux et responsable de ses systèmes d'information et de communication, ainsi que de protéger son patrimoine et son image de marque.

5. La charte est annexée au règlement intérieur de l'établissement. Elle pourra évoluer en fonction du contexte légal et de la politique de sécurité notamment applicable au sein de l'établissement.

6. Pour une meilleure compréhension de la charte, l'utilisateur est invité à prendre contact avec le Responsable de la sécurité des systèmes d'information (RSSI) de l'établissement (rssi@sorbonne-universite.fr).

2. Définitions

7. Au sens de la charte, les termes ci-dessous ont la signification suivante :

- « application » : logiciel de traitement automatisé de données numériques, accessible à partir du réseau interne de l'université ou par internet ;

- « backup » : solution de secours informatique présentant une configuration compatible avec celle de l'établissement, pouvant être hébergée par l'université ou par un site extérieur ;

- « charte » : le présent document et ses annexes constituant la charte des systèmes d'information et de communication de l'établissement ;

[1] Le présent document se présente sous la forme d'une charte car il lie un ensemble d'acteurs sans mécanisme de signature. La charte pose des règles impératives, à respecter dans le cadre de l'activité professionnelle en l'occurrence, et dont les manquements sont sanctionnés sur le terrain de la responsabilité disciplinaire, civile et pénale. Il ne s'agit pas, en conséquence, de principes généraux, ou d'ordre déontologique ou éthique.

- « code malveillant » : logiciel développé dans le but de nuire à un système informatique ou d'exfiltrer des données des utilisateurs (virus, vers, chevaux de Troie, keyloggers, etc.) ;

- « consommable » : produit ou constituant qui disparait par l'usage des systèmes d'information et de communication (consommables d'impression, d'encre, fournitures de bureau diverses, etc.) ;

- « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ;

- « filtrage » : ensemble d'outils informatiques visant à limiter l'accès à certains sites Internet en raison de leurs contenus (contrôle des contenus, des URL, protocolaire, etc.) ;

- « matériel nomade » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de l'établissement ;

- « moyen d'authentification » : moyen permettant l'accès aux systèmes d'information et de communication et pouvant prendre diverses formes : login/mot de passe, biométrie, signature électronique, cartes avec ou sans contact, etc. ;

- « scan » : contrôle à travers des outils informatiques de la présence de mots clés dans des contenus (dossiers, documents, courriers électroniques, pièces-jointes, fichiers, etc.) ;

- « service en ligne » : service de communication par voie électronique de mise à disposition du public ou de catégories de public, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée[2] ;

- « signe distinctif » : signe permettant l'identification d'une entreprise, d'un produit ou d'un service : marques, dessins et modèles, enseignes, nom commercial, dénomination sociale, nom de domaine, et faisant généralement l'objet d'une protection par le droit de la propriété intellectuelle ;

- «systèmes d'information et de communication » : ressources et moyens informatiques et moyen de communication électronique, recouvrant tout matériel informatique, câblage, périphériques (tels que imprimantes simples ou multifonctions, webcam, etc.), disquette, disque dur externe ou interne, carte mémoire, CD-Rom, clé USB, ordinateur, tablette, PDA, photocopieurs, routeur, scanner, radiographie, etc… et toute ressource informatique de toute nature (logiciels, applications, bases de données, etc., et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau, ainsi les moyens de communication électronique recouvrant internet et les télécommunications (tels

[2] Loi n°2004-575 art. 1 I du 21-6-2004 pour la confiance en l'économie numérique.

que téléphone, équipement sans fil, carte de communication sans fil, terminaux portables, le matériel nomade, messagerie, forum, sites web, etc.) ;

- « trace informatique » : donnée informatique témoignant de l'existence d'une opération au sein d'une application ou du système d'information ;

- « webmail » : service de messagerie accessible par l'intermédiaire d'un navigateur internet, qui permet donc l'émission, la consultation et la manipulation de courriers électroniques ;

3. Portée et opposabilité

8. La charte étant annexée au règlement intérieur, elle est applicable de fait et produit, à ce titre, les mêmes effets.

9. En conséquence, l'utilisateur est supposé en avoir pris connaissance.

10. L'utilisation des moyens et ressources informatiques et numériques par les instances représentatives du personnel ou pour l'exercice d'un mandat syndical pourra faire l'objet d'un accord distinct de la charte.

4. Champ d'application

4.1 Personnes concernées

11. La charte est applicable, et donc opposable, à toute personne faisant partie du personnel autorisée à accéder aux systèmes d'information et de communication, ce, quel que soit son statut : agent de la fonction publique titulaire ou non titulaire, contractuel, stagiaire, apprenti, vacataire, doctorant, hébergé, invité, personnel externe (incubateur, collaborateur scientifique etc.) concourant à l'exécution des missions du service public de la recherche et de l'éducation).

12. La charte est complétée d'un document spécifique, dit « charte de l'administrateur » s'appliquant aux personnels disposant d'un accès administrateur sur un ou plusieurs composants informatiques connectés aux systèmes d'information de l'établissement.

13. Sont visés par la charte :

- l'ensemble des systèmes d'information et de communication qui sont la propriété de l'établissement et/ou qui sont mis à la disposition des utilisateurs à des fins professionnelles et/ou tout autre nouveau système qui serait mis en place ;

- l'ensemble des systèmes d'information et de communication qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu, auprès d'une personne habilitée (chef de service ou directeur d'unité), une autorisation d'utilisation dans le cadre de son activité professionnelle.[3] La charte de l'administrateur est, dans ce cas, applicable à l'utilisateur.

[3] A défaut d'un document signé, une autorisation peut être obtenue par courriel.

4.2 Usages concernés

14. La charte s'applique à tous les types d'usage de moyens et de ressources informatiques et numériques, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu :

- dans les locaux de l'établissement[4] , quelle que soit leur localisation ;
- dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.).

L'établissement étant raccordé au réseau internet opéré par le GIP 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).

5. Conditions d'utilisation générales

5.1 Usage professionnel

5.1.1 Systèmes d'information et de communication de l'établissement

15. Les systèmes d'information et de communication quelle que soit leur nature, sont réservés à un usage professionnel et sont donc présumés avoir un caractère professionnel, et ce, quelles que soient les conditions effectives d'utilisation.

16. Selon la jurisprudence, sont présumés avoir un caractère professionnel, notamment[5] :

- les fichiers créés par un utilisateur grâce aux systèmes d'information et de communication de l'établissement ou de ses moyens ou ressources, pour l'exécution de son travail, sauf lorsque celui-ci les identifie comme étant « privés » ;
- les connexions établies par un utilisateur sur des sites internet pendant son temps de travail grâce aux systèmes d'information et de communication de l'établissement, pour l'exécution de son travail ;
- les clés USB dès lors qu'elles sont connectées à un outil informatique mis à la disposition de l'utilisateur par l'employeur dans le cadre de son contrat de travail.

17. Il en résulte que :

[4] Les locaux de l'établissement visent son siège social ainsi que ses établissements secondaires. Il est rappelé que la présente charte, au même titre que le règlement intérieur, devra notamment être affichée au sein de ces établissements.

[5] Cass. soc. 18-10-2006 M. X… c/ société Jalma emploi et protection sociale (JEPS) ; Cass. soc. 18-10-2006 M. X. c/ société Techni-Soft ; Cass. soc. 9-7-2008 pourvoi n° 06-45800 ; Cass. soc. 12-2-2013 Mme X. c/ société PBS n°11-28649.

- l'établissement peut y accéder hors de la présence de l'utilisateur, pour des raisons de continuité d'activité ou par mesure de sécurité ;

- aucune information à caractère professionnel ne peut être ni stockée dans un répertoire informatique utilisé à des fins non professionnelles, ni émise ou reçue via le courrier électronique non professionnel.

18. **Messagerie électronique.** En particulier, l'adresse électronique, composée de « prénom.nom@sorbonne-universite.fr », est professionnelle. Elle ne doit donc pas être utilisée dans un autre contexte, et notamment diffusée sur des services en ligne, sans rapport avec l'activité professionnelle[6].

19. Les listes de diffusion permettant la réception automatique et périodique d'informations doivent être réservées à un usage professionnel.

20. L'inscription sur une liste de diffusion requiert une autodiscipline des utilisateurs : chacun doit s'assurer au préalable et, de manière continue, de la pertinence et de la nécessité de celle-ci ainsi que de ses conséquences (fréquence de réception des messages, poids des messages, encombrement des réseaux, etc.).

21. **Services en ligne et applications.** L'accès à des services en ligne et applications est également réservé à un usage professionnel.

5.1.2 Moyens personnels de l'utilisateur

22. L'utilisateur ne peut utiliser à des fins professionnelles des systèmes d'information et de communication qui sont sa propriété personnelle ou qu'il détient à titre personnel, sans obtenir une autorisation préalable auprès de son directeur de service ou directeur d'unité, pour toute connexion aux réseaux filaires de l'établissement.

5.2 Usage non professionnel

23. Bien que les systèmes d'information et de communication de l'établissement soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles est tolérée.

24. Cette tolérance pourra être suspendue ou limitée en cas d'abus.

25. Un tel usage non professionnel ne doit pas :

- perturber le bon fonctionnement des systèmes d'information et de communication, du service et de l'établissement en général ;

- compromettre ses activités et particulièrement ses missions d'intérêt général et la continuité du service ;

[6] CE 15-10-2003 M. Jean-Philippe O.

- porter atteinte aux obligations qui incombent aux utilisateurs compte tenu de leur statut et notamment, les obligations de dignité, de loyauté, de discrétion, de neutralité ou de réserve ;

- porter atteinte ou être susceptible d'engager la responsabilité de l'établissement ;

- poursuivre un but lucratif;

- porter atteinte à l'image de marque ou à la réputation de l'établissement.

26. L'usage non professionnel des systèmes d'information et de communication se traduit dans les faits par :

- la possibilité de créer un répertoire informatique non professionnel ;

- la possibilité d'utiliser à des fins non professionnelles la messagerie électronique professionnelle (pour rappel « prénom.nom@sorbonne-universite.fr »).

27. Afin de garantir la confidentialité des répertoires et messages électroniques non professionnels, il est impératif que l'utilisateur utilise le terme « PRIVE »:

- sur le répertoire informatique ;
- dans la zone objet du message électronique et le tiers destinataire du message devra être informé de cet usage ;
- si le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, sms…), le message à caractère non professionnel doit débuter par le terme « PRIVE ».

28. A défaut d'utiliser le terme « PRIVE », tous les répertoires informatiques et tous les messages informatiques sont considérés comme professionnels.

29. L'utilisateur est entièrement responsable de l'usage des systèmes d'information et de communication de l'établissement à des fins privées et dégage en conséquence l'établissement de toute responsabilité.

30. Le caractère non professionnel de l'usage des systèmes d'information et de communication interdit, par principe, à l'établissement, d'accéder aux contenus ou données émis, reçus ou échangés dans ce cadre.

31. Le caractère non professionnel du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que :

- l'établissement puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'établissement en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée[7] ;
- ces éléments fassent l'objet de conservation technique dans le cadre de la mise en œuvre des sauvegardes planifiées par l'entité ou le service ;

En cas de détection ou de suspicion de la présence d'un code malveillant, il soit procédé :

[7] Cass. soc. 17-5-2005 pourvoi n°03-40.017.

- à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;

- à ce qu'un administrateur, ou toute personne « habilitée », accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information et de communication, ce, notamment, dans le cadre d'opérations de maintenance[8] ;

- à ce que l'établissement puisse, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisé par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.).

32. Il est rappelé, que ce soit à titre professionnel ou non professionnel, qu'il est interdit de se connecter sur des sites à caractère pornographique, pédopornographique, zoophile, injurieux, violent, raciste, antisémite ou nazi, d'incitation à la haine ou à la violence ou à la commission d'acte illicite, discriminatoire, diffamatoire, faisant l'apologie du terrorisme, contrefaisant, ou manifestement contraire à l'ordre public ou de télécharger ou visionner ou stocker ou transmettre, etc. des contenus de telle nature.

5.3 Conditions d'accès et d'identification

33. Chaque utilisateur est doté d'un ou de plusieurs moyens d'authentification permettant l'accès aux moyens et ressources informatiques et numériques.

34. Les moyens d'authentification sont confidentiels.

35. Il est, dès lors, interdit à l'utilisateur :

- de procéder à la moindre divulgation à un tiers ou à un autre utilisateur, même intra-service, de son ou de ses moyens d'authentification ;

- d'utiliser un moyen d'authentification autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;

- de supprimer, masquer ou modifier son identité ou son identifiant ;

- d'user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès ;

[8] Fiche n°7 du guide pour les employeurs et les salariés, 2010, de la Cnil : « Les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ils sont conduits par leurs fonctions mêmes à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique des sites visités, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…). »

- lorsqu'un accès distant lui est accordé, d'utiliser d'autres moyens d'authentification que ceux qui lui sont remis à cet effet.

36. Les mots de passe doivent être robustes et modifiés régulièrement conformément à la politique de gestion des mots de passe prévue par la PSSI de l'établissement.

37. En termes de sécurité et de confidentialité, l'utilisateur devra suivre toutes les prescriptions complémentaires qui lui seront signifiées par le Chargé de sécurité des systèmes d'information (CSSI,) ou à défaut par le RSSI.

5.3.1 Perte, vol ou compromission

38. Si ses moyens d'authentification ont fait l'objet d'une communication ou qu'il existe un risque qu'ils aient été communiqués, l'utilisateur doit renouveler ses moyens d'authentification, contacter la hotline de la DSI (https://hotline.sorbonne-univserite.fr) et avertir le CSSI de son unité ou à défaut le RSSI de l'établissement.

39. L'utilisateur devra aviser, sans délai, le CSSI de son unité ou à défaut le RSSI, de la perte ou du vol d'un équipement informatique dont il a l'usage, afin qu'une étude d'impacts soit menée. Il devra également, selon les cas, soit assister l'établissement, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

40. En cas de perte, de vol, ou de suspicion de compromission de ses moyens d'authentification, l'utilisateur est tenu d'en aviser sans délai le CSSI, ou à défaut le RSSI, en suivant, le cas échéant la procédure formalisée permettant d'invalider et/ou de renouveler ses moyens d'authentification. Cet acte d'information est de nature à dégager la responsabilité de l'utilisateur pour les agissements qui auraient lieu post-déclaration.[9]

41. En cas d'incident, l'établissement se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer le droit d'accès de toute personne aux systèmes d'information et de communication. Il s'efforcera, autant que faire se peut, de prévenir l'utilisateur concerné dans des délais raisonnables, notamment en cas de maintenance.

5.4 Gestion des absences et des départs

42. En cas d'absence ou de départ de l'utilisateur, l'établissement se réserve le droit de mettre en place une solution de re-routage des messages électroniques ou toute autre solution technologique permettant d'assurer la continuité de l'activité du service.

43. En cas d'absence de l'utilisateur, pour quelque raison et durée que ce soit, l'établissement se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tout document à caractère professionnel de l'utilisateur, ayant recours en tant que de besoin, aux codes administrateurs systèmes.

[9] La procédure de désactivation des identifiants, à la suite d'une suspension ou d'une suppression de l'accès aux moyens informatiques et de communication électronique, devra être prévue dans un livret technique.

44. Lors de son départ, l'utilisateur doit :

- supprimer, au plus tard, la veille de son départ le répertoire et les messages électroniques nommés « PRIVE », ainsi que tous les documents de même nature. A défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés sans être consultés et sans qu'aucune copie ne soit réalisée.

45. Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois (3) mois, le compte messagerie de l'utilisateur, ainsi que ses moyens d'authentification, sont désactivés au plus tôt.

6. Conditions d'utilisation spécifiques

6.1 Mobilité et accès distant

46. Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des systèmes d'information et de communication.

47. Ainsi, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations, données et ressources du système 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'établissement ou le CSSI de son unité.

6.2 Télétravail

48. L'établissement se réserve la possibilité de mettre en œuvre du télétravail selon la législation en vigueur.

49. Le cas échéant, l'utilisation autorisée au télétravail devra suivre les dispositions de la charte ainsi que l'ensemble des procédures et instructions données par l'établissement pour l'utilisation des systèmes d'information et de communication.

6.3 Gestion des connaissances et de l'espace collaboratif

50. Chaque utilisateur s'engage à être attentif à la pertinence des informations diffusées au sein des espaces collaboratifs et à travers les outils de gestion des connaissances mis à sa disposition par l'établissement. Il veille, notamment, à s'informer des règles de diffusion d'un document, notamment lorsqu'il s'agit d'informations nominatives ou à caractère personnel.

51. Par souci de qualité, de responsabilité et de protection du patrimoine informationnel de l'établissement, l'utilisation de ces mêmes espaces et outils peut faire objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

6.4 Médias sociaux

52. Les réseaux sociaux permettent aux utilisateurs de créer de nouvelles relations professionnelles et d'optimiser les échanges professionnels autour de leurs projets. Cependant, leur utilisation peut être source de risques et de responsabilité notamment en termes d'image, ou de fraude. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

6.4.1 Usage professionnel

53. Dans le cadre de la sphère professionnelle, l'utilisateur doit obtenir au préalable l'autorisation de son supérieur hiérarchique pour pouvoir participer à un réseau social et/ou créer un espace sur un réseau social au nom de sa structure.

54. Si l'autorisation a été donnée, l'utilisateur doit se conformer aux règles et instructions édictées par son supérieur hiérarchique, ce dernier étant seul compétent pour déterminer les conditions d'utilisation du réseau social.

55. De plus, lorsqu'un réseau social est utilisé l'utilisateur devra :

- s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de l'établissement ;

- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de l'établissement ;

- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle, de droit de la presse, de propos illicites) ;

- utiliser uniquement les outils de communication de l'établissement, selon les instructions qui lui ont été données;

- s'abstenir de diffuser toute information confidentielle ou toute information commerciale sensible relative à l'établissement ou à ses partenaires ;

- prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les systèmes d'information et de communication de l'établissement.

56. En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra immédiatement consulter son supérieur hiérarchique.

57. L'autorisation donnée pourra être retirée, modifiée ou suspendue par le supérieur hiérarchique dès lors que l'intérêt de l'établissement le justifie.

6.4.2 Usage non professionnel

58. Dans le cadre de la sphère non professionnelle et hors les murs de l'établissement, l'utilisateur est bien évidemment libre d'utiliser les réseaux sociaux. Cependant, il

s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations confidentielles et des informations sensibles relatives à l'établissement ou à ses partenaires.

7. Protection de la propriété intellectuelle, des informations et des données

7.1 Propriété intellectuelle et droit à l'image

59. L'utilisation des systèmes d'information et de communication de l'établissement implique le respect des droits de propriété intellectuelle et du droit à l'image.

60. Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- utiliser les logiciels et applications, dans les conditions de la licence souscrite par l'établissement ;

- ne pas effectuer de copie illicite de logiciel ou d'applications et, a fortiori, de tenter d'installer des logiciels ou applications pour lesquels l'établissement ne possèderait pas un droit d'usage ;

- ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'établissement ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;

- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles, sans autorisation ou licence ;

- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des utilisateurs ou de tiers à l'établissement.

7.2 Préservation du secret et de la confidentialité[10]

7.2.1 Règles générales

61. La sauvegarde des intérêts de l'établissement nécessite le respect par l'utilisateur d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et des données dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

[10] Les informations secrètes sont protégées aux termes de la loi (ex. : secret défense) et les informations confidentielles sont protégées en application d'une convention. Le caractère confidentiel de ces informations résulte donc de la volonté des parties.

62. Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;
- n'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres utilisateurs ;
- ne pas extraire ces informations et données confidentielles et ne pas les reproduire sans l'accord préalable du supérieur hiérarchique et/ou les détourner de leur utilisation normale à des fins non professionnelles ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein de l'établissement.

63. La diffusion de toute information ou donnée confidentielle ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

7.2.2 Chiffrement

64. Il est interdit aux utilisateurs de chiffrer les répertoires, dossiers ou boites ou libellés à caractère privé ou non professionnel.

65. L'utilisation de procédés de chiffrement est soumise au séquestre des clefs privées qui sont conservées par le directeur du service ou le RSSI de l'établissement par délégation, et par le directeur d'unité ou son CSSI par délégation.

7.3 Protection des données à caractère personnel

7.3.1 Devoirs des utilisateurs

66. Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018.

67. Dans ce cadre, les utilisateurs devront informer le Délégué à la protection des données (dpd@sorbonne-universite.fr) et se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.

68. Conformément à la législation applicable à la protection des données personnelles, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un traitement de données personnelles sont les suivants :

- le respect des finalités initiales du traitement ;
- la pertinence et l'exactitude des données au regard des finalités poursuivies ;
- l'information des personnes à la collecte des données et la conservation du recueil de leur consentement en cas de signature électronique ou manuscrite;
- le droit d'accès, de rectification ;
- le droit d'opposition ;
- la mise en œuvre de mesures de sécurité adaptée à la sensibilité des données traitées, résultant d'une étude d'impact pour les personnes privées en cas de divulgation, altération ou destruction des données les concernant.
- le contrôle rigoureux de la diffusion de données à caractère personnel à l'attention de tiers extérieurs, en incluant notamment les clauses adaptées dans les contrats avec les sous-traitants.
- La destruction des données au-delà de la période de conservation prévue.

7.3.2 Droits des utilisateurs

69. L'établissement (Sorbonne Université) met en œuvre des traitements de données à caractère personnel en relation avec l'usage et la sécurité des systèmes d'information et de communication couverts par la présente charte. L'établissement (Sorbonne Université) s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

L'établissement Sorbonne Université a désigné un Délégué à la protection des données joignable à l'adresse dpd@sorbonne-universite.fr.

70. Les catégories suivantes de données sont traitées :

- Informations professionnelles
- Informations relatives à l'identité
- Coordonnées professionnelles
- Log de connexion et autre trace informatique
- Informations sur l'utilisation des systèmes d'information et de communication ;

71. Ces catégories de données proviennent essentiellement des systèmes d'information et de communication ainsi que des annuaires informatiques et des directions des ressources humaines.

72. Ces données sont conservées selon les durées légales.

73. Ces données sont destinées à l'établissement (Sorbonne Université) ainsi qu'aux personnes habilitées au sein de l'établissement (Sorbonne Université) et aux autorités habilitées.

74. Les traitements opérés dans le cadre de la charte ont pour finalité :

- le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;

- la gestion des annuaires et référentiels permettant de définir les autorisations d'accès aux applications et réseaux ;

- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des systèmes d'information et de communication, notamment la conservation des logs de connexion, des traces informatiques et des données de toute nature, conformément à la Politique de gestion des journaux informatisés (PGJI) notamment à des fins d'historisation et de preuve de l'utilisation des systèmes d'information et de communication ;

- la gestion de la messagerie électronique ;

- le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;

- le contrôle du respect de la charte et les audits de sécurité ;

- les statistiques, investigations et enquêtes,

75. Ces finalités permettent à l'établissement (Sorbonne Université) de poursuivre des intérêts légitimes liés à la bonne utilisation et à la sécurité de ses systèmes d'information et de communication dans le respect des droits des utilisateurs.

76. A toutes fins utiles, il est rappelé que les données collectées auprès des utilisateurs sont obligatoires aux fins de bonne gestion, d'organisation et de sécurité des systèmes d'information et de communication.

77. Conformément à la loi « Informatique et libertés », les utilisateurs sont informés, en particulier, qu'ils disposent d'un droit d'interrogation, d'accès, de limitation, d'effacement, de rectification et d'opposition au traitement des données les concernant et qui s'exerce auprès du Délégué à la protection des données (dpd@sorbonne-universite.fr). Par ailleurs, les utilisateurs disposent d'un droit de réclamation auprès de la Cnil.

78. Les personnes concernées peuvent également donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès. Une personne peut être désignée pour exécuter ces directives et elle aura alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. Lorsqu'il s'agit de

directives particulières, elles peuvent également être confiées aux responsables de traitement en cas de décès.

7.4 Enregistrements

7.4.1 Vidéo-protection

79. Les utilisateurs sont informés de la mise en place d'un dispositif de vidéosurveillance dans les locaux de l'établissement à des fins de sécurité et de prévention des atteintes aux biens et/ou aux personnes.

80. L'enlèvement ou la neutralisation de tout ou partie de ce dispositif de vidéosurveillance sans justificatif sont strictement interdits.

7.4.2 Enregistrements audio/visuels

81. Dans le cadre professionnel et dans l'objectif d'atteindre une certaine qualité de service, des outils techniques d'enregistrements vidéo et sonores sont mis en place.

82. Peuvent être soumis à des enregistrements notamment les cours, les web-conférences, les visio-conférences, les conférences téléphoniques.

83. Les utilisateurs sont informés de l'existence de ces outils d'enregistrement et du fait qu'ils sont activés par défaut dans certains lieux, notamment les amphithéâtres, sans qu'il soit besoin de le rappeler systématiquement à l'utilisateur.

8. Sécurité et vigilance

8.1 Sécurité

84. A des fins de précaution, certaines configurations peuvent être verrouillées par l'établissement (poste de travail, accès internet, etc.).

85. Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des systèmes d'information et de communication mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information de l'établissement.

86. L'utilisateur doit se conformer notamment, mais non limitativement, aux règles de conduite suivante :

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;

- ne pas modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;

- ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes d'information et de communication ou aux réseaux à travers les matériels dont il a usage ;

- ne pas utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;

- ne pas effectuer des opérations pouvant nuire aux relations internes ou externes de l'établissement.

A revoir

87. En cas de réception de messages non sollicités (spams), et notamment en cas de tentative de phishing visant à obtenir ses identifiants, l'utilisateur veille à :

- ne pas l'ouvrir sans s'être assuré préalablement de son innocuité ;
- ne pas y répondre ;
- ne pas le transférer ;
- informer la hotline de la DSI ;
- agir sur instruction du service informatique de l'établissement ou de la faculté, du CSSI de l'unité, ou du RSSI.

88. L'utilisateur s'efforcera de signaler, sans délai, tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les systèmes d'information et de communication.

8.2 Traçabilité

89. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des systèmes d'information et de communication mis à la disposition des utilisateurs, l'établissement se réserve le droit de mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des systèmes d'information et de communication.

90. Les traces informatiques sont conservées pour une durée limitée de un an.

91. Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

8.3 Filtrage

92. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ses systèmes d'information et de communication l'établissement se réserve le droit de mettre en place des outils de filtrage permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet ou d'applications.

93. Ces outils, en ce qu'ils portent entre autres sur l'accès à internet, permettent un contrôle des connexions des utilisateurs.

94. Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

8.4 Scan informatique

95. L'établissement se réserve le droit de mettre en œuvre des opérations de scan des systèmes d'information et de communication tels que le scan des éléments professionnels de l'utilisateur, et notamment des documents, des dossiers, des courriers électroniques, pièces jointes, fichiers[11].

96. Les outils de scan informatique n'ont pas pour objet l'ouverture des éléments identifiés. Ils permettent à l'établissement de disposer d'un dispositif d'alerte prudentiel et rapide de ses systèmes d'information et de communication.

97. Les documents, dossiers, courriers électroniques, pièces jointes, etc. identifiés comme « PRIVE » ne seront pas consultés par l'établissement, sauf dans le cadre des dispositions légales particulières de la jurisprudence en la matière et de la charte.

8.5 Mesures d'urgence et plan de continuité d'activité

98. L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, l'établissement peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

[11] L'employeur peut installer un dispositif de contrôle de la messagerie des employés à condition de :

- consulter le comité technique en l'informant de l'installation et de la finalité du dispositif, ainsi que des modalités d'archivage des messages électroniques ;
- informer l'utilisateur ;
- le dispositif doit être déclaré auprès de la Cnil ;
- ne pas scanner les messages électroniques identifiés comme privés dans l'objet ou dans un fichier réservé sur la messagerie électronique. Les messages non identifiées comme privés sont considérés comme professionnels. L'ouverture d'un message électronique privé hors des conditions prévues par la loi est constitutive du délit de violation des correspondances électroniques punie par l'article 432-9 du Code pénal de trois ans d'emprisonnement et de 45.000 euros d'amende. Un licenciement décidé sur la base des méls privés de l'utilisateur pourrait être considéré comme sans cause réelle et sérieuse. La copie des méls professionnels de l'utilisateur constitue une preuve loyale, licite et proportionnelle. Pour éviter les contestations, il convient d'effectuer les opérations de contrôle sur le poste informatique de l'utilisateur en présence de :
  - une personne disposant de la compétence technique nécessaire (exemple : administrateur réseau) ;
  - un huissier de justice attestant du déroulement des opérations et de la preuve du respect de la procédure de contrôle. Pour le contrôle de messages électroniques identifiés comme privés, il est convient d'obtenir une décision de justice autorisant le contrôle et désignant un huissier de justice. Il est convient de prévoir, également, la désignation d'un spécialiste informatique par le juge.

De manière générale, le contrôle doit obéir à une procédure stricte.

99. Dans cette hypothèse, l'utilisateur pourra être amené, à la demande de l'établissement, à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

100. Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

9. Contrôle, maintenance et gestion des ressources

9.1 Contrôle et audit

101. Les opérations de contrôle et d'audit portent sur la régularité de l'utilisation des systèmes d'information et de communication. Elles se justifient par les obligations incombant à l'établissement.

102. En effet, de par son activité, l'établissement est soumis à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et de la loi dite « Informatique et Libertés ».

103. L'établissement, en tant qu'employeur, dispose également d'un pouvoir de contrôler l'activité des utilisateurs et en particulier, le respect par eux de la charte.

104. L'utilisation des moyens et ressources informatiques et numériques pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

105. L'établissement se réserve ainsi le droit, notamment :

- de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
- de contrôler l'origine licite des logiciels installés ;
- de conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

106. En outre, en cas d'incident, l'établissement se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;

- vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;

- procéder à toutes copies utiles pour faire valoir ses droits.

107. Tout intervenant en charge de contrôles ou d'audit doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des utilisateurs. Quand il s'agit d'un prestataire externe, la signature d'une clause de confidentialité est demandée.

108. Les utilisateurs sont toutefois informés que les administrateurs systèmes et réseaux sont conduits, de par leurs fonctions et selon des procédures déterminées, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

109. Néanmoins, ces administrateurs systèmes et réseaux sont tenus au secret professionnel et ne peuvent utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

110. En cas de non-respect avéré de la charte par un utilisateur, et suivant la gravité des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus par la Direction des Systèmes d'Information.

9.2 Maintenance

111. La mise à disposition de moyens et ressources informatiques et numériques implique nécessairement des opérations de maintenance technique (maintenance corrective, maintenance préventive ou évolutive), et ce, pour assurer le bon fonctionnement et la sécurité de ceux-ci.

112. Ces opérations prennent la forme d'une intervention d'une « personne habilitée» soit sur site, soit à distance, conduisant alors cette personne à effectuer une « prise en main à distance » selon un calendrier préétabli ou en cas d'incident.

113. En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'utilisateur de communiquer ses moyens d'authentification.

114. Dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présent sur le poste ou le matériel nomade de l'utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

115. Si, à l'occasion d'opérations de maintenance, une utilisation anormale et/ou un contenu illicite ou préjudiciable sont identifiées, l'établissement en tirera toute conséquence.

9.3 Consommations

116. Pour la bonne gestion des ressources liées aux systèmes d'information et de communication :

- pour la téléphonie fixe, les éléments de la communication (date, heure, durée, coût et numéros appelés) le contrôle des consommations peut être effectué sur la base des factures détaillées sans divulgation des 4 derniers digits des numéros appelés ;

- pour les systèmes d'information et de communication nomades, les éléments de la communication (date, heure, durée, coût et numéros appelés) sont disponibles via les opérateurs téléphoniques mobiles, à travers les services de suivi des consommations qu'ils proposent.

117. L'enregistrement des conversations téléphoniques est strictement interdit, sauf à en informer préalablement l'interlocuteur conformément à l'article « enregistrements ».

9.3.1 Règles de conservation, de sauvegarde et d'archivage électronique

118. Chaque utilisateur doit mettre en œuvre et organiser, selon les instructions de sa hiérarchie, les moyens nécessaires à la conservation des messages, des informations et des données de toute nature lorsque cela est nécessaire.

119. L'utilisateur est dans l'obligation de respecter les règles ou la politique de conservation et d'archivage de l'établissement.

120. Les traces détaillées d'activité sont conservées pendant les durées légales ou conventionnelles, à l'issue desquelles elles sont détruites.

121. Ces traces valent preuve de l'utilisation des systèmes d'information et de communication.

122. Ces traces peuvent faire l'objet d'un traitement statistique.

123. Ces traces peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

124. Les sauvegardes, back up et archivages électroniques concernant les éléments du répertoire et les messages nommés « PRIVE », sont conservés sous la seule et entière responsabilité de l'utilisateur.

10. Responsabilité et sanctions

125. L'utilisateur est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des moyens et ressources informatiques et numériques en conformité avec la présente charte ;

- dans la sphère de sa vie privée résiduelle, seul, à l'exclusion donc de toute responsabilité de l'établissement, de tout usage des moyens et ressources informatiques et numériques à caractère non professionnel.

126. Le non-respect des dispositions légales et règlementaires, ainsi que de la charte, expose l'utilisateur en cause à des sanctions disciplinaires, prévues notamment dans le règlement intérieur, et/ou à des poursuites judiciaires.

127. En outre, l'utilisateur s'expose à des sanctions concernant son droit d'utiliser les systèmes d'information et de communication, notamment, le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie des systèmes d'information et de communication, de sites web et des applications, ou l'exclusion.

11. Entrée en vigueur

128. Dans le cadre de sa fonction consultative, le comité technique a examiné le respect des dispositions légales et réglementaires de la présente et a donné un avis pour son application. La présente charte entrera en vigueur un mois à compter de sa publication par l'établissement.