المملكة المغربية
ⵜⴰⴳⵍⴷⵉⵜ ⵏ ⵍⵎⵖⵔⵉⴱ
ROYAUME DU MAROC

المجلس الأعلى للتربية والتكوين والبحث العلمي
ⴰⵙⴳⵎⵉⵍ ⴰⵡⴰⵍⵏ ⵏ ⵜⵙⴳⵎⵉⵔⵜ ⴷ ⵜⵙⵡⵉⵔⵉ ⴷ ⵜⵙⵙⵏⵙⵉ ⴰⵎⴰⵡⴰⵏ
Conseil Supérieur de l'Education, de la Formation et de la Recherche Scientifique

CHARTE DU BON USAGE

DU SYSTÈME D'INFORMATION, DES MOYENS NUMÉRIQUES ET AUDIOVISUELS

PRESENTE PAR	VALIDE PAR	APPROUVER PAR
PÔLE SYSTEMES D'INFORMATION	SECRETARIAT GENERAL	PRESIDENCE
SIGNATURE : Abdellatif ATMANI Directeur du pôle Systèmes d'Information	SIGNATURE : Aziz KAICHOUH Secrétaire Général Conseil Supérieur de l'Education, de la Formation et de la Recherche Scientifique	SIGNATURE : Rahma BOU-REQIA Présidente du Conseil Supérieur de l'Education de la Formation et de la Recherche Scientifique
DATE : 31 JUIL. 2025	DATE : 31 JUIL. 2025	DATE : 03 SEP. 2025

ELABORE PAR	V1	PÔLE SYSTEMES D'INFORMATION	Septembre 2016
	V2	PÔLE SYSTEMES D'INFORMATION	Décembre 2024
	V3	PÔLE SYSTEMES D'INFORMATION	Juillet 2025
DESTINATAIRES	MEMBRES ET PERSONNEL DU CONSEIL		
DATE DE MISE EN APPLICATION	A LA DATE D'APPROBATION PAR LA PRESIDENTE		
NOMBRE DE PAGES	09		
NOMBRE D'ANNEXES	01		

PRÉAMBULE

Le Conseil met à la disposition de ses utilisateurs un ensemble de ressources essentielles à l'exercice de leurs missions, attributions et prérogatives. Ces ressources englobent le système d'information, les moyens informatiques et numériques, ainsi que les dispositifs audiovisuels. La présente Charte a pour objectif d'encadrer les modalités d'usage de ces composantes, des données et des informations traitées, en précisant les systèmes et moyens fournis par l'administration, garante du respect de la législation et de la réglementation en vigueur, et de la sécurité des systèmes d'information.

Elle vise également à définir les règles que doivent respecter les utilisateurs et les administrateurs de ces systèmes et moyens. Plus spécifiquement, cette Charte a pour but de :

- ✓ Définir les conditions d'accès et les règles d'utilisation des systèmes d'information, des moyens informatiques, numériques et audiovisuels du Conseil.
- ✓ Sensibiliser les utilisateurs aux risques inhérents à l'utilisation de ces systèmes et moyens, notamment en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité des données et des informations traitées.
- ✓ Préciser les règles relatives à l'enregistrement audiovisuel des réunions et activités, ainsi que les conditions de leur archivage, de leur consultation et de la participation à distance.

Cette charte s'applique à l'ensemble des membres du Conseil et à son personnel, ainsi qu'à toute personne utilisant les ressources du Conseil.

ARTICLE 1. RÉFÉRENCES LÉGISLATIVES ET RÉGLEMENTAIRES

L'utilisateur est tenu de respecter les dispositions légales et réglementaires qui régissent ses activités au sein et en dehors du Conseil, dès lors qu'il utilise les moyens mis à sa disposition. Ces références incluent, sans s'y limiter :

- ✓ **Loi n° 05-20** relative à la cybersécurité, promulguée par le Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020).
- ✓ **Loi n° 07-03,** promulguée par le Dahir n°1-03-197 du 11/11/03, complétant le Code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données (articles 607-3 et suivants).
- ✓ **Loi 43-20** relative aux services de confiance pour les transactions électroniques.
- ✓ **Loi N° 09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- ✓ **Dahir n° 1-00-20** du 9 kaada 1420 (15 février 2000) portant promulgation de la Loi n° 2-00 relative aux droits d'auteur et droits voisins (articles 11 à 22).
- ✓ La **Directive nationale de la sécurité des systèmes d'information (DNSSI)** de la DGSSI.

Toute autre loi ou réglementation applicable en matière de protection des données, de propriété intellectuelle et de sécurité des systèmes d'information.

ARTICLE 2. DÉFINITIONS

Pour la bonne compréhension de la présente Charte, les termes suivants sont définis comme suit :

- ✓ **Système d'Information (SI) :** Ensemble des ressources matérielles, logicielles, applications, bases de données, réseaux et moyens de sécurité mis à disposition par le Conseil pour l'exercice de ses missions.
- ✓ **Utilisateur :** Toute personne ayant accès au SI du Conseil ou utilisant les moyens informatiques, numériques ou audiovisuels du Conseil, ou qui traite des données du Conseil, quel que soit son statut (membre, personnel, stagiaire, intérimaire) et quel que soit son lieu ou mode de travail (sur site, à distance).
- ✓ **Pôle des Systèmes d'Information (PSI) :** Entité du Conseil en charge du développement, de la gestion et de la sécurité du système d'information, incluant les moyens informatiques, numériques et audiovisuels.
- ✓ **Administrateur :** Membre de l'équipe du PSI qui s'occupe d'administrer une ou plusieurs composantes

du système d'information.

- ✓ **Traitements de données** : Opérations informatisées ou non portant sur des données telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.
- ✓ **Données concernées** : Données traitées par le système d'information du Conseil, y compris celles disponibles sur les matériels mobiles (PC, tablettes, téléphones, disques amovibles, etc.), qu'il s'agisse de données produites par les partenaires du Conseil, par les entités métier ou de gestion du Conseil, ou transitant sur un dispositif d'information du Conseil (mail, échange et partage de fichiers, etc.). Sont également comprises les données qui sortent du système d'information, quel qu'en soit le lieu d'hébergement.
- ✓ **Usages concernés** : La présente Charte s'applique à tous les types d'usage des composantes du système d'information, des moyens et des ressources informatiques, numériques et audiovisuels, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu dans les locaux du Conseil, dans le cadre d'un usage « nomade » ou dans le cadre d'un accès distant.
- ✓ **Information professionnelle** : Données ou informations utilisées dans un contexte de travail.
- ✓ **Donnée à caractère personnel** : Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (nom, adresse postale et électronique, IP, identifiants de connexion, numéro de téléphone, photographie, voix, données de localisation).
- ✓ **Enregistrement audiovisuel** : Capture et conservation de flux audio, vidéo ou combinés (audiovisuels) de réunions, activités ou événements, à des fins de documentation, d'archivage ou de communication.
- ✓ **Instances du Conseil** : Assemblée générale, Bureau du Conseil, Commissions permanentes, commissions adhoc, groupes de travail.

ARTICLE 3. DOMAINE D'APPLICATION DE LA CHARTE

Sauf mention contraire, les règles décrites dans la présente Charte s'appliquent à toute personne qui utilise le système d'information, les moyens informatiques, numériques et audiovisuels du Conseil. Cela inclut, sans s'y limiter, les membres du Conseil, le personnel permanent, les stagiaires et les intérimaires.

Les utilisateurs sont tenus de s'assurer que toute personne à laquelle ils permettraient d'accéder au système d'information et aux ressources du Conseil accepte et respecte les règles énoncées dans la présente Charte.

ARTICLE 4. ENGAGEMENTS

4.1. Engagements du Conseil

Le Conseil s'engage à :

- ✓ Assurer la disponibilité, l'intégrité et la confidentialité de ses données et de son système d'information. À cette fin, il définit les règles d'usage qu'il porte à la connaissance de l'utilisateur par la présente Charte.
- ✓ Mettre en œuvre toutes les mesures nécessaires pour garantir la sécurité du système d'information et la protection des utilisateurs.
- ✓ Faciliter l'accès des utilisateurs aux ressources du système d'information, des moyens numériques et audiovisuels dont l'usage est nécessaire à l'exercice de leurs activités et fonctions. Les ressources mises à leur disposition sont principalement à usage professionnel.

4.2. Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait des ressources du système d'information, des moyens numériques et audiovisuels auxquelles il a accès. Il a une obligation de réserve, de discrétion et de confidentialité à l'égard des données, informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut au Conseil et à

la réglementation en vigueur.

ARTICLE 5. CONDITIONS D'ACCÈS ET D'UTILISATION DES RESSOURCES NUMÉRIQUES ET AUDIOVISUELLES

5.1. Droits d'accès au Système d'Information à usage professionnel

- ✓ Le droit d'accès au système d'information est temporaire, personnel et incessible. Il est attribué individuellement à l'utilisateur, normalement enregistré auprès du PSI selon la procédure d'ouverture d'un compte nominatif en vigueur au Conseil.
- ✓ Ce droit d'accès est accordé exclusivement pour les activités professionnelles des utilisateurs. Il prend fin en cas de départ de l'utilisateur du Conseil (fin de contrat ou d'activité) ou si le comportement de l'utilisateur est contraire aux règles énoncées par la présente Charte.
- ✓ Lors de l'ouverture du compte, l'utilisateur reçoit un ou plusieurs identifiants de connexion (nom d'utilisateur et mot de passe) qui peuvent lui donner accès, en fonction des besoins de son activité, à :
    - Au moins un poste de travail ;
    - Aux serveurs du Conseil et aux services et applications qu'ils hébergent ;
    - Aux données collectées auprès des partenaires et/ou données produites en interne ;
    - À une adresse de messagerie professionnelle ;
    - Au réseau interne ;
    - À l'internet et aux ressources numériques et audiovisuelles du Conseil.

5.2. Règles Générales d'Utilisation des Ressources du Système d'Information

- ✓ Les utilisateurs sont responsables, en tout lieu, de l'usage qu'ils font du système d'information du Conseil. Ils sont tenus à une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels ils accèdent.
- ✓ L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles. Les utilisateurs utiliseront uniquement des identifiants personnalisés. Le partage d'identifiant, même temporairement, n'est pas autorisé. En cas de besoin, des identifiants supplémentaires pourront être demandés. Les comptes génériques anonymes ne sont pas autorisés, même pour les stagiaires qui devront se voir ouvrir des comptes nominatifs.
- ✓ L'utilisateur protégera son compte par la technologie fournie (mot de passe, double authentification, certificat, etc.). Il devra respecter les règles de sécurité préconisées par le Conseil concernant le choix des mots de passe ainsi que les modalités d'utilisation des méthodes d'authentification.
- ✓ L'utilisateur est averti des nombreuses tentatives d'escroquerie visant à lui subtiliser ses identifiants (hameçonnage). Il ne devra jamais communiquer ses identifiants (mots de passe, certificats, etc.), en particulier en réponse à des courriers électroniques, suspects ou non, ou à des demandes téléphoniques. Il prendra les mesures préconisées par le Conseil pour éviter une communication involontaire. Si, par exemple pour un dépannage, il devait communiquer un identifiant, cela se fera de préférence en présence physique de la personne, et dans tous les cas, celle-ci devra être parfaitement identifiée (par exemple, par une confirmation visuelle ou téléphonique).
- ✓ En cas d'usage inapproprié au regard de la présente Charte, l'utilisateur peut se voir suspendre ou retirer tout ou partie des moyens informatiques et numériques mis à sa disposition et peut se voir restreindre ses droits d'accès au système d'information du Conseil. Il pourra également faire l'objet d'une procédure disciplinaire.
- ✓ L'utilisation des moyens informatiques et numériques du Conseil, ou simplement de l'adresse de messagerie, respecte le principe de neutralité et le devoir de réserve et de discrétion professionnelle.
- ✓ Les utilisateurs doivent impérativement utiliser les canaux institutionnels fournis par le Conseil, notamment les adresses mail. Cela garantit une gestion rigoureuse et sécurisée des échanges de documents de travail, assure la traçabilité et prévient toute fuite d'information.

5.3. Respect de la Vie en Collectivité et Consommation des Ressources

- ✓ L'utilisateur ne doit à aucun moment oublier qu'il vit et travaille au sein d'une communauté. Il s'interdit toute utilisation abusive d'une ressource commune (imprimante, réseau, espace disque, processeur,

accès Internet, licences flottantes, etc.) et veille à faire un usage sobre et raisonné des ressources.

- ✓ Les activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau comme la consultation de contenu audio ou vidéo en temps réel, le téléchargement de fichiers nombreux ou volumineux, etc.) devront être effectuées sur les équipements dédiés à ces activités et en accord, selon les situations, avec les responsables ad hoc du PSI.
- ✓ L'utilisateur s'exprimant au travers des moyens informatiques mis à sa disposition, en particulier sur des supports externes, devra le faire avec le respect du devoir de réserve et des règles de savoir-vivre, son expression engageante directement ou indirectement le Conseil.
- ✓ Les responsables du PSI se réservent le droit de bloquer, en conformité avec les dispositions législatives et réglementaires et de la jurisprudence, l'accès à des sites ou à des services n'ayant aucun rapport avec l'exercice professionnel ou perturbant le bon fonctionnement du système d'information du Conseil.
- ✓ L'utilisateur s'interdit de perturber volontairement tout autre utilisateur du système d'information, de masquer sa véritable identité ou de s'approprier le mot de passe d'un autre utilisateur.

5.4. Utilisation des moyens audiovisuels et participation à distance

5.4.1. Réunions et activités soumises à enregistrement :

- ✓ Les réunions des instances du Conseil sont enregistrées à des fins de sauvegarde du patrimoine informationnel du Conseil et d'archivage de l'historique de ses activités.
- ✓ Les événements et activités organisés par le Conseil (Colloques, conférences, journées d'étude, auditions, ateliers, focus groupe, ...) sont enregistrées à des fins de transcription, de documentation et d'archivage du patrimoine informationnel du Conseil.

5.4.2. Accès aux réunions à distance

L'accès à distance aux réunions ou activités des instances du Conseil, qu'elles soient organisées intégralement en ligne ou en mode hybride (présentiel & distantiel), est strictement réservé aux participants dûment invités par l'organisateur de la réunion ou de l'activité, via un lien d'accès dédié.

Chaque participant à distance doit se connecter :

- ✓ Soit avec son adresse institutionnelle (@csefrs.ma), permettant un accès automatique à la réunion.
- ✓ Soit par un compte personnel, auquel cas le participant sera mis en attente et accepté dans la réunion après vérification de son identité.

L'usage de pseudonymes ou d'identifiants anonymes est interdit, sauf autorisation explicite de l'organisateur de la réunion lors de la validation en salle d'attente.

5.4.3. Assistance Technique et Sécurité

Le Conseil met en place un dispositif d'assistance technique pour assurer la qualité des connexions et résoudre les incidents pendant les réunions distancielles ou hybrides. Un protocole de sécurité est appliqué selon la sensibilité de la réunion, incluant l'utilisation d'un mot de passe d'accès, une salle d'attente virtuelle et/ou une authentification à double facteur.

ARTICLE 6. ACCÈS AUX DONNÉES ET CONFIDENTIALITÉ

6.1. Protection des données Professionnelles

L'accès aux informations conservées ou circulant dans le système d'information doit être limité aux données propres à l'utilisateur et aux données publiques. Il est formellement interdit de copier, de prendre connaissance ou d'intercepter des informations détenues ou échangées par d'autres utilisateurs sans leur autorisation explicite, même si ces informations n'ont pas été explicitement protégées. Cette règle s'applique également aux échanges de type messagerie électronique ou conversation directe dont l'utilisateur n'est destinataire ni directement, ni en copie.

Les données professionnelles, en particulier les données descriptives du SEFRS, les données de gestion, les

A C

versions intermédiaires de rapports, les logiciels, les bases et les résultats de traitements, etc., sont considérées comme bénéficiant d'un classement « Confidentiel Conseil » et doivent être traitées en conséquence.

6.2. Protection des données à caractère Personnel

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 notamment par la Loi n°09-08. Le Conseil s'engage à assurer la conformité de ses processus de traitement de données à caractère personnel auprès de la CNDP.

Les utilisateurs devront informer le Secrétariat Général, préalablement à leurs besoins de ce type de traitement, afin d'enclencher la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.

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 lors de 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 adaptées 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.

Par conséquent, tout utilisateur est tenu d'assurer la protection des données à caractère personnel qu'il traite dans le cadre de ses fonctions, notamment en :

- ✓ Protégeant les codes d'accès aux applications et systèmes d'information qu'il utilise ;
- ✓ Ne conservant pas ces données au-delà de la durée nécessaire au traitement auquel elles sont destinées ;
- ✓ Informant immédiatement sa hiérarchie et le Secrétariat Général si toute personne utilisatrice des outils informatiques, services numériques et des moyens de communication constatait un défaut dans la protection de données à caractère personnel ;
- ✓ Sécurisant la communication de données à caractère personnel, afin que la confidentialité, l'intégrité et l'authenticité des informations soient assurées.

ARTICLE 7. SÉCURITÉ DU SYSTÈME D'INFORMATION ET DES MOYENS NUMÉRIQUES ET AUDIOVISUELS

7.1. Préservation de l'intégrité des données et des informations

- ✓ Il est rappelé que les données de travail appartiennent au Conseil, l'utilisateur doit être attentif à les protéger et ne pas les divulguer sans le consentement explicite du Conseil. En particulier en cas d'export de ces données à l'extérieur, l'utilisateur doit examiner avec précaution les contrats d'hébergement, surtout gratuits, pour ne pas céder les données à des tiers non consentis (cas de la plupart des fournisseurs de volumes de stockages gratuits). Dans tous les cas l'utilisateur devra avoir le consentement du Conseil.
- ✓ Si l'utilisateur est amené à traiter des données du SEFRS agrégées ou détaillées mises à sa disposition par le PSI, ou des données collectées dans le cadre d'un projet de son entité, les résultats des traitements effectués sur ces données doivent être mis à la disposition du PSI, sous formats exploitables, pour conservation, réutilisation ultérieure et archivage.
- ✓ L'utilisateur s'engage à ne pas modifier ou détruire d'autres fichiers ou flots d'information que ceux qui lui appartiennent en propre, sauf accord de leur propriétaire.

A C

- ✓ L'utilisateur a la responsabilité d'archivage des documents qu'il possède.
- ✓ Le PSI du Conseil exploite différents systèmes de sauvegarde des données des utilisateurs, dans le cadre d'un engagement de moyens. L'utilisateur pourra demander la restauration de ces données en fonction de la durée de rétention prévue dans la politique de sauvegarde.
- ✓ À son départ du Conseil, l'utilisateur transférera ses données professionnelles au PSI en accord avec son responsable et fera son affaire de l'archivage et de l'effacement de ses données personnelles. L'utilisateur ne pourra se prévaloir d'un quelconque dommage en cas d'usage ultérieur ou d'effacement de ses données professionnelles ou en cas d'accès à ses données personnelles ou d'effacement de celles-ci.

7.2 Préservation de l'intégrité des moyens informatiques et numérique :

- ✓ L'utilisateur est responsable de l'utilisation qu'il fait de son poste de travail.
- ✓ L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, etc. Le PSI se réserve le droit de désinstaller tout logiciel perturbant le bon fonctionnement du poste de travail.
- ✓ L'utilisateur doit suivre les consignes de sécurité applicables au sein du Conseil, notamment en matière d'accès et d'anti-virus.
- ✓ L'utilisateur s'engage à ne pas désactiver les logiciels installés par le PSI concernant notamment la mise à jour de l'anti-virus, les mises à jour de sécurité du système d'exploitation, l'outil de gestion du parc, les outils de sauvegarde automatique.
- ✓ Le PSI ne demandera jamais la transmission des identifiants de connexion de l'utilisateur.
- ✓ Il est rappelé que les administrateurs peuvent accéder aux postes de travail et données des utilisateurs, en présence des utilisateurs, pour des besoins de diagnostic, de sécurité, d'installation de correctif, etc. (ex. : mises à jour ou installation de correctifs, suppression de fichier infecté, y compris si celui-ci est de nature privée).
- ✓ Il est rappelé que les administrateurs sont aussi autorisés à effectuer des vérifications des moyens d'authentification sur les ressources, afin de tester régulièrement, par exemple, la robustesse des mots de passe choisis par les utilisateurs, et ainsi les inciter à en améliorer la sécurité.
- ✓ Si un utilisateur est amené à se servir du système d'information du Conseil depuis l'extérieur, il ne peut le faire qu'en se conformant strictement aux procédures et en utilisant exclusivement l'outillage ad hoc mis à sa disposition (VPN). Il doit respecter les dispositions de la présente Charte et appliquer les recommandations du PSI.
- ✓ La connexion au réseau informatique de nouvelles machines (postes de travail, périphériques, imprimantes, photocopieuses, dispositifs de visioconférence), le déplacement et/ou la modification de la connexion de machines existantes, la déconnexion de machines réformées, l'ajout de commutateurs, de bornes wifi, de modems ou de services aux réseaux, ne pourront être faits que par le PSI.
- ✓ L'utilisateur doit se connecter régulièrement au réseau du Conseil pour s'assurer de la bonne mise à jour de la solution antivirus et de l'application des correctifs de sécurité.
- ✓ Les postes de travail portables, doivent être redémarrés régulièrement, en particulier après l'installation de correctifs de sécurité.
- ✓ L'installation de nouveaux logiciels, ou la modification de logiciels existants, ayant un impact sur des programmes ou des bibliothèques utilisées par la communauté des usagers, ne pourra être faite que par l'administrateur du parc informatique du Conseil.

7.5. Préservation des enregistrements audiovisuels

Le Pôle du Système d'Information (PSI) est l'entité chargée de la réalisation, de la sauvegarde et de la sécurité des enregistrements audiovisuels des réunions et des activités des instances du Conseil. Des mesures rigoureuses sont mises en œuvre pour garantir l'intégrité et l'authenticité des enregistrements :

- ✓ Les personnes du PSI, responsables des enregistrements, veillent à ce que les mesures appropriées soient prises pour que les enregistrements du Conseil soient authentiques et pour empêcher toute altération.
- ✓ L'archive des enregistrements est stockée dans une baie dédiée à cet effet, dans le data center interne du Conseil, avec une politique de sauvegarde et de rétention conforme aux normes et réglementations en vigueur.
- ✓ Les baies de stockage des archives audiovisuelles du Conseil sont sécurisées derrière une plateforme de sécurité périmétrique, permettant d'empêcher toute tentative d'intrusion interne ou externe.

ARTICLE 8 : TRAÇABILITÉ

- ✓ L'utilisateur est informé que différents dispositifs du système informatique, liés aux obligations légales, à la gestion de la sécurité et de la qualité de service et à la recherche des pannes et incidents, enregistrent des événements.
  Par conséquent des outils de traçabilité sont mis en place sur tous les systèmes d'information.
- ✓ Ces enregistrements peuvent donner lieu à des analyses systématiques de volumétrie ou de détection de comportements anormaux. Ils peuvent à l'occasion être utilisés pour identifier des utilisations manifestement abusives au sens des différentes clauses de cette Charte.
- ✓ L'utilisateur est informé que les mécanismes de sauvegarde peuvent garder trace d'activités le concernant ou de fichiers qu'il a par ailleurs décidé de supprimer, et ce pendant la durée de rétention maximale des différents supports de sauvegarde.

ARTICLE 9 : ANOMALIES, ANALYSE ET CONTROLE DE L'UTILISATION DU SI

9.1 Anomalies

Lorsque des anomalies mettant en cause le bon fonctionnement ou la sécurité du système d'information sont relevées, ou lorsqu'elles révèlent une méconnaissance des droits de la propriété intellectuelle, ces anomalies sont signifiées à l'utilisateur par les voies appropriées et sont éliminées avec son accord. En cas de désaccord, le problème est remonté au niveau du responsable dont dépend l'utilisateur et au PSI du Conseil. En cas d'urgence, le PSI peut se passer d'un accord préalable.

9.2 Maintenance, analyse et contrôle

- ✓ Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau, peuvent être analysés et contrôlés dans le respect de le législation applicable et notamment de la Loi 05.20 et la DNSSI ;
- ✓ Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

9.3 Responsabilités et droits d'administration

L'administration des postes de travail est de la responsabilité du PSI. Dans le cas où un utilisateur dispose des droits d'administration de son poste de travail, il est tenu :

- ✓ De réserver l'utilisation de la connexion comme administrateur aux tâches qui le nécessitent et de travailler habituellement avec un profil simple utilisateur ;
- ✓ De se conformer aux consignes d'administration énoncées ;
- ✓ D'appliquer les dispositions de la présente Charte ;

- ✓ De respecter les contrats signés avec les fournisseurs de logiciels, ainsi que leurs closes particulières en matière de copie et d'usage.

ARTICLE 10 : MISE EN GARDE - LIMITATION DES USAGES

- ✓ L'utilisateur est tenu de respecter l'ensemble des règles définies dans la présente Charte, ainsi que les textes de référence applicables rappelés dans le présent document.
- ✓ Tout manquement à ces règles et mesures de sécurité et de confidentialité est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des sanctions disciplinaires et pénales en fonction de la gravité des faits constatés par les instances compétentes. Le Conseil, via le PSI, se réserve le droit de restreindre ou de suspendre, sans préavis, son accès au système d'information ou son accès à l'Internet, de lui supprimer les droits d'administrateur de son poste de travail, d'installer sur son poste de travail un logiciel de supervision et de prendre toute autre mesure qu'il jugera nécessaire.
- ✓ Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est également passible de sanctions.
- ✓ Le transfert de données via un support externe (clef USB, disque externe, ...) depuis un poste de travail hors de contrôle du Conseil, peut amener à une contamination par un virus. Cette opération devra se faire avec prudence, par exemple avec une analyse préalable du support externe par l'antivirus du poste destinataire. En cas de doute, l'utilisateur est tenu de contacter le représentant du PSI.
- ✓ L'utilisateur est informé de la présence de systèmes automatiques de filtrage, aussi bien sur le réseau que sur les serveurs et postes de travail. Ces dispositifs, comme les anti-virus, visent à maintenir en sécurité le système d'information. Occasionnellement ils peuvent filtrer des données légitimes, le Conseil ne pourra en être tenu responsable. Dans ce cas, une information sera délivrée pour éveiller la vigilance des utilisateurs.
- ✓ Tout traitement de données à caractère personnel, y compris la simple collecte, doit être analysé, étudié et répertorié dans le registre des traitements, maintenu au Secrétariat Général, conformément aux dispositions législatives et réglementaires en vigueur.
- ✓ Lors de la réforme du matériel de stockage informatique (disques dur, clef USB, ...) les données stockées devront être détruites de manière sûre (destruction physique des supports, ...) suivant les préconisations de la Directive nationale de sécurité des systèmes d'information (DNSSI) en vigueur.
- ✓ L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale du Conseil et/ou de l'utilisateur.
- ✓ L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à la hiérarchie supérieure.
- ✓ La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel.
- ✓ Enfin, les messages électroniques sont conservés sur les serveurs du Conseil et sont automatiquement archivés.

ANNEXE

DESCRIPTION DES COMPOSANTES DU SYSTEME D'INFORMATION ET DES MOYENS INFORMATIQUES, NUMERIQUES ET AUDIOVISUELLES DU CONSEIL

1. SYSTEME D'INFORMATION :

Le système d'information du Conseil est constitué, notamment, des composantes suivantes : gestion :

- ✓ Bases de données descriptives du SEFRS (scolarité, appui social, ressources humaines, résultats, ...) ;
- ✓ Base de données résultantes des enquêtes, sondage et tests réalisées par les instances et entités du Conseil ;
- ✓ Portail des recueils statistiques officielles du SEFRS ;
- ✓ Système d'information de gestion du Conseil (RH, comptabilité, stock, patrimoine,)
- ✓ Système d'information de gestion documentaire du Conseil ;
- ✓ Système de collaboration et de gestion de documents ;
- ✓ Système de communication internes et externes du Conseil (site web, majliscom, emajlis, ...)
- ✓ Système de gestion et de conservation des enregistrements audiovisuels du Conseil
- ✓ Plateforme de conservation des documents du Conseil
- ✓ Plateforme de gestion des enquêtes sur le web.

L'accès aux composantes du système d'information et aux bases de données est octroyé aux utilisateurs, selon les habilitations nécessaires, en fonction de leur activité et besoins.

2. SYSTEME INFORMATIQUE & NUMERIQUE : MOYENS ET SERVICES

Les moyens informatique et numériques du Conseil mis à disposition des utilisateurs consistent en :

a) Les moyens informatiques matériels :

- ✓ Les postes de travail Fixe & portable et postes téléphoniques ;
- ✓ Les imprimantes, photocopieurs et scanners, etc. ;
- ✓ Les équipements nomades (tablette, téléphone portable, disque amovible, appareil photo, ...) ;
- ✓ Les équipements réseau (switch, point d'accès wifi, modem, routeur, ...) ;
- ✓ Les équipements audiovisuels (vidéo projecteur, tableau interactif, ...) ;
- ✓ La plateforme de téléphonie sur IP ;
- ✓ Les serveurs et les baies de stockage.

b) Les moyens informatiques logiciels :

- ✓ Systèmes d'exploitation ;
- ✓ La plateforme de sécurité poste de travail (Antivirus, ...) ;
- ✓ Les outils bureautiques (Suite Microsoft Office) ;
- ✓ Les logiciels de traitement graphique ;

c) Les services informatiques et de sécurité :

- ✓ L'accès à Internet ;
- ✓ La messagerie électronique ;
- ✓ La plateforme de sécurité périmétrique du réseau (antivirus, antispam, Firewall, ...) ;
- ✓ Les outils de communication et de collaboration (Microsoft 365) ;
- ✓ Les espaces de stockage sur les serveurs locaux ;
- ✓ Le stockage individuel sur le cloud(@csefrs.ma) ;
- ✓ Sauvegarde des données professionnelles de l'utilisateurs sur le cloud(@csefrs.ma) ;
- ✓ Rapatriement des données cloud en local ;
- ✓ La sauvegarde des environnements locaux des utilisateurs (données spécifique désignées par l'utilisateur et stockées sur les serveurs locaux).

d) Les moyens audiovisuels :

- ✓ Équipements d'enregistrement audio et vidéo (caméras, microphones, enregistreurs)
- ✓ Systèmes de visioconférence (plateformes logicielles et équipements matériels)
- ✓ Écrans de projection et systèmes de sonorisation des salles de réunion
- ✓ Plateformes de diffusion en direct (streaming)
- ✓ Plateformes d'archivage et de consultation des enregistrements audiovisuels