



جامعة باتنة 1 - الحاج لخضر
University of Batna 1
Hadj Lakhdar

CHARTRE REGISSANT L'USAGE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION AU SEIN DE L'UNIVERSITE

SOMMAIRE

1. PRÉAMBULE ET OBJET

2. CHAMP D'APPLICATION

3. OBLIGATIONS ET RESPONSABILITÉS DE L'UTILISATEUR

- 3.1. Définition de l'utilisateur
- 3.2. Devoirs fondamentaux
- 3.3. Confidentialité et secret professionnel

4. GESTION DES COMPTES ET ACCÈS

5. UTILISATION DES LOGICIELS

- 5.1. Logiciels sous licence et logiciels libres
- 5.2. Logiciels développés en interne

6. COMMUNICATION ET RÉSEAUX SOCIAUX

- 6.1. Messagerie électronique professionnelle
- 6.2. Utilisation d'Internet
- 6.3. Usage des Réseaux Sociaux

7. GESTION DES ÉQUIPEMENTS ET SÉCURITÉ

- 7.1. Equipements Informatiques Mis à disposition par l'université de Batna 1
- 7.2. Usage à des fins personnelles
- 7.3. Protection contre les malwares

8. DROIT DE PROPRIÉTÉ INTELLECTUELLE

9. CONTRÔLE, INCIDENTS ET SANCTIONS

10. ENTRÉE EN VIGUEUR

1. PRÉAMBULE ET OBJET

Objet

- La présente charte définit les règles d'usages et de sécurité que l'Université de Batna 1 et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun. Elle définit également les règles de sécurité que les utilisateurs doivent respecter et cela afin de permettre un usage optimal des ressources informatiques et des services internet de l'Université

Préambule

- L'évolution exponentielle des technologies de l'information et de la communication, et la diversification des solutions accroissent la nécessité de reconsidérer la politique d'utilisation des ressources de tout système d'information de n'importe quel institution ou entreprise, de ce fait, une charte d'utilisation du système d'information doit être définie.
- Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.
-
- Le «système d'information» constitue l'ensemble des ressources matérielles, logicielles et réseaux de télécommunications et de données, pouvant être mis à disposition de l'utilisateur par l'Université de Batna 1. L'informatique nomade (ordinateurs portables, téléphones portables, ...) est également un des éléments constitutifs du système d'information.

2. CHAMP D'APPLICATION

La présente charte s'applique à tous les utilisateurs. Elle s'applique, au même titre, aux utilisateurs autorisés à accéder au système d'information/Informatique de l'université Batna 1 via leurs équipements informatiques personnels.

3. OBLIGATIONS ET RESPONSABILITÉS DE L'UTILISATEUR

a. 3.1. Définition de l'utilisateur

- Un « utilisateur » est toute personne autorisée à accéder aux ressources du système d'information, dans le cadre de l'exercice de son activité universitaire, quel que soit son statut et son type d'accès, de manière permanente ou temporaire, aux ressources informatiques de l'Université :
- Tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche ;
- Tout étudiant inscrit à l'université de batna1 ;
- Tout prestataire ou partenaire1 ayant contracté avec l'université ;
- Toute personne autorisée

b. 3.2. Devoirs fondamentaux

- Respecter la présente charte et veiller au strict respect de son application par les utilisateurs sous sa responsabilité.
- Concourir à la protection des ressources du système d'information mises à sa disposition dans le cadre de l'exercice de ses fonctions.
- Signaler à la structure habilitée toute violation ou tentative de violation de l'intégrité des ressources du système d'information mises à sa disposition.
- Ne pas modifier les paramètres de l'équipement informatique et des ressources du système d'information mis à sa disposition, ni tenter de contourner aucun des systèmes d'information mis à sa disposition, ni tenter de contourner aucun des systèmes de sécurité mis en place par l'université.

- Ne pas se livrer à une activité concurrente à celle de l'université ou susceptible de lui causer un quelconque préjudice en utilisant son système d'information.

c. 3.3. Confidentialité et secret professionnel

Responsabilités :

- L'utilisateur est le responsable direct de l'usage des ressources informatiques et du système d'information mis à sa disposition dans le cadre de l'exercice de ses fonctions. Tout manquement aux dispositions de la présente charte engage la responsabilité de l'utilisateur, en vertu du règlement intérieur.

Confidentialité :

- L'utilisateur est tenu à l'obligation du secret professionnel et ne doit en aucun cas divulguer des données qu'il manipule dans le cadre de l'exercice de ses fonctions.
- L'utilisateur ne doit pas tenter de prendre connaissance des données que seuls d'autres utilisateurs sont autorisés à manipuler.
- Les utilisateurs administrateurs de ressources du système d'information ne doivent en aucun cas prendre connaissance des données et informations auxquelles ils peuvent accéder dans le cadre de l'exercice de leurs fonctions. Ils doivent respecter les règles d'éthique et de déontologie définies dans des procédures et documents spécifiques.
-

4. GESTION DES COMPTES ET ACCÈS

- Compte Utilisateur et Droit D'accès :

- L'attribution d'un compte à un utilisateur donne lieu à des droits d'accès spécifiques aux ressources du système d'information plateformes ou Messagerie professionnelle de l'université.
- L'utilisateur est responsable de l'usage des ressources du système d'information sur lesquelles il dispose de droits d'accès.

- L'utilisateur doit :

- Mémoriser le mot de passe de son compte et le garder strictement confidentiel.
- Verrouiller sa session de travail avant de quitter son poste de travail ;
- Signaler, à la structure habilitée, toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
- Signaler, à la structure habilitée, tout droit d'accès non afférent à ses fonctions (accès à certains fichiers, affectation à un groupe, ...) ;
- Informer la structure habilitée de tout changement de poste ou d'habilitations impliquant une modification de ses droits d'accès ou ceux de ses subordonnés.

- L'utilisateur ne doit pas :

- Communiquer son compte à d'autres utilisateurs. Le compte est strictement personnel.
- Utiliser ou tenter d'utiliser des comptes autres que le sien.
- Conserver le mot de passe de son compte en lieu non sûr (post-it sur le bureau, fichier en clair, etc...).

5. UTILISATION DES LOGICIELS

5.1. Logiciels sous licence et logiciels libres

- L'utilisateur est responsable de l'usage des logiciels mis à sa disposition, il est tenu de faire preuve d'un usage loyal et rationnel en respectant les recommandations de sécurité du logiciel lors de toute manipulation de données extraites du système d'information.
- Le recours par l'utilisateur à l'usage d'un logiciel libre doit être motivé. La structure habilitée se prononce sur l'autorisation ou pas de l'usage du logiciel libre en tenant compte des paramètres de compatibilité, de sécurité, de support et d'évolutivité.

5.2. Logiciels développés en interne

- Tout logiciel ou macro est « propriété exclusive de l'université » s'il est développé en interne par les moyens et personnel de l'université.

6. COMMUNICATION ET RÉSEAUX SOCIAUX

6.1. Messagerie électronique professionnelle

La messagerie électronique de l'université de Batna 1 (@univ-batna.dz et @univ-batna1.edu.dz) est mise à la disposition des utilisateurs (Enseignants, Etudiants et Personnels Administratif) pour un usage strictement professionnel.

- L'utilisateur est tenu de préserver le bon fonctionnement de ce service par le respect des règles de sécurité et de bon usage définies infra et s'abstenir, entre autres, de diffuser des messages, des documents, des informations, des images ou des vidéos, particulièrement :
 - Portant atteinte à l'image de l'université.
 - Portant atteinte au respect des droits des personnes et droits publics.
 - De publicité ou de propagande.
 - À caractère autre que défini par la vocation de l'Université et la recherche scientifique.
- L'utilisateur doit :
 - Utiliser exclusivement la messagerie de l'université lors des échanges professionnels ;
 - Vérifier, avant l'envoi de messages, l'identité des destinataires et leur habilitation à recevoir les informations transmises.
 - Protéger les messages contenant des données classifiées conformément aux directives de la procédure de sécurisation des documents électroniques classifiés en vigueur.
- L'utilisateur ne doit pas :
 - Ouvrir les messages électroniques reçus de source douteuse, ces messages devront être impérativement supprimés ;
 - Cliquer sur tout lien ou ouvrir des pièces jointes contenus dans des messages dont l'origine semble douteuse ;
 - Tenter d'accéder à des messages autres que les siens. En cas de réception par erreur d'un message professionnel dont on n'a pas l'habilité, prévenir immédiatement l'expéditeur et procéder à la suppression du message ;
 - Utiliser l'adresse email professionnelle pour l'inscription aux réseaux sociaux ou souscrire notamment, à des groupes de Newsletter ou forums non professionnels ;
 - Procéder à des diffusions de messages non professionnels pouvant entraîner la saturation et la dégradation du service de messagerie ;
 - Relayer des messages de type Hoax1 comportant des instructions demandant de les faire suivre à d'autres personnes.

6.2. Utilisation d'Internet

L'université de Batna 1 met à la disposition des utilisateurs un accès à internet dans le cadre de l'exercice de leurs fonctions. L'utilisateur est informé que pour des raisons de sécurité et d'éthique l'accès à certains sites ou services internet peut être limité ou prohibé.

Lors de la navigation sur internet via le réseau de l'université :

L'utilisateur doit :

- Se connecter exclusivement à travers la connexion sécurisée mise à sa disposition.
- Se conformer aux lois en vigueur, en particulier celles relatives aux publications à caractère injurieux, raciste, pornographique et diffamatoire.
- Faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les forums de discussions.

L'utilisateur ne doit pas :

Contourner les restrictions d'utilisation d'internet mises en place par l'université, notamment dans le but de :

- Se livrer à une activité personnelle ou à des fins lucratives ;
- Accéder à des sites douteux, aux pratiques illégales très souvent vecteur de propagation de Malwares ;
- Diffuser, télécharger des données, des logiciels ou du contenu multimédia protégés par le droit de propriété intellectuelle ;
- Prendre part à des jeux en ligne ou à des paris.

6.3. Usage des Réseaux Sociaux

- Les réseaux sociaux sont des outils de communication et de collaboration, largement utilisés, L'université de Batna 1, exploite les multiples avantages des réseaux sociaux à bon escient. L'utilisateur est responsable de l'usage des réseaux sociaux, il est tenu de respecter les règles citées ci-après.

L'utilisateur doit :

- S'abstenir de porter préjudice à l'université par la publication de contenu de nature à nuire à son image ou à celle de ses employés ;
- Se conformer à l'obligation de réserve vis-à-vis de l'institution.
- Respecter les Conditions Générales d'Utilisation (CGU) des réseaux sociaux utilisés ;
- Veiller à vérifier la véracité de l'information et sa source pour ne pas faire office de relayer des Hoax.

L'utilisateur ne doit pas :

- Partager des données professionnelles ou tout autre contenu multimédia de l'institution, notamment via messageries instantanées grand public ;
- Utiliser son adresse de messagerie professionnelle pour s'identifier ou s'inscrire sur des réseaux sociaux à titre personnel ;
- Fournir des informations liées à sa position au sein de la Société telles que sa fonction, son grade ou responsabilité sur les réseaux sociaux non professionnels notamment, lors du renseignement des formulaires d'inscription ;
- Propager des Malwares. Le fait de faire suivre ou de cliquer sur des publications douteuses pourrait nuire à la sécurité du poste de travail et du système d'information de l'université.

Supervision de la navigation Internet :

- L'utilisateur est informé qu'un dispositif de supervision et de filtrage est mis en place pour s'assurer du bon fonctionnement du service internet et contrôler son utilisation. Le dispositif permet d'enregistrer tous les accès aux sites effectués par les utilisateurs.

7. GESTION DES ÉQUIPEMENTS ET SÉCURITÉ

7.1. Equipements Informatiques Mis à disposition par l'université de Batna 1

Supervision de la navigation Internet :

- L'utilisateur est informé qu'un dispositif de supervision et de filtrage est mis en place pour s'assurer du bon fonctionnement du service internet et contrôler son utilisation. Le dispositif permet d'enregistrer tous les accès aux sites effectués par les utilisateurs.

7.2. Usage à des fins personnelles

- L'usage des équipements informatiques à des fins personnelles est toléré dans la stricte mesure où il demeure exceptionnel et doit obéir aux conditions suivantes.
- **L'utilisateur ne doit pas :**
- Entraver ou interférer avec l'activité professionnelle ;
- Configurer la messagerie électronique et instantanée personnelles sur les smartphones et tablettes ;
- Exercer une activité commerciale privée, de divertissement ou politique ;
- Générer des coûts supplémentaires pour l'université par l'usage abusif de consommables.

7.3. Protection contre les malwares

- Les Malwares peuvent s'introduire dans un système d'information par différents moyens, notamment par support amovible (clé USB, et autres), logiciel non autorisé, messagerie électronique, internet, etc...
- L'utilisateur est tenu de respecter et de se conformer aux règles de sécurité mises en place afin de préserver les données et les ressources du système d'information et de lutter contre les Malwares et les cyberattaques.

L'utilisateur doit :

- Signaler tout comportement anormal ou suspect ou toute anomalie détectée au niveau de son équipement informatique notamment :
- Blocage ;
- Ouverture intempestive de fenêtres à l'écran ;
- Affichage et disparition immédiate de boîtes de dialogue au démarrage ;
- Message d'erreur cyclique et récurrent ;
- Présence de fichiers inconnus (film, musique, etc.) ;
- Lenteur inexplicable.
- Etre attentif aux messages d'alerte de son antivirus ;
- Contribuer à atténuer la propagation de Malwares en n'activant pas les macros sur les produits offices ou autres, qu'en cas de besoin ;
- Se prémunir contre d'éventuelles pertes de fichiers importants qui peuvent être occasionnées par ransomwares, en les stockant sur des espaces de stockage sécurisés.
- Veiller à soumettre, pour analyse virale, toute clé USB ou autre support amovible fourni par des tiers ou exploité en dehors du système d'information, avant son utilisation.

L'utilisateur ne doit pas :

- Installer des logiciels, sans autorisation, qui peuvent être un vecteur de propagation de Malwares.
- Tenter de désactiver, désinstaller ou supprimer l'antivirus fourni par l'institution ;
- Cliquer sur les publicités qui s'affichent sur les pages web ;
- Opérer des téléchargements illicites (logiciels craqués, œuvres protégées...) très souvent vecteurs de propagation de Malwares.

8. DROIT DE PROPRIÉTÉ INTELLECTUELLE

- L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.
- Toute création ou œuvre intellectuelle produite par l'utilisateur dans le cadre professionnel est considérée comme propriété intellectuelle de l'université Batna1.

9. CONTRÔLE, INCIDENTS ET SANCTIONS

- En cas d'incident pouvant affecter la sécurité informatique, l'organisme peut :

- Isoler ou neutraliser provisoirement toute donnée, fichier ou matériel en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information ;
 - Prévenir le responsable de la sécurité informatique de l'université Batna1.
- Non-respect de la charte :**
- Le non-respect des règles définies dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des mesures disciplinaires proportionnelles à la gravité des faits constatés.
 - Sous réserve que soit informé le responsable hiérarchique, le responsable de la sécurité informatique peut :
 - Avertir un utilisateur ;
 - Limiter ou retirer provisoirement les accès d'un utilisateur à ses différents comptes ;
 - Effacer, compresser ou isoler toute données ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information.

10. ENTRÉE EN VIGUEUR

- Cette Charte entre vigueur dès sa notification aux utilisateurs. Elle est publiée sur le site web de l'Université de Batna1 et envoyée par mail.