الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieu
de la recherche scientifique
Université Mouloud Mammeri de
Tizi-Ouzou

وزارة التعليم العالي والبحث العلمي

جامعة مولود معمري تيزي وزو

Charte de sécurité informatique

Textes de référence

Texte légal ou réglementation.	**Références.**
Réglementation relative aux mesures cryptographiques.	Décret exécutif n°16-61 du 02 Joumada El Oula 1437 correspondant au 11 février 2016 modifiant et complétant le décret exécutif n° 09-410 du 23 Dhou El-Hidja 1430 correspondant au 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles.
Les règles générales relatives à la poste et aux communications électroniques	loi n°18-04 du 24 Chaâbane 1439 correspondant au 10 mai 2018 fixant les règles générales relatives à la poste et aux communications électroniques.
Propriété intellectuelle (Les logiciels)	Ordonnance n°03-05 du 19 Joumada EL Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins.
Certification électronique	Loi n°15-04 du 11 Rabie Ethani 1436 correspondant au 1er Février 2015 fixant les règles générales relatives à la signature et à la certification électroniques. Décret n°2016-134 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'Autorité nationale de certification électronique. Décret n°2016-135 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant la nature, la composition, l'organisation et le fonctionnement de l'Autorité gouvernementale de certification électronique.
Protection des données à caractère personnel.	Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.
Les infractions liées aux technologies de l'information et de la communication	Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 05 aout 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.
Lutte contre la cybercriminalité.	Décret présidentiel n° 14-252 du 13 Dhou El Kaada 1435 correspondant au 8 septembre 2014 portant ratification de la convention arabe pour la lutte contre la cybercriminalité.
Droits sur les travaux scientifiques – thèses de doctorat	Décret exécutif n°22-208 du 5 Dhou El Kâada 1443 correspondant au 5 juin 2022 fixant le régime des études et de la formation en vue de l'obtention des diplômes de l'enseignement supérieur.

Charte de sécurité informatique

Préambule

L'université Mouloud Mammeri de Tizi-Ouzou met à la disposition des utilisateurs des moyens informatiques afin de leur permettre d'accomplir les missions qui leurs sont assignées. Une mauvaise utilisation de ces moyens augmente les risques d'atteinte à la sécurité du système d'information de l'université.

Chaque faculté et vice-rectorats désigne un responsable informatique. Ces informaticiens, sous le contrôle du Centre des Systèmes et Réseaux, constituent la cellule de sécurité informatique de l'université. Elle est présidée par le RSSI (Responsable de la sécurité des systèmes d'information).

Article 1 : Objet

La présente charte a pour objet de définir les conditions et modalités d'utilisation des ressources informatiques de l'Université Mouloud Mammeri de Tizi-Ouzou. Elle définit également les règles de sécurité que les utilisateurs doivent respecter.

Article 2 : Champ d'application

La présente charte s'applique à toute personne ayant accès, de manière permanente ou temporaire et avec le matériel de l'université ou son matériel personnel, aux ressources informatiques de l'Université Mouloud Mammeri de Tizi-Ouzou.

Le RSSI, le Centre des Systèmes et Réseaux et les informaticiens des facultés sont tenus de la faire appliquer.

Article 3 : de la propriété des ressources informatiques

Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive de l'Université Mouloud Mammeri de Tizi-Ouzou ;

Article 4 : Conditions d'accès aux ressources et au réseau informatique

Tout accès aux ressources et aux plateformes web de l'Université Mouloud Mammeri de Tizi-Ouzou est soumis à une procédure d'authentification préalable.

Tout utilisateur est seul responsable de ses publications sur le web.

Article 5 : responsabilité de l'utilisateur

L'utilisateur est seul responsable de toute utilisation des moyens d'authentification mis à sa disposition par l'Université Mouloud Mammeri de Tizi-Ouzou.

L'utilisateur est tenu de modifier ses mots de passe dès sa première connexion sur les plateformes.

Article 6 : protection des moyens d'authentification

Afin de préserver les moyens d'authentification mis à sa disposition, l'utilisateur doit :

- Veiller à la protection et à la préservation de ses informations secrètes d'authentification;
- Changer périodiquement ses informations secrètes d'authentification ;
- Utiliser des mots de passe d'au moins douze caractères composés de lettres, de chiffres et de caractères spéciaux ;

Il est strictement interdit de communiquer ses informations secrètes d'authentification aux tiers.

Article 7 : Utilisation des ressources informatiques

- Les ressources informatiques de l'Université Mouloud Mammeri de Tizi-Ouzou ne peuvent être utilisées qu'à des fins en relation directe avec ses activités professionnelles à l'UMMTO ;
- L'utilisateur doit préserver les ressources et les moyens informatiques mis à sa disposition ;
- L'utilisateur n'est pas autorisé à installer / désinstaller ou à déployer des applications ou des logiciels sur les moyens ou les ressources informatiques mis à sa disposition sans autorisation préalable ;

Article 8 : Obligations de l'organisme vers les utilisateurs

L'organisme doit :

- Mettre à la disposition de l'utilisateur les ressources informatiques nécessaires à l'exécution des missions qui lui incombent ;
- Garantir le bon fonctionnement et la disponibilité des ressources informatiques ;
- Maintenir la qualité du service fourni aux utilisateurs dans la limite des moyens alloués ;
- Informer les utilisateurs des procédures et des politiques applicables en matière de ressources informatiques ;
- Mettre en œuvre les moyens nécessaires pour assurer la confidentialité et l'intégrité des documents et des échanges électroniques des utilisateurs ;
- Informer les utilisateurs que les activités sur le réseau et les systèmes font l'objet d'une surveillance automatisée ;
- Sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

Article 9 : Obligations de l'utilisateur

L'utilisateur doit :

- Respecter les lois et règlements en vigueur ;
- Respecter la présente charte ainsi que les différentes procédures et politiques de l'Université ;
- Appliquer scrupuleusement les mesures et les directives de sécurité informatique de

l'Université ;

- Ne pas utiliser ou tenter d'utiliser les comptes d'autrui ;
- Signaler sans délai tout fonctionnement suspect ou incident de sécurité.

Article 10 : de la sécurité et de la protection du poste de travail

L'utilisateur doit respecter scrupuleusement les consignes de sécurité suivantes :

- Verrouiller l'accès au poste de travail en cas d'absence, même temporaire ;
- Alerter les services techniques en cas de découverte d'un nouvel équipement connecté au poste de travail ;
- S'assurer que son poste de travail dispose d'un antivirus, et informer le service concerné de toute alerte de sécurité ;
- Ne jamais connecter des équipements personnels au poste de travail ;
- Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser ;
- Eteindre l'ordinateur pendant les périodes d'inactivité prolongée (nuit, weekend, vacances ,…) ;
- Ne pas intervenir physiquement sur le matériel (ouvrir les unités centrales, ...).

Article 11 : de l'utilisation de la messagerie électronique professionnelle

L'Université Mouloud Mammeri de Tizi-Ouzou met à la disposition des étudiants, enseignants et fonctionnaires ATS des comptes de messagerie électronique professionnelle dans le domaine ummto.dz, qui leurs permettent d'émettre et de recevoir des messages électroniques à caractère professionnel.

Des comptes de messagerie professionnelle sont également créés pour les manifestations scientifiques et les services administratifs de l'UMMTO.

L'utilisation de la messagerie professionnelle est obligatoire dans le cadre des activités professionnelles à l'UMMTO ;

La messagerie professionnelle ne peut être utilisée qu'à des fins professionnelles, pédagogiques ou de recherche. A cet effet, il est strictement interdit de :

- L'utiliser pour l'enregistrement sur les réseaux sociaux, les forums et les sites web ;
- Ouvrir les pièces jointes et/ou les liens hypertexte transmis à partir d'adresses mail inconnues ;
- Ouvrir la boite mail professionnelle à partir des espaces communautaires d'accès à internet notamment les cybercafés ;

Lorsque les missions de l'utilisateur nécessitent son enregistrement sur les réseaux sociaux, les forums ou les sites web, une adresse mail dédiée à cet effet lui est attribuée après avis favorable de l'autorité habilitée.

L'utilisateur doit faire preuve de vigilance lors de l'utilisation des courriers électroniques et ceci en s'assurant que :

- L'adresse du destinataire est bien formulée ;

- Le destinataire est habilité à accéder au contenu transmis ;
- Les bonnes pièces jointes ont été rattachée au document.

Les comptes professionnels des services (décanat, services, vice-rectorats…) sont la propriété du service. Chaque responsable sortant doit communiquer ses coordonnées de connexion à son successeur sans effacer aucune donnée du compte. Cette opération doit figurer dans le PV de passation de consignes.

Article 12 : de l'utilisation d'Internet

Les utilisateurs ayant accès à Internet s'engagent à :

- Limiter l'utilisation d'Internet à des fins pédagogiques, d'apprentissage ou professionnelles. L'exploration d'Internet à des fins personnelles est, toutefois, tolérée, mais ne doit en rien porter atteinte au bon fonctionnement du réseau ou à la productivité de l'utilisateur. Elle se fera, exclusivement, en dehors des heures de travail ;
- L'accès à Internet ne peut être utilisé à des fins prohibées, décrites ci-dessous ;
- Il est strictement interdit d'accéder aux sites dont le contenu est illégal ;
- L'accès à des sites de téléchargement de torrents ou l'utilisation d'aspirateurs de bande passante sont strictement interdits ;
- Ne pas surcharger le réseau de l'université ;
- Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus.
- La bande passante de l'université est répartie équitablement entre ses différents services. Toutefois, une partie du débit peut être réquisitionnée lors des opérations importantes, telle que l'inscription des nouveaux bacheliers.

Article 13 : de l'utilisation de la plateforme de télé-enseignement

L'université Mouloud Mammeri de Tizi-Ouzou dispose d'une plateforme de télé-enseignement gérée par le Centre des Systèmes et Réseaux. Les informaticiens des facultés disposent d'un accès administrateur pour gérer leurs parties de cette plateforme.

Tous les enseignants-chercheurs et tous les étudiants de l'Université disposent d'un compte sur la plateforme de télé-enseignement.

Ces utilisateurs sont responsables des données qu'ils publient sur cette plateforme.

Les données publiées doivent être uniquement à caractère pédagogique, dont le contenu reste la propriété de son auteur. Toute sorte de plagiat est interdite et son auteur en assume les conséquences.

Article 14 : du dépôt institutionnel de l'université

Les thèses et mémoires des enseignants et étudiants, ainsi que les résumés des communications, sont publiés sur le dépôt institutionnel de l'université (dSpace). Ces données sont alors

consultables en ligne sur les plateformes web de l'université.

Article 15 : des appareils mobiles et de supports de stockage

L'utilisateur doit :

- Signaler, à la hiérarchie dans l'immédiat, toute perte ou vol d'un appareil mobile ou support de stockage professionnel ;
- Verrouiller les appareils mobiles contenant des données professionnelles lorsqu'ils ne sont pas utilisés ;
- Interdire formellement pour toute personne étrangère à l'UMMTO de transférer des documents par support amovible, tout échange de document doit se faire par courriel. Dans le cas où le volume de données exige le recours à un support amovible, ce dernier doit être analysé par les services compétents avant toute utilisation ;
- Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage ;
- Garder ses appareils mobiles et supports de stockage amovible sur soi, lors des déplacements professionnels.

Article 16 : Mesures de sécurité à appliquer lors des déplacements à l'étranger

- Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage ;
- Le missionnaire doit supprimer toutes les données professionnelles sensibles, non nécessaires à la mission, de tous les supports amovibles avant tout déplacement à l'étranger ;
- Il doit informer la hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger ;
- Il est interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles ;
- Il doit mentionner dans les comptes rendus de la mission, la liste des objets connectés offerts lors du déplacement ;
- Il est formellement interdit qu'un transfert des documents par un étranger se fasse via des supports de stockage amovibles. Tout échange de document doit se faire exclusivement par courriel ;
- Le missionnaire doit changer les mots de passe utilisés pendant la mission.

Article 17 : fin de la relation liant l'utilisateur à l'UMMTO

- Lorsque la relation liant l'utilisateur à l'Université prend fin, l'utilisateur doit restituer à l'organisme toutes les ressources informatiques matérielles mises à sa disposition ;
- L'Université procédera à la suppression de l'ensemble des accès logiques de l'utilisateur aux ressources informatiques mises à sa disposition.

- Les comptes de messagerie professionnelle resteront opérationnels même après le départ de l'utilisateur.

Article 18 : gestion des incidents

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

- Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- Isoler ou neutraliser provisoirement toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information ;
- Prévenir le responsable informatique de la faculté, le Centre des Systèmes et Réseaux ou le RSSI.

Article 19 : du 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'entrainer à son encontre des mesures disciplinaires proportionnelles à la gravité des faits constatés.

Sous réserve que soit informé le responsable hiérarchique, les responsables de la sécurité informatiques peuvent :

- Avertir un utilisateur ;
- Limiter ou retirer provisoirement les accès d'un utilisateur ;
- Effacer, comprimer ou isoler toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information.

Sans préjudice des sanctions disciplinaires le contrevenant aux dispositions de la présente charte peut faire l'objet de poursuites judiciaires.

Article 20 : entrée en vigueur

Cette Charte entre en vigueur dès sa publication sur le site web de l'université. Elle est affichée lors de l'authentification au réseau local de l'université et notifiée aux utilisateurs par mail professionnel.