Université de Ghardaïa

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

uer

Université De Ghardaïa :

26/12/2022

Sommaire

1. Préambule

1. La présente charte de L'Université de Ghardaïa 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 des ressources informatiques 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 ressources informatiques et numériques, en conformité avec les dispositions légales et réglementaires applicables ainsi que la jurisprudence des Cours et Tribunaux.
3. Elle tient compte notamment des recommandations du référentiel national de sécurité de l'information (RNSI2020).
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 ressources informatiques et numériques.
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 cellule de sécurité de l'information (RCSI) de l'établissement (mailto:rcsi@univ-ghardaia.dz)

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 d'un poste informatique, 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 moyens et des ressources informatiques et numériques de l'établissement ;
   - **« 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, internet, réseau interne ou poste informatique personnel, 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 ;
- **« 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 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, invité, personnel externe (incubateur, collaborateur scientifique etc.) concourant à l'exécution des missions du service public de la recherche et de l'éducation.
12. 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.

4.2 Usages concernés

13. 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, 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.).

5. Conditions d'utilisation générales

5.1 Usage professionnel

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

14. 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.
15. Selon la jurisprudence, sont présumés avoir un caractère professionnel, notamment :
    - 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.
16. Il en résulte que :

- 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.

17. **Messagerie électronique.** En particulier, l'adresse électronique, composée de «nom .prénom @univ-ghardaia.dz », 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.
18. Les listes de diffusion permettant la réception automatique et périodique d'informations doivent être réservées à un usage professionnel.
19. 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.).
20. **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

21. 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 de l'établissement.

5.2 Usage non professionnel

22. 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.
23. Cette tolérance pourra être suspendue ou limitée en cas d'abus.
24. 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 ;
    - 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.
25. 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 «nom. prénom@univ-ghardaia.dz »).

26. 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 ».
27. A défaut d'utiliser le terme « PRIVE », tous les répertoires informatiques et tous les messages informatiques sont considérés comme professionnels.
28. 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.
29. 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.
30. 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 ;
    - 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 :

    - 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 ;
    - 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 autorité habilitée à cet effet.
31. 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, injurieux, violent, raciste, 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

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

34. 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 ;
    - lorsqu'un accès distant lui est accordé, d'utiliser d'autres moyens d'authentification que ceux qui lui sont remis à cet effet.

35. Les mots de passe doivent être robustes et modifiés régulièrement conformément à la politique de gestion des mots de passe.
36. En termes de sécurité et de confidentialité, l'utilisateur devra suivre toutes les prescriptions complémentaires qui lui seront signifiées par le responsable de la cellule de sécurité des d'information (RCSI).

5.3.1 Perte, vol ou compromission

37. 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, et avertir le RCSI de l'établissement.
38. L'utilisateur devra aviser, sans délai, le RCSI, de la perte ou du vol d'un équipement informatique dont il a l'usage, afin qu'une étude d'impacts soit menée.
39. 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 RCSI, 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.
40. 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.