

# Politique de la sécurité du système d'information



## Charte d'utilisation du système d'information du CESE

2023

# SOMMAIRE

## Table des matières

<b>I.</b>	<b>Etat d'art</b> .....	<b>3</b>
<b>I.1.</b>	<b>Préambule</b> .....	<b>3</b>
<b>I.2.</b>	<b>Domaine d'application de la charte</b> .....	<b>3</b>
<b>I.3.</b>	<b>Les principes de base de son élaboration</b> .....	<b>3</b>
<b>I.4.</b>	<b>Les règles de déontologie</b> .....	<b>4</b>
<b>I.5.</b>	<b>Responsabilité de l'utilisateur</b> .....	<b>4</b>
<b>I.6.</b>	<b>Sécurité et protection du système d'information</b> .....	<b>5</b>
<b>II.</b>	<b>Dispositions générales d'application de la charte : Comité de Pilotage</b> .....	<b>5</b>
<b>III.</b>	<b>Règles d'utilisation des outils informatiques</b> .....	<b>6</b>
<b>III.1.</b>	<b>Matériels, Réseaux et production informatique</b> .....	<b>6</b>
<b>III.2.</b>	<b>Accès aux ressources informatiques</b> .....	<b>6</b>
<b>III.3.</b>	<b>Logiciels applicatifs, progiciels et bureautique</b> .....	<b>7</b>
<b>III.3.1.</b>	<b>Détention et installation de logiciels</b> .....	<b>7</b>
<b>III.3.2.</b>	<b>Progiciels et logiciels applicatifs</b> .....	<b>7</b>
<b>III.4.</b>	<b>Messagerie électronique et services Office 365</b> .....	<b>7</b>
<b>III.5.</b>	<b>Directives pour l'Utilisation de l'Intelligence Artificielle au CESE</b> .....	<b>8</b>
<b>III.6.</b>	<b>Utilisation d'internet</b> .....	<b>9</b>
<b>IV.</b>	<b>Activités interdites</b> .....	<b>9</b>
<b>V.</b>	<b>Règles générales</b> .....	<b>10</b>
<b>V.1.</b>	<b>Sanctions</b> .....	<b>10</b>
<b>V.2.</b>	<b>Modification de la charte</b> .....	<b>10</b>
<b>V.3.</b>	<b>Engagement et acceptation</b> .....	<b>10</b>

# I. État d'art

## I.1. Préambule

### **Charte d'Utilisation et de Sécurité du Système d'Information**

Cette charte établit les principes de sécurité et les règles d'utilisation du système d'information auxquels le **Conseil Économique, Social et Environnemental (CESE)** ainsi que ses utilisateurs s'engagent à adhérer. Elle détaille les responsabilités et les droits impartis à chaque partie.

**Code de Conduite** : Cette charte sert de cadre pour définir les normes d'utilisation des moyens de communication et des technologies de l'information déployées par le **CESE**.

**Définition de l'Utilisateur** : Le terme « utilisateur » réfère à toute personne qui, dans l'exercice de ses fonctions professionnelles, a accès aux ressources informatiques du **CESE**, que ce soit en tant qu'employé ou en tant que prestataire externe sous contrat.

**Système d'Information** : Le système d'information (SI) comprend l'ensemble des outils, des progiciels, des logiciels, ainsi que tout équipement informatique fourni par le **CESE** pour soutenir les besoins professionnels en matière de traitement, de circulation et de diffusion de données.

L'objectif est d'améliorer l'efficacité, la qualité du travail et la capacité de prise de décision au sein du **CESE**.

## I.2. Domaine d'application de la charte

Cette charte s'applique obligatoirement à tous les utilisateurs des ressources et moyens informatiques du **Conseil Économique, Social et Environnemental (CESE)**. Elle est explicitement destinée à l'ensemble du personnel du **CESE**, incluant mais ne se limitant pas aux consultants, stagiaires, agents de sécurité, personnel de maintenance, ainsi qu'à toute personne ayant un accès, qu'il soit direct ou à distance, aux systèmes d'information du **CESE**.

## I.3. Les principes de base de son élaboration

- **Objectif de la Charte** : L'intention de cette charte est de sensibiliser et d'inculquer un sens de responsabilité parmi les utilisateurs du **Conseil Économique, Social et Environnemental (CESE)**, concernant la gestion des informations, particulièrement celles de nature confidentielle.
- **Surveillance des Moyens Informatiques** : Tous les outils informatiques et de communication au sein du **CESE** sont soumis à une vérification et à un contrôle rigoureux par les services compétents de chaque entité administrative.
- **Usage Professionnel** : Les équipements informatiques et de communication sont exclusivement destinés à un usage professionnel au sein du **CESE**.
- **Droit de Vérification** : Le **CESE** se réserve le droit d'employer tous les moyens de vérification et de contrôle nécessaires pour superviser l'utilisation faite de ses systèmes d'information. Tout utilisateur en violation des termes de cette charte peut être sujet à des mesures disciplinaires, conformément aux règles administratives en vigueur.

## I.4. Les règles de déontologie

Chaque utilisateur est tenu responsable de l'utilisation qu'il fait des ressources du système d'information du **Conseil Économique, Social et Environnemental (CESE)**. Il doit adhérer scrupuleusement aux principes de déontologie informatique, ce qui inclut notamment l'interdiction de :

- **Masquer son Identité** : Il est impératif d'utiliser sa véritable identité dans toute correspondance électronique. L'usage de pseudonymes est formellement interdit.
- **Usurpation de Mot de Passe** : Il est interdit de s'approprier le mot de passe d'un autre utilisateur.
- **Modification ou Destruction de Données** : Il est prohibé de modifier ou de détruire des informations appartenant à autrui sur tout système informatique du CESE.
- **Accès Non Autorisé** : Accéder à des informations sans l'autorisation de leur propriétaire est strictement défendu.
- **Atteinte à l'Intégrité d'Autrui** : Il est défendu de nuire à l'intégrité d'autres utilisateurs, que ce soit par des messages, des textes ou des images provocants.
- **Perturbation des Réseaux et systèmes** : Il est interdit d'interrompre le fonctionnement normal du réseau ou de tout système connecté ou non au réseau.

Chaque utilisateur doit veiller à respecter ces directives pour maintenir un environnement informatique sécurisé et respectueux au sein du **CESE**.

## I.5. Responsabilité de l'utilisateur

Chaque utilisateur est responsable des outils informatiques qui lui sont confiés ainsi que de la sécurité physique des ressources qu'il emploie. Il est également chargé de contribuer à la sécurité du système d'information et de s'abstenir de toute action pouvant compromettre le fonctionnement ou l'intégrité du système. Voici les obligations qui lui incombent :

- **Protection des Données** : Assurer la sécurité de l'accès à ses données personnelles et au réseau.
- **Adhésion aux Directives** : Respecter scrupuleusement les consignes établies dans la présente charte, y compris celles relatives à l'utilisation des mots de passe.
- **Signalement d'Incidents** : Rapporter immédiatement tout incident ou dysfonctionnement du système (comme l'apparition de virus, la présence ou la disparition inattendue de fichiers) à la DSI.
- **Usage Conforme des Ressources** : S'abstenir de consulter, télécharger, stocker, publier ou diffuser des documents, informations ou fichiers qui sont illégaux, contraires à l'ordre public, nuisibles à l'intégrité des données du **CESE** ou qui violent la confidentialité des informations.
- **Interdiction de Transmission Non Autorisée** : Éviter de transmettre sans autorisation préalable tout programme, information, ou fichier pouvant être préjudiciable. En cas de réception accidentelle de tels éléments, l'utilisateur est tenu de les éliminer immédiatement.
- **Conduite Responsable** : Agir avec responsabilité et intégrité, respecter les règles et procédures établies, et œuvrer pour le bien du **CESE** et de ses partenaires.
- **Respect des Mesures de Confidentialité** : Observer toutes les précautions nécessaires, y compris les mesures de confidentialité, pour protéger les intérêts du **CESE**.
- **Alerte en cas de Non-Conformité** : Informer sa hiérarchie ou la DSI en cas de témoignage de non-respect de cette charte.

## I.6. Sécurité et protection du système d'information

Le but principal de protéger le système d'information est de garantir la continuité et la qualité des services offerts aux utilisateurs, tout en assurant l'intégrité et la confidentialité des données traitées. Pour cela, certaines pratiques sont strictement interdites :

- **Interdiction d'Installer des Logiciels Compromettants** : Il est formellement interdit d'installer tout logiciel qui pourrait compromettre la sécurité, que ce soit directement ou indirectement.
- **Usage Responsable des Ressources** : Il est défendu d'utiliser des programmes qui pourraient saturer les ressources ou inonder la bande passante du réseau.
- **Non-Introduction de Programmes Nuisibles** : L'introduction de virus ou de tout autre programme nuisible est strictement prohibée.
- **Prohibition du Piratage et de l'Espionnage** : Tout acte de piratage ou d'espionnage est formellement interdit.
- **Modification de Configuration** : Il est interdit de modifier la configuration des machines sans autorisation.
- **Usage Exclusif de Son Compte Personnel** : Chaque utilisateur doit utiliser uniquement son propre compte et ne pas tenter de masquer son identité ou d'utiliser des comptes d'autres personnes.

En plus de ces interdictions, chaque utilisateur est responsable de la sécurité de l'accès aux dispositifs informatiques (ordinateurs portables, PC, etc.) qui lui sont attribués. Il doit s'assurer de fermer les sessions ouvertes à son nom avant de quitter son poste de travail ou activer la mise en veille automatique, sécurisée par mot de passe, après une période d'inactivité.

## II. Dispositions générales d'application de la charte : Comité de Pilotage

Le Comité de Pilotage du CESE, composé du Président, du Secrétaire Général et du Directeur des Systèmes d'Information (DSI), a pour missions :

- **Établissement du Plan d'Action Annuel** : La Direction des Systèmes d'Information (DSI) est chargée d'élaborer un plan d'action annuel conforme aux directives de cette charte. Ce plan doit recenser les incidents et les risques identifiés ainsi que définir les mesures préventives et correctives à adopter.
- **Suivi de la Politique de Sécurité du Système d'Information** : Le comité de pilotage assure le suivi de la mise en œuvre de cette politique de sécurité, avec pour objectifs de :
  - a. Analyser et évaluer les plans d'action établis par la DSI,
  - b. Garantir une optimisation du système d'information par une convergence des politiques et outils de sécurité de ses sous-systèmes (matériel, logiciels, ressources financières et humaines),
  - c. Suggérer des directives complémentaires, en prenant en compte les évolutions technologiques récentes et les nouvelles normes réglementaires.
- **Actualisation de la Charte** : Le comité est aussi chargé de la révision régulière de cette charte pour garantir son alignement avec les stratégies organisationnelles et les obligations légale.

### III. Règles d'utilisation des outils informatiques

Les données et le patrimoine documentaire du **Conseil Économique, Social et Environnemental (CESE)** sont de nature confidentielle et peuvent parfois être très sensibles. L'accès à certaines ressources informatiques, telles que les bases de données, les résultats des enquêtes et des études avant leur publication officielle, ainsi que les dossiers des ressources humaines, est conditionné par une autorisation préalable du Président et du Secrétaire générale du CESE.

#### III.1. Matériels, Réseaux et production informatique

Les principes suivants doivent être scrupuleusement respectés par tous les utilisateurs :

- **Déplacement de Matériel** : Il est impératif de déclarer tout déplacement de matériel informatique à la Direction des Systèmes d'Information (DSI) avant tout transfert. Une autorisation écrite doit être obtenue de la part de la DSI pour garantir la conformité avec les procédures de sécurité et de gestion des équipements.
- **Réaffectation de Matériel** : Toute réaffectation de matériel informatique et des logiciels qui lui sont associés doit impérativement être coordonnée avec les service concernés (DSI et DAAF).
- **Entretien du Matériel** : Chaque utilisateur est tenu de prendre soin du matériel informatique qui lui est attribué. En cas de détection d'anomalie, il doit immédiatement en informer le responsable de l'entité informatique.
- **Utilisation Optimisée des Ressources** : Les activités susceptibles de solliciter intensivement les ressources informatiques (telles que l'impression de gros volumes de documents ou l'utilisation intensive du réseau) doivent être planifiées après consultation avec l'entité informatique et réalisées à des moments qui minimisent l'impact sur les autres utilisateurs.

#### III.2. Accès aux ressources informatiques

- **Gestion des Sessions** : Chaque utilisateur qui ouvre une session sur un PC, une station de travail, un portable ou un serveur, doit obligatoirement la fermer avant de quitter les lieux, particulièrement dans les espaces ouverts. En cas d'absence de courte durée, il est fortement conseillé de verrouiller la session avec un mot de passe.
- **Contrôle de l'Accès par les Stagiaires et les Visiteurs** : L'accès au parc informatique par les stagiaires et les visiteurs doit être strictement surveillé et placé sous la responsabilité de l'encadrant.
- **Assignation des Profils d'Administrateurs** : L'attribution des profils d'administrateurs doit faire l'objet d'une étude approfondie et être autorisée par le Président du CESE ou le Secrétaire général.
- **Confidentialité des Mots de Passe des Administrateurs** : Les mots de passe administratifs sont confidentiels et ne doivent en aucun cas être partagés ou divulgués.
- **Accès aux Locaux Informatiques** : L'accès aux locaux de l'entité informatique par des personnes extérieures ne peut se faire qu'en présence d'un membre du personnel de cette entité.
- **Contrôle d'Accès aux Locaux Techniques** : Chaque entité administrative doit assurer un contrôle rigoureux de l'accès aux locaux contenant des équipements informatiques qui lui sont affectés.

### III.3. Logiciels applicatifs, progiciels et bureautique

#### III.3.1. Détention et installation de logiciels

- **Installation de Logiciels de Bureautique** : L'installation de logiciels de production bureautique au sein du CESE est une prérogative exclusive de la Direction des Systèmes d'Information (DSI). Cette centralisation vise à assurer une gestion cohérente et sécurisée des applications standardisées.
- **Installation de Logiciels Spécifiques** : Pour les logiciels spécifiques, leur installation doit également être effectuée sous la supervision directe de la DSI. Cela permet de garantir que toutes les procédures sont conformes aux standards de sécurité et d'interopérabilité établis par le CESE.
- **Signalement de Problèmes de Sécurité** : Les utilisateurs doivent rapporter sans délai à la DSI tout problème pouvant affecter la sécurité du système informatique. Cela inclut les anomalies dans la gestion des protections, les failles systémiques, ou l'existence de logiciels suspects. La vigilance et la réactivité des utilisateurs sont des composantes essentielles pour préserver la sécurité des infrastructures informatiques.

#### III.3.2. Progiciels et logiciels applicatifs

##### Obligations des Utilisateurs :

- **Respect des Instructions** : Les utilisateurs doivent respecter scrupuleusement toutes les consignes émises par les responsables des progiciels ou logiciels installés.
- **Usage Approprié des Logiciels** : Il est interdit aux utilisateurs d'installer ou d'utiliser des logiciels à des fins qui ne sont pas conformes aux missions du CESE.
- **Responsabilité des Données** : Chaque utilisateur assume l'entière responsabilité de l'intégrité des données manipulées ou gérées par les logiciels.

##### Interdictions Formelles :

- **Installation de Logiciels Non Autorisés** : Les utilisateurs s'interdisent d'installer des logiciels ou des outils autres que ceux officiellement mis en œuvre par le CESE.
- **Modification des Logiciels** : Il est interdit de modifier les logiciels installés par le CESE.
- **Changement de Configuration** : Les utilisateurs ne doivent pas installer des logiciels qui pourraient altérer la configuration des machines.
- **Actions Nuisibles au Système** : Il est prohibé d'effectuer toute opération susceptible de perturber le bon fonctionnement du système, comme la suppression de répertoires ou de fichiers nécessaires ou la modification d'adresses IP.

### III.4. Messagerie électronique et services Office 365

L'utilisation de la messagerie électronique du CESE doit se faire exclusivement dans le cadre des activités professionnelles et dans le respect de la législation en vigueur. Voici les règles spécifiques à suivre :

- **Responsabilité du Contenu** : Chaque utilisateur est responsable du contenu qu'il insère ou envoie via la messagerie électronique du CESE.
- **Confidentialité des Messages** : Il est interdit de lire ou de prendre connaissance de messages électroniques appartenant ou destinés à une autre personne sans autorisation.

- **Usurpation d'Identité** : Les utilisateurs ne doivent pas usurper l'identité d'autrui ni intercepter des communications entre tiers.
- **Utilisation Appropriée des Services** : Les services de messagerie ne doivent pas être utilisés pour diffuser des données confidentielles ou illégales.
- **Correction et Respect** : Chaque utilisateur doit maintenir un haut niveau de courtoisie dans ses échanges électroniques.
- **Messages Professionnels** : Les messages non professionnels ou pouvant offenser la sensibilité des autres, notamment ceux contenant des images provocantes ou des propos injurieux, racistes, etc., sont strictement interdits.
- **Prévention de la Saturation du Réseau** : Pour éviter la surcharge du réseau, les utilisateurs doivent éviter d'envoyer des messages non essentiels et limiter la liste des destinataires aux personnes directement concernées.

#### Concernant l'Utilisation des Services Microsoft Office 365 au CESE :

- **Accès aux Services** : Votre compte Office 365 vous permet d'accéder à la plupart des produits Microsoft en utilisant l'adresse e-mail qui vous est attribuée par l'administrateur @cese .ma.
- **Gestion des Données** : L'administrateur du domaine peut accéder à toutes les données stockées dans votre compte, y compris vos e-mails, en conformité avec les politiques de confidentialité de Microsoft.
- **Contrôle Administratif** : L'administrateur de domaine a le pouvoir de désactiver certains services ou de limiter votre capacité à transférer des données en dehors de votre compte professionnel.
- **Implications Légales** : L'accord juridique entre vous et l'administrateur @cese .ma peut influencer l'accès à votre compte, la gestion des données, et les conditions d'utilisation.

### III.5. Directives pour l'Utilisation de l'Intelligence Artificielle au CESE

- **Conformité aux Protocoles IT** : Les employés du CESE doivent strictement adhérer aux protocoles définis par la DSI concernant le déploiement et l'utilisation des technologies d'intelligence artificielle. Ces protocoles incluent la sélection rigoureuse des technologies, leur installation et configuration selon les meilleures pratiques de sécurité, des tests et validations approfondis pour assurer l'exactitude et l'efficacité des systèmes, et une maintenance régulière incluant des mises à jour de sécurité. Il est également requis que tous les systèmes d'IA soient utilisés dans le respect total des mesures de protection des données et de la confidentialité, avec une formation adéquate des utilisateurs pour une manipulation sécurisée et efficace. Des audits réguliers doivent être menés pour garantir la conformité continue aux directives internes et légales. Ces mesures garantissent que les outils d'IA, y compris les chatbots et les outils d'analyse de données, sont utilisés de manière optimale et sécurisée au sein du CESE.
- **Protection des Données** : Il est impératif de maintenir la confidentialité et l'intégrité des données manipulées par les applications d'IA, en particulier lorsqu'elles concernent des informations sensibles du CESE.
- **Éducation et Formation** : Les utilisateurs des outils d'IA doivent participer activement à des sessions de formation organisées par le CESE pour comprendre pleinement les capacités, les risques et les restrictions de ces technologies.
- **Surveillance Continue** : Une collaboration étroite avec la direction des systèmes d'information est requise pour surveiller l'efficacité des outils d'IA et évaluer régulièrement leur impact sur les opérations du CESE.
- **Éthique et Responsabilité** : Tous les employés engagés dans l'utilisation des outils d'IA doivent s'assurer que leur utilisation est éthique et responsable, en accord avec les valeurs et les objectifs du CESE.



### III.6. Utilisation d'internet

- **Utilisation Professionnelle Prioritaire** : L'usage d'Internet doit principalement répondre à des besoins professionnels. La consultation de sites inappropriés, tels que les sites pornographiques, ceux promouvant des activités criminelles ou racistes, appelant à la haine raciale, ou les forums de discussion non professionnels, est formellement interdite.
- **Publication Responsable** : Tout contenu publié en ligne doit être acquis légalement, sans enfreindre les droits d'autrui, et sans exposer le CESE à des risques légaux.
- **Prudence avec les Informations Personnelles** : Il est interdit de fournir des informations personnelles associées au CESE, telles que les adresses email, lors de l'utilisation d'Internet à des fins personnelles ou pour la création de comptes sans l'autorisation explicite de la direction informatique.
- **Usage Modéré d'Internet** : L'accès à Internet ne doit pas être utilisé de manière abusive, surtout si l'usage n'est pas strictement professionnel.
- **Interdiction de Nuire** : Il est absolument interdit d'utiliser l'accès Internet du CESE pour nuire à d'autres institutions ou individus, que ce soit à leur patrimoine informationnel ou physique.
- **Prudence avec les Liens et Téléchargements** : Ouvrir des liens d'origine inconnue ou dont le contenu semble douteux est interdit, tout comme télécharger ou installer des données ou des programmes non vérifiés.

### IV. Activités interdites

Les employés du CESE doivent s'abstenir de :

- **Violation de Droits de Propriété Intellectuelle** : Il est interdit de distribuer, installer ou utiliser des versions non autorisées (« piratées ») de tout produit numérique (logiciels, musiques, magazines, ouvrages, etc.) qui sont soumis à des droits de licence que le CESE n'a pas légalement acquis.
- **Introduction de Codes Malicieux** : Il est strictement défendu d'introduire des codes malicieux tels que virus, vers, chevaux de Troie, e-mail bombs, etc., sur l'infrastructure réseau du CESE.
- **Confidentialité des Identifiants** : Les utilisateurs ne doivent ni dévoiler, partager, ni rendre accessibles les identifiants électroniques (comptes et mots de passe) d'autres utilisateurs.
- **Gestion Sécurisée des Mots de Passe** : Il est interdit d'inscrire des mots de passe sur un support papier ou dans un fichier non crypté.
- **Utilisation Appropriée des Ressources Informatiques** : Les ressources informatiques et les services réseau du CESE ne doivent pas être utilisés pour transmettre des documents dont la circulation contrevient aux lois en vigueur ou peut nuire à autrui.
- **Non-interférence avec les Sessions Utilisateur** : L'utilisation de tout programme, script, commande ou envoi de messages dans le but d'interférer ou de désactiver les sessions des utilisateurs via le réseau local ou Internet est formellement interdite.
- **Protection des Informations de Réseau** : Il est essentiel de ne pas divulguer des informations sur tout ou une partie du réseau du CESE qui pourraient compromettre la sécurité du système d'information.

## V. Règles générales

### V.1. Sanctions

Toute violation de la présente charte expose la personne concernée à des sanctions pénales prévues par le code pénal ou à des sanctions disciplinaires prévues dans le statut de la fonction publique.

### V.2. Modification de la charte

Cette charte est susceptible d'être modifiée à chaque fois que l'usage des ressources informatique, le changement des dispositions réglementaires et/ou les évolutions technologiques l'imposent.

### V.3.Engagement et acceptation

Tout utilisateur du CESE doit attester avoir pris connaissance de la charte de l'utilisation du système d'information et s'engager à l'appliquer pour une utilisation professionnelle de toutes les ressources informatiques.

Tout contrevenant aux dispositions de la présente charte sera exposé aux dispositions prévues par la loi.

Je soussigné(e).....(Nom, prénom),

(Cochez selon votre qualité)

- Membre du CESE
- Personnel du CESE
- Agent temporaire ou stagiaire au CESE
- Prestataire externe, travaillant pour le CESE .....

M'engage à respecter les consignes et règles citées dans la Charte de l'utilisation du système d'information.

Fait à ....., le ...../...../.....

(Signature)