CHARTE D'UTILISATION DE LA MESSAGERIE INSTITUTIONNELLE

UNIVERSITÉ M'HAMED BOUGARA DE BOUMERDES

Version 2.0
Date d'entrée en vigueur : Janvier 2025
Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC)

Préambule

La messagerie électronique constitue le premier moyen de communication de l'établissement, utilisé en raison de la facilité et de la rapidité de transmission et de réception électronique d'information. L'Université M'hamed Bougara de Boumerdès (UMBB) met à disposition de l'ensemble des utilisateurs (étudiants, enseignants, personnel administratif et technique) un service de gestion de messagerie qui répond à un objectif pédagogique et professionnel.

La présente charte définit les règles relatives à l'utilisation des ressources et services mis à disposition par l'université et tend à sensibiliser les utilisateurs aux risques liés à leur utilisation en termes d'intégrité et de confidentialité des données traitées et de sécurité informatique.

Elle s'inscrit dans le respect des valeurs universitaires, de la déontologie académique, de la législation algérienne en vigueur et des normes internationales de protection des données personnelles.

Elle vise à définir les règles d'usage, les droits et obligations des utilisateurs, ainsi que les mesures de sécurité et de gouvernance associées à ce service institutionnel géré par le Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC).

Article 1 : Objet et Champ d'Application

1.1 Objet de la charte

La présente charte définit les règles et bonnes pratiques d'utilisation de la messagerie électronique institutionnelle de l'UMBB. Elle s'applique à l'ensemble des services de messagerie fournis par l'université sous le domaine **@univ-boumerdes.dz** ou tout autre domaine institutionnel en usage.

1.2 Champ d'application

Cette charte s'applique à tous les utilisateurs disposant d'un compte de messagerie institutionnelle :

- Personnels enseignants-chercheurs et enseignants
- Personnels administratifs, techniques et de service
- Doctorants et post-doctorants

- Étudiants inscrits à l'université
- Partenaires externes bénéficiant d'un compte institutionnel temporaire

1.3 Périmètre technique

Le champ d'application couvre l'ensemble des services de messagerie et outils collaboratifs mis à disposition par l'université :

- La création, l'envoi et la réception de courriels via les serveurs de messagerie institutionnels
- L'utilisation des applications et services connectés au compte de messagerie (webmail, clients de messagerie standards IMAP/POP/SMTP, applications mobiles)
- La gestion des données professionnelles échangées par ce moyen de communication
- L'utilisation des calendriers et agendas partagés ou personnels
- L'utilisation du Drive universitaire (stockage et partage de documents - quota de 15 Go)
- L'utilisation des outils d'édition collaborative de documents (traitement de texte, tableurs, présentations)
- L'utilisation des services de visioconférence institutionnelle
- Les carnets d'adresses et contacts institutionnels
- L'accès à distance et la synchronisation multi-appareils

Important : Le stockage de données à caractère personnel sur le Drive universitaire est strictement interdit. Seules les données liées aux activités universitaires, académiques, scientifiques et administratives sont autorisées.

Article 2 : Principes Généraux d'Utilisation

2.1 Cadre juridique général

L'utilisation de la messagerie électronique s'inscrit dans le cadre légal et réglementaire en vigueur et, notamment, des dispositions relatives au droit au respect de la vie privée et à l'usage professionnel.

2.2 Valeur juridique de l'email

- Tout message électronique ainsi que ses éventuelles pièces jointes, envoyé depuis la messagerie professionnelle, engage non seulement la responsabilité et l'image de l'utilisateur mais aussi celle de l'université
- L'usage de la messagerie électronique doit être adapté à l'organisation interne de l'université
- Respect des procédures de contrôle, de validation et d'autorisation, de la hiérarchie, de l'éthique et de la déontologie
- Tout message ou contenu pouvant porter atteinte à l'image de l'établissement public est susceptible de faire l'objet de sanctions disciplinaires

2.3 Usage professionnel et académique prioritaire

La messagerie institutionnelle est mise à disposition prioritairement pour les communications liées aux activités universitaires, académiques, scientifiques et administratives :

- Échanges pédagogiques entre enseignants et étudiants

- Coordination des activités de recherche
- Communication administrative et institutionnelle
- Relations avec les partenaires académiques et professionnels
- Diffusion d'informations officielles de l'université

2.4 Usage personnel encadré

La messagerie doit être utilisée à des **fins professionnelles et académiques**. L'utilisation de la messagerie à des fins personnelles est toutefois autorisée de manière raisonnée, à condition qu'elle :

- Reste exceptionnelle et limitée en volume
- N'interfère pas avec les activités professionnelles
- N'entrave pas le trafic normal des messages professionnels
- Ne contrevienne pas aux règles de l'institution
- N'entraîne pas de surcharge des infrastructures
- Respecte les principes déontologiques et éthiques

Tout abus caractérisé peut entraîner des mesures de restriction d'accès.

2.5 Interdictions formelles

Sont strictement prohibées les utilisations suivantes :

- **Activités commerciales non autorisées** : Toute utilisation commerciale à des fins lucratives personnelles ou externes sans autorisation explicite de la direction
- **Contenus illicites** : Diffusion de contenus contraires à la loi algérienne (contenus diffamatoires, injurieux, discriminatoires, racistes, sexistes, pornographiques)
- **Prosélytisme** : Promotion d'idéologies politiques, religieuses ou sectaires susceptibles de porter atteinte à la neutralité de l'établissement
- **Chaînes de messages** : Transmission de chaînes de messages, canulars (hoax) ou messages sans rapport avec l'activité universitaire
- **Activités malveillantes** : Envoi de virus, logiciels malveillants, tentatives de phishing ou toute activité de nature à compromettre la sécurité des systèmes
- **Usurpation d'identité** : Utilisation du compte d'autrui ou dissimulation de sa propre identité

2.6 Respect de la déontologie académique

L'ensemble des utilisateurs (étudiant, doctorant, enseignant, personnel administratif et technique) est soumis à un certain nombre d'obligations liées à la déontologie et à la loyauté dans l'usage qui est fait des Systèmes d'Information et de Communication (SIC).

L'usage de la messagerie doit respecter les principes fondamentaux de l'éthique universitaire :

- Ces outils doivent être utilisés avec discernement, honnêteté, courtoisie et intégrité afin de garantir la confidentialité des informations circulant sur les supports informatiques
- Respect de la liberté d'expression dans le cadre académique
- Courtoisie et professionnalisme dans les échanges

- Respect de la hiérarchie institutionnelle tout en préservant la libre circulation de l'information académique
- Protection de l'intégrité scientifique et intellectuelle
- Dans tous les cas, l'utilisateur est responsable de l'usage qu'il fait des outils informatiques et de communication mis à sa disposition par l'université, tant d'un point de vue moral que pénal

2.7 Discrétion professionnelle

La discrétion professionnelle doit être respectée pour toutes les données, informations ou documents dont les utilisateurs ont connaissance dans l'exercice de leurs fonctions, qu'elles concernent les utilisateurs de l'université, leurs différents interlocuteurs ou les usagers du service public.

En cas d'utilisation d'appareils personnels (téléphone mobile, tablette, ordinateur) pour consulter la messagerie électronique de l'université, l'utilisateur doit impérativement protéger ces appareils par tous moyens, notamment par un code confidentiel.

Article 3 : Confidentialité et Protection des Données

3.1 Respect de la confidentialité

Les utilisateurs s'engagent à respecter la confidentialité des informations échangées via la messagerie, particulièrement pour :

- Les données personnelles des étudiants (notes, situations personnelles, dossiers administratifs)
- Les informations relatives aux activités de recherche (résultats non publiés, données expérimentales)
- Les données financières et comptables de l'université
- Les délibérations des instances universitaires
- Les informations relatives aux ressources humaines

3.2 Obligation de discrétion professionnelle

Les messages échangés dans le cadre professionnel ne doivent pas être partagés avec des tiers non autorisés, sauf :

- Obligation légale (réquisition judiciaire)
- Autorisation explicite de l'émetteur
- Nécessité de service dûment justifiée

3.3 Protection des données personnelles

Conformément à la loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, l'université s'engage à :

- Traiter les données de messagerie dans le strict respect de leur finalité
- Ne collecter que les données nécessaires au fonctionnement du service
- Assurer la sécurité et la confidentialité des données

- Respecter les droits des utilisateurs (accès, rectification, suppression)
- Ne pas transférer les données vers des tiers sans consentement, sauf obligation légale

3.4 Accès administratif et traçabilité

L'université, par l'intermédiaire du Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC), peut accéder aux données de messagerie dans les cas suivants strictement encadrés :

- Maintenance technique et optimisation des infrastructures
- Sécurisation du système et prévention des incidents
- Investigation en cas d'incident de sécurité avéré
- Réquisition judiciaire ou administrative
- Nécessité de continuité de service en cas d'absence prolongée (avec autorisation hiérarchique)

Les utilisateurs sont informés que ces accès sont journalisés et traçables. Tout accès administratif doit être justifié et documenté.

3.5 Archivage et conservation des données

Les courriels peuvent être archivés selon les politiques de l'université :

- **Conservation opérationnelle** : Les messages sont conservés sur les serveurs actifs pendant la durée d'activité du compte
- **Archivage légal** : Certains messages à caractère administratif ou juridique peuvent être archivés conformément aux obligations légales
- **Durée de conservation** : Les données personnelles ne sont conservées que pendant la durée strictement nécessaire
- **Suppression sécurisée** : Les données supprimées sont effacées de manière sécurisée selon les procédures en vigueur

Les utilisateurs sont encouragés à :

- Classer et organiser leurs messages
- Supprimer régulièrement les messages obsolètes ou sans valeur administrative
- Archiver localement les messages importants avant la désactivation de leur compte

Article 4 : Responsabilités des Utilisateurs

4.1 Protection des identifiants et mots de passe

Chaque utilisateur est personnellement responsable de la sécurité de son compte :

- **Confidentialité absolue** : Ne jamais communiquer son mot de passe à quiconque, y compris au personnel informatique
- **Complexité des mots de passe** : Utiliser des mots de passe forts combinant lettres majuscules et minuscules, chiffres et caractères spéciaux (minimum 12 caractères recommandés)
- **Renouvellement régulier** : Changer son mot de passe au minimum tous les 6 mois, ou immédiatement en cas de suspicion de compromission

- **Unicité** : Ne pas réutiliser le même mot de passe pour d'autres services

4.2 Authentification renforcée

Les utilisateurs sont fortement encouragés à activer l'authentification à double facteur (2FA) lorsqu'elle est disponible, notamment pour :

- L'accès aux données sensibles
- Les comptes à privilèges élevés (responsables administratifs, enseignants-chercheurs)
- L'accès depuis l'extérieur du réseau universitaire

4.3 Signalement des incidents

En cas de suspicion de compromission du compte ou de tentative de fraude, l'utilisateur doit :

- Signaler immédiatement l'incident au CRSIC via l'adresse : **crsic@univ-boumerdes.dz**
- Changer immédiatement son mot de passe si l'accès au compte est encore possible
- Documenter les circonstances de l'incident (messages suspects reçus, comportements anormaux)
- Coopérer avec le CRSIC pour l'investigation et la résolution de l'incident

4.4 Responsabilité du contenu

Chaque utilisateur est juridiquement responsable du contenu des messages qu'il envoie depuis son compte institutionnel. Il doit s'assurer que :

- Les informations communiquées sont exactes et vérifiées
- Les pièces jointes transmises sont exemptes de virus
- Le ton et le contenu respectent les règles de courtoisie et de professionnalisme
- Les droits de propriété intellectuelle sont respectés (citations, références)

4.5 Gestion des absences

En cas d'absence prolongée, l'utilisateur doit :

- Configurer un message d'absence automatique indiquant la durée et une personne de contact alternative
- Prévoir une délégation de traitement des messages urgents si nécessaire (avec autorisation hiérarchique)
- Informer sa hiérarchie des dispositions prises

Article 5 : Bonnes Pratiques d'Utilisation

5.1 Gestion des destinataires

- **Destinataires principaux (À)** : Réserver aux personnes directement concernées par l'action attendue
- **Copie (Cc - Copie Carbone)** : Permet de placer un destinataire en copie d'un email. Celui-ci n'est pas le destinataire principal, mais peut être intéressé par le sujet ; il n'est pas attendu de lui une

réponse directe. Cette fonction permet à tous les destinataires de savoir qui est en réception du message

- **Copie cachée (Cci - Copie Carbone Invisible)** : Permet d'ajouter un ou plusieurs destinataire(s) caché(s) au message. À l'inverse du champ Cc, cette fonction permet d'envoyer un message à un grand nombre de destinataires sans que leurs identités et adresses emails ne soient visibles des autres destinataires. Cela est particulièrement utile pour protéger l'anonymat des correspondants
- **Répondre à tous** : Utiliser avec discernement pour éviter la surcharge des boîtes de réception
- **Vérification** : Toujours vérifier l'exactitude des adresses avant envoi, particulièrement pour les messages sensibles

Recommandation : Utiliser avec modération les fonctions Cc et Cci.

5.2 Rédaction des messages

5.2.1 Objet du message

Chaque email comporte impérativement un objet. L'objet du message doit être clair, concis et correspondre parfaitement au contenu du message. Il doit à la fois permettre au destinataire d'identifier immédiatement le sujet traité, et contenir des mots clés permettant de retrouver facilement l'email lors d'une recherche dans la messagerie électronique.

5.2.2 Corps du message

- **Structure** : Organiser le message en paragraphes courts et aérés
- **Ton professionnel** : Adopter un ton courtois et respectueux, même en cas de désaccord
- **Langue** : Privilégier le français ou l'arabe pour les communications institutionnelles, l'anglais pour les échanges internationaux
- **Relecture** : Relire systématiquement avant envoi pour corriger les erreurs et vérifier la clarté. L'utilisation de l'outil de correction orthographique peut s'avérer utile

5.2.3 Signature électronique

L'email doit se terminer par une signature mentionnant la fonction et les coordonnées de l'émetteur. Inclure une signature électronique complète (nom, fonction, coordonnées institutionnelles).

5.3 Gestion des pièces jointes

- **Taille limitée** : Limiter la taille des pièces jointes à **25 Mo** maximum par message
- **Fichiers volumineux** : Pour les fichiers supérieurs à 25 Mo, utiliser obligatoirement le Drive universitaire (15 Go de stockage disponible) ou les plateformes de partage sécurisé de l'université
- **Format** : Privilégier les formats standards et non propriétaires (PDF pour les documents finalisés)
- **Nommage** : Utiliser des noms de fichiers explicites et signifiants
- **Sécurité** : Analyser les pièces jointes avec un antivirus avant envoi
- **Compression** : Compresser les fichiers multiples ou volumineux (format ZIP) dans la mesure du possible
- **Données personnelles** : Ne jamais stocker de données à caractère personnel sur le Drive universitaire ; ce service est réservé exclusivement aux données liées aux activités universitaires, académiques, scientifiques et administratives

Important : Les pièces jointes doivent être, dans la mesure du possible, compressées à l'aide d'un logiciel dédié pour réduire leur taille.

5.4 Respect des horaires et de la qualité de vie au travail

- **Horaires d'envoi** : Privilégier les horaires de travail normaux (8h-17h) pour l'envoi de messages professionnels
- **Droit à la déconnexion** : Respecter le droit à la déconnexion en dehors des heures de travail ; un message envoyé le soir ou le week-end n'exige pas de réponse immédiate
- **Urgences réelles** : Réserver les mentions URGENT ou IMPORTANT aux situations réellement critiques
- **Délai de réponse** : Accepter qu'un délai de réponse raisonnable (24-48h ouvrées) soit la norme

5.5 Gestion des listes de diffusion

- **Usage modéré** : Limiter l'usage des listes de diffusion aux communications réellement nécessaires
- **Pertinence** : S'assurer que le message concerne effectivement tous les destinataires
- **Autorisation** : Respecter les règles d'utilisation des listes institutionnelles
- **Réponses groupées** : Éviter de répondre à l'ensemble d'une liste si la réponse ne concerne qu'une personne

5.6 Impact environnemental

Dans une démarche de responsabilité environnementale, les utilisateurs sont encouragés à :

- Limiter le nombre de destinataires au strict nécessaire
- Éviter l'envoi de pièces jointes volumineuses inutiles
- Supprimer régulièrement les messages obsolètes
- Vider périodiquement la corbeille et les spams
- Privilégier les plateformes collaboratives pour le partage de documents

Article 6 : Sécurité Informatique

6.1 Sensibilisation et formation

Le CRSIC organise régulièrement des sessions de sensibilisation et de formation portant sur :

- L'identification des tentatives de phishing et d'hameçonnage
- La détection des logiciels malveillants
- Les bonnes pratiques de sécurité informatique
- Les procédures de signalement des incidents
- Les évolutions technologiques et réglementaires

Tous les utilisateurs sont vivement encouragés à participer à ces formations.

6.2 Identification des menaces informatiques

Pour des raisons de sécurité et de confidentialité évidentes, l'utilisateur ne doit pas transférer ses fichiers professionnels sur sa messagerie personnelle. De plus, il ne faut pas oublier de se protéger contre les détournements de la messagerie.

- **Le SPAM** : email non sollicité, envoyé massivement et souvent de manière répétitive à des destinataires dont l'adresse électronique a été collectée sans leur consentement
- **Les VIRUS** : un email accompagné d'un ou plusieurs fichiers attachés présente une probabilité non négligeable que ces fichiers soient infectés. Cela est particulièrement le cas avec des fichiers exécutables (.exe), de fichiers de liaison (.pif). La vigilance des utilisateurs quant à la réception de ce type de fichiers est impérative
- **Le PHISHING (hameçonnage)** : tentative de récupération de données confidentielles basée sur la tromperie et le leurre, afin de les utiliser à des fins frauduleuses
- **Le HOAX (contenu malveillant)** : fausse information propagée spontanément par les internautes. En cas de doute, il est recommandé d'utiliser le site de référence hoaxbuster.com

6.3 Comportements de sécurité à adopter

Afin de préserver au mieux la sécurité informatique, les utilisateurs ont pour obligation d'adopter les comportements suivants :

- **Vérifier l'expéditeur** : Examiner attentivement l'adresse de l'expéditeur, même si le nom affiché semble familier
- **Méfiance face aux urgences** : Se méfier des messages créant un sentiment d'urgence ou de menace
- **Liens suspects** : Ne jamais cliquer sur des liens dans des messages non sollicités ; vérifier l'URL en survolant le lien
- **Pièces jointes douteuses** : Faire preuve d'une vigilance particulière vis-à-vis du format des pièces jointes avant leur ouverture. Ne jamais ouvrir les pièces jointes provenant d'expéditeurs inconnus ou suspects
- **En cas de doute** : En cas de doute sur la fiabilité de l'expéditeur d'un email, supprimer le message sans lire son contenu
- **Mot de passe sécurisé** : Définir un mot de passe correspondant aux critères élevés de sécurité (emploi de majuscules, chiffres et caractères spéciaux) et s'abstenir de le divulguer à un autre utilisateur ou à un tiers
- **Non-divulgation de données** : Ne jamais transférer ou publier, sous quelque forme que ce soit, des données confidentielles de l'université (documents de travail, etc.) sans l'autorisation préalable et expresse de sa hiérarchie
- **Signalement** : Signaler auprès du CRSIC toute tentative de fraude ou de violation de son compte de messagerie. Transférer immédiatement tout message suspect à **securite@univ-boumerdes.dz**

6.4 Protection des appareils

Les utilisateurs accédant à la messagerie depuis des appareils personnels ou professionnels doivent :

- Maintenir le système d'exploitation à jour avec les derniers correctifs de sécurité
- Installer et maintenir à jour un antivirus et un pare-feu
- Éviter l'accès depuis des ordinateurs publics ou partagés non sécurisés
- Verrouiller les appareils par un code ou mot de passe

- Activer le chiffrement des données sur les appareils mobiles
- Ne pas enregistrer les mots de passe dans les navigateurs sur les appareils partagés

6.5 Connexions sécurisées

- **Réseau universitaire** : Privilégier l'accès depuis le réseau sécurisé de l'université
- **VPN** : Utiliser obligatoirement le VPN institutionnel pour l'accès à distance depuis l'extérieur
- **WiFi public** : Éviter l'accès à la messagerie institutionnelle via des réseaux WiFi publics non sécurisés
- **HTTPS** : S'assurer que la connexion au webmail utilise le protocole HTTPS (cadenas dans la barre d'adresse)

6.6 Mesures d'urgence en cas de compromission

En cas de détection d'une compromission de compte, le CRSIC se réserve le droit de :

- Suspendre temporairement l'accès au compte compromis
- Réinitialiser le mot de passe
- Analyser les journaux de connexion et les messages suspects
- Alerter les destinataires de messages frauduleux envoyés depuis le compte
- Mettre en place des mesures de sécurité renforcées

L'utilisateur sera informé et devra coopérer pleinement pour la résolution de l'incident.

Article 7 : Continuité de Service et Support

7.1 Disponibilité du service

Le CRSIC s'engage à assurer la disponibilité optimale du service de messagerie :

- **Objectif de disponibilité** : 99% hors périodes de maintenance programmée
- **Maintenance** : Les interventions de maintenance seront annoncées au moins 48h à l'avance sauf urgence
- **Support technique** : Service d'assistance disponible pendant les horaires d'ouverture de l'université

7.2 Quota et limites

Pour garantir la qualité de service pour tous, les limites suivantes s'appliquent :

- **Espace de stockage messagerie** : Quota par défaut de **15 Go** par compte
- **Espace de stockage Drive** : Quota par défaut de **15 Go** par compte (réservé exclusivement aux données universitaires)
- **Taille des messages** : Maximum 25 Mo par message (pièces jointes incluses)
- **Envois groupés** : Limitation à 500 destinataires par message
- **Archivage** : Conservation des messages pendant la durée d'activité du compte

Important : Les utilisateurs sont seuls responsables de la sauvegarde de leurs données. Aucune récupération de données ne sera possible après la suppression du compte.

7.3 Contact et assistance

- **Support technique** : crsic@univ-boumerdes.dz
- **Sécurité informatique** : securite@univ-boumerdes.dz
- **Téléphone** : 024 79 58 87

Article 8 : Engagements et Sanctions

8.1 Engagements de l'université

L'université s'engage à :

- Fournir un accès au service de messagerie à toute personne remplissant les conditions définies dans cette charte
- Assurer la disponibilité optimale du service (objectif de 99% hors périodes de maintenance programmée)
- Garantir la sécurité et la confidentialité des données selon les moyens techniques à sa disposition
- Former et sensibiliser les utilisateurs aux bonnes pratiques de sécurité informatique
- Respecter la législation en vigueur en matière de protection des données personnelles

8.2 Engagements de l'utilisateur

L'utilisateur s'engage à :

- Prendre connaissance de la présente charte et respecter l'ensemble de ses dispositions
- Accepter explicitement les conditions d'utilisation lors de la première connexion
- Assurer la sécurité de son compte et ne pas apporter volontairement de perturbation au fonctionnement du service
- Être responsable de toutes les conséquences d'une mauvaise utilisation de son compte messagerie
- Sauvegarder régulièrement ses données importantes
- Se tenir informé des évolutions de la charte

8.3 Gradation des sanctions

Le non-respect des dispositions de la présente charte peut entraîner des sanctions graduées selon la gravité des manquements :

8.4 Premier niveau : Avertissement

En cas de manquement mineur ou d'utilisation inappropriée non intentionnelle :

- Avertissement écrit adressé à l'utilisateur
- Rappel des règles et bonnes pratiques
- Demande de régularisation immédiate

- Notification à la hiérarchie le cas échéant

8.5 Deuxième niveau : Suspension temporaire

En cas de récidive ou de manquement de gravité moyenne :

- Suspension temporaire de l'accès à la messagerie (durée proportionnelle à la gravité)
- Convocation pour entretien avec la hiérarchie et le CRSIC
- Trace au dossier administratif

8.6 Troisième niveau : Sanctions disciplinaires graves

En cas de manquement grave ou d'infractions répétées :

Tout utilisateur de compte messagerie de l'université ne respectant pas les règles et obligations définies dans la présente charte pourra donner lieu à :

- Suspension définitive de l'accès à la messagerie institutionnelle
- Saisine de la commission de discipline compétente
- Application du règlement intérieur de l'université
- Poursuites judiciaires si nécessaire (usurpation d'identité, diffamation, etc.)

8.7 Infractions graves

Constituent des infractions graves notamment :

- L'usurpation d'identité numérique
- La diffusion de contenus illicites ou diffamatoires
- Les tentatives d'intrusion ou de compromission des systèmes
- L'utilisation de la messagerie pour des activités illégales
- La divulgation d'informations confidentielles
- Le harcèlement via messagerie électronique

8.8 Procédure contradictoire

Toute sanction disciplinaire sera précédée d'une procédure contradictoire permettant à l'utilisateur :

- D'être informé des faits reprochés
- De présenter ses observations et sa défense
- D'être entendu par sa hiérarchie
- De recourir aux instances compétentes selon le règlement intérieur

Article 9 : Gestion du Cycle de Vie des Comptes

9.1 Attribution des comptes

L'Université M'hamed Bougara de Boumerdès (UMBB) met à disposition de chaque membre de l'établissement, quel que soit son statut (étudiant, doctorant, vacataire, enseignant, personnel administratif et technique), une adresse email nominative sous la forme : ***p*rénom.*nom*@univ-boumerdes.dz**

L'utilisateur bénéficie d'un accès au service de messagerie proposé par l'université après acceptation de la présente charte.

9.2 Création des comptes

Les comptes de messagerie sont créés selon les modalités suivantes :

- **Pour les personnels (ATS)** : Lors de la prise de fonction, création au niveau du CRSIC ou service réseau du rectorat
- **Pour les étudiants (Licence et Master)** : Création au niveau des facultés
- **Pour les doctorants** : Création au niveau du CRSIC ou service réseau du rectorat
- **Pour les enseignants permanents et vacataires** : Création au niveau du CRSIC ou service réseau du rectorat, nécessitant une attestation de travail de l'année actuelle
- **Pour les partenaires** : Sur demande motivée avec durée limitée

Tous les formulaires de demande de création de compte email ou de réinitialisation de mot de passe se trouvent sur le site web de l'UMBB (CRSIC).

9.3 Identifiants et accès

- Le moyen d'accès au service de messagerie institutionnelle, mis à disposition de l'utilisateur, est constitué d'un identifiant et d'un mot de passe strictement personnels, confidentiels et incessibles
- Dans le cas de perte de ses codes d'accès, l'utilisateur peut récupérer l'accès aux services de messagerie en prenant contact avec le CRSIC ou en suivant les procédures de récupération disponibles sur le portail de l'université

9.4 Désactivation et suppression

Les comptes sont désactivés puis supprimés selon les règles suivantes :

- **Étudiants diplômés (Licence, Master 2)** : Suppression automatique **sans préavis** après la soutenance pour les étudiants qui ne poursuivent pas d'études supérieures (Master, Doctorat). Les utilisateurs sont **seuls responsables** de la sauvegarde de leurs données avant la soutenance.
- **Étudiants poursuivant des études** : Maintien du compte actif durant la continuité pédagogique (passage Licence → Master, Master → Doctorat)
- **Personnels** : Désactivation à la date de départ (mutation, radiation, décès), suppression après **3 mois.**
- **Partenaires** : Désactivation à l'échéance prévue, suppression après **3 mois**

9.5 Responsabilité de sauvegarde des données

IMPORTANT : Les utilisateurs sont **seuls responsables** de la sauvegarde de leurs données.

- Le propriétaire du compte est responsable de toutes les conséquences d'une mauvaise utilisation de son compte messagerie
- Aucune récupération de données ne sera possible après la suppression du compte

- Aucun préavis ne sera envoyé pour la suppression des comptes étudiants après soutenance
- Le CRSIC ne procède à aucune sauvegarde ou archivage des données personnelles des utilisateurs
- Il est fortement recommandé d'effectuer régulièrement des sauvegardes locales de vos messages, contacts et fichiers importants
- Pour les étudiants en fin de cursus : **sauvegarder impérativement toutes les données avant la soutenance**
- L'utilisateur s'engage à ne pas apporter volontairement de perturbation au fonctionnement du service

Article 10 : Évolution et Révision de la Charte

10.1 Révision périodique

Cette charte fait l'objet d'une révision périodique au minimum tous les 2 ans, ou plus fréquemment en cas de :

- Évolution significative de la réglementation
- Changements technologiques majeurs
- Incidents de sécurité nécessitant une adaptation des règles
- Retours d'expérience des utilisateurs

10.2 Communication des modifications

Toute modification substantielle de la charte sera communiquée aux utilisateurs par :

- Publication sur le site web de l'université
- Notification par courrier électronique
- Affichage dans les espaces institutionnels
- Information lors des réunions des instances universitaires

10.3 Engagement de conformité

Chaque utilisateur s'engage à :

- Prendre connaissance de la présente charte
- Respecter l'ensemble de ses dispositions
- Se tenir informé de ses évolutions
- Accepter explicitement les conditions d'utilisation lors de la première connexion

Article 11 : Validation et Mise en Application

11.1 Autorités compétentes

La présente charte est :

- Élaborée par le Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC)

- Validée par le Conseil de Direction de l'Université M'hamed Bougara de Boumerdes
- Applicable à compter du **1er janvier 2025**

11.2 Diffusion

Cette charte est :

- Accessible depuis le site web institutionnel de l'université
- Affichée dans les services concernés

11.3 Responsables de la mise en œuvre

- **Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC)** : Responsable technique et opérationnel
- **Sous-direction des Personnels et de la Formation** : Application des sanctions pour les personnels
- **Vice-Rectorat chargé de la Pédagogie** : Application pour les étudiants
- **Secrétariat Général** : Coordination générale et arbitrage

---

Annexe : Glossaire

Messagerie institutionnelle : Service de courrier électronique fourni par l'université sous le domaine @univ-boumerdes.dz

Phishing (hameçonnage) : Technique frauduleuse visant à obtenir des informations confidentielles en se faisant passer pour un tiers de confiance

Double authentification (2FA) : Méthode de sécurité nécessitant deux preuves d'identité distinctes pour accéder à un compte

VPN (Virtual Private Network) : Réseau privé virtuel permettant une connexion sécurisée à distance

HTTPS : Protocole de communication sécurisé utilisant le chiffrement SSL/TLS

Malware : Logiciel malveillant conçu pour endommager ou infiltrer un système

Quota : Espace de stockage alloué à chaque compte de messagerie

CRSIC : Centre des Réseaux et des Systèmes d'Information et de Communication

Drive universitaire : Service de stockage et de partage de fichiers en ligne institutionnel (quota de 15 Go)

IMAP/POP/SMTP : Protocoles standards de messagerie permettant l'accès aux emails via différents clients de messagerie

SPAM : Email non sollicité, envoyé massivement et souvent de manière répétitive

HOAX : Fausse information ou canular propagé spontanément par les internautes

RGPD : Règlement Général sur la Protection des Données (applicable en Europe, inspirant les bonnes pratiques internationales)

ATS : Personnel Administratif, Technique et de Service

Contacts Utiles

Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC)
Université M'hamed Bougara de Boumerdes
Avenue de l'Indépendance, 35000 Boumerdes

Support technique : crsic@univ-boumerdes.dz
Sécurité informatique : securite@univ-boumerdes.dz
Site web : www.univ-boumerdes.dz

Document élaboré par le Centre des Réseaux et des Systèmes d'Information et de Communication (CRSIC)
Université M'hamed Bougara de Boumerdes
Janvier 2025