المندوبية السامية للتخطيط
HAUT-COMMISSARIAT AU PLAN

Charte des Systèmes d'Information

Haut Commissariat au Plan

Etat des versions successives

Indice	*Date*	*Observations*
1	2015	Première version
2	2024	

SOMMAIRE

I. Etat d'art

I.1. Préambule

LE HCP met à la disposition de son personnel, pour les besoins professionnels du service, le patrimoine informationnel et documentaire, le système d'information et l'infrastructure informatique et de télécommunication (désignés ci-après par "Le Système d'Information du HCP" ou "SI") afin d'en assurer une utilisation principalement professionnelle, sécurisée, efficiente et optimale.

Cette charte définit les règles d'usage et de sécurité du système d'information que le Haut-Commissariat au Plan (HCP) et l'utilisateur s'engagent à respecter. Elle précise les droits et devoirs de chacun.

Il s'agit d'un code de bonne conduite ayant pour objectif de définir les conditions générales d'utilisation des moyens de communication et des outils informatiques mis en œuvre par le HCP.

Le terme "utilisateur" désigne toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information, qu'elle soit agent du HCP ou prestataire ayant un contrat avec le HCP.

Le terme "entité" désigne toutes les directions centrales ou régionales du HCP.

I.2. Domaine d'application de la charte

Les dispositions de cette charte s'imposent de plein droit à tous les utilisateurs des moyens ou des ressources informatiques du HCP. Elle est destinée, de manière impérative, à tout le personnel du HCP, y compris les consultants, les stagiaires, les agents de sécurité, les agents chargés de la maintenance, ainsi qu'à toute personne ayant un accès direct ou à distance aux systèmes d'information du HCP. Nul n'est censé l'ignorer.

I.3. Accès au Système d'Information

Les droits d'accès au système d'information et les habilitations sont octroyés conformément aux usages et procédures en vigueur, notamment pour la gestion de la documentation, la gestion des comptes, l'affectation des droits sur les applications et la procédure de gestion des habilitations et des accès logiques.

Les droits d'accès électroniques sont accordés en échange d'un nom d'utilisateur et d'un mot de passe strictement individuels et non transférables, même temporairement. Leur utilisation engage la responsabilité de l'utilisateur. Le mot de passe doit être tenu secret et sera systématiquement désactivé lorsque l'utilisateur quitte le HCP ou en cas de violation d'une des obligations imposées par la présente charte. Il peut être modifié lorsqu'un utilisateur change de rattachement au sein du HCP.

De plus, l'utilisateur est tenu de protéger l'accès à son ordinateur qui lui est assigné. Il doit fermer toutes les sessions ouvertes à son nom avant de quitter les lieux, ou bien activer la mise en veille automatique (protégée par un mot de passe) après une courte période d'inactivité.

L'accès au SI peut être accordé à des personnes externes au HCP, telles que des stagiaires ou des consultants, mais uniquement avec des habilitations limitées et prédéfinies, et sous la responsabilité et le contrôle direct d'un utilisateur HCP dûment identifié. Ces habilitations sont portées à la connaissance des responsables du SI.

Pour chaque domaine relevant du SI, les droits et habilitations sont accordés après l'accord du responsable du domaine. Ils sont affichés de manière transparente pour les parties prenantes et les utilisateurs intervenant dans ledit domaine.

II. Principes fondamentaux

II.1. Les principes de base de son élaboration

L'objectif recherché par la charte est de sensibiliser et responsabiliser les utilisateurs quant à l'utilisation de l'information au sein du HCP, en particulier pour ce qui concerne les informations confidentielles.

Tous les moyens informatiques et de communication du HCP font l'objet de vérifications et de contrôles par les services compétents au sein de chaque entité administrative.

Les moyens informatiques et de communication sont destinés à un usage strictement professionnel.

Le HCP se réserve le droit d'utiliser tous les moyens de vérification et de contrôle concernant l'utilisation des systèmes d'information par les utilisateurs. En cas de constatation d'une violation des dispositions de la présente charte, l'utilisateur fautif s'expose à des mesures disciplinaires conformément à la réglementation en vigueur au sein de l'administration.

II.2. Les règles de déontologie

Chaque utilisateur est responsable de l'usage qu'il fait des ressources du SI. Il s'engage à respecter les règles de la déontologie informatique et à s'abstenir de réaliser intentionnellement des opérations susceptibles d'avoir les conséquences suivantes :

- Masquer sa véritable identité, usurper l'identité d'autrui ou s'approprier le mot de passe d'autrui, ainsi que d'utiliser des comptes autres que ceux auxquels il a légitimement accès.
- Contourner les procédures de sécurité en place.
- Utiliser une ressource matérielle ou informationnelle sans avoir obtenu une autorisation explicite de la personne, de l'autorité ou de l'instance à laquelle elle est attribuée, même si cette ressource n'est pas protégée.

- Reproduire, télécharger, copier, diffuser, modifier ou utiliser des logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir préalablement obtenu l'autorisation des titulaires de ces droits.
- Porter atteinte à l'intégrité d'un autre utilisateur, notamment par le biais de messages, textes ou images provocants.
- Perturber le fonctionnement normal du réseau ou de l'un des systèmes connectés ou non au réseau.

De plus, tout utilisateur est tenu d'informer immédiatement le service concerné de chaque entité du HCP en cas de découverte d'une lacune de sécurité, d'un incident ou d'une activité suspecte liée à la sécurité du SI, qu'il s'agisse d'une faille logique ou physique.

II.3. Conditions de confidentialité

Les documents, données, fichiers, messages ou communications réseaux, voix et données sont soumis au principe de confidentialité et leur accès est réservé exclusivement à leur(s) propriétaire(s).

Le respect de cette confidentialité implique notamment :

- Veiller à ce que les informations confidentielles ne soient pas divulguées à des personnes non autorisées.
- Prendre toutes les mesures nécessaires pour assurer la confidentialité des données.
- Assurer la sécurité de tous les actifs organisationnels du HCP, qu'il s'agisse de documents papier, de CD, etc.

L'utilisateur est informé de manière transparente sur les mécanismes de contrôle et de sécurité mis en place. Il est sensibilisé et informé de ses droits et de ses responsabilités vis-à-vis du SI HCP.

Tout accès clandestin ou non explicitement autorisé est strictement interdit.

III. Sécurité

La sécurité du SI est l'affaire de tous et doit avoir la priorité et l'importance requises.

III.1. Responsabilité de l'utilisateur

L'utilisateur est responsable des outils et du matériel qui lui sont attribués. Il est également responsable de la sécurité physique des ressources qui lui sont confiées, que ce soit à son lieu de travail ou lors de déplacements. Il doit contribuer à la sécurité du système d'information en s'abstenant de toute action susceptible de perturber son bon fonctionnement ou d'en compromettre l'intégrité. À cet égard, il doit :

- Protéger l'accès à ses données et au réseau.
- Contribuer, dans la mesure du possible, à la vérification de l'installation d'un antivirus sur son poste.
- Respecter les consignes énoncées dans la présente charte, notamment celles liées à l'utilisation des mots de passe.
- Signaler tout incident suspect ou tout dysfonctionnement du système (comme l'apparition de virus ou la présence/disparition inopinée de fichiers) au service concerné de chaque entité du HCP.
- S'abstenir de consulter, télécharger, stocker, publier ou diffuser, via les moyens informatiques et de communication, des informations ou des programmes contraires à la loi, à l'ordre public ou portant atteinte aux ressources du HCP, en particulier à l'intégrité et à la préservation des données, ainsi qu'à la confidentialité des informations et des données du HCP et/ou de ses utilisateurs. De même, il doit éviter toute action contraire aux bonnes mœurs ou susceptible de porter atteinte au respect de la personne humaine et de sa dignité.
- S'interdire de solliciter l'envoi par des tiers, en pièces jointes, de tels programmes ou informations, ainsi que de les transmettre à des tiers sans l'autorisation préalable du responsable compétent. Si l'utilisateur reçoit de tels éléments, il doit les détruire immédiatement après les avoir identifiés.
- Éviter d'ouvrir, de répondre ou de transférer des messages de type spam ou douteux qui n'ont pas été détectés et bloqués par le serveur de messagerie.
- Agir en toute circonstance avec responsabilité, en respectant les règles et les procédures en vigueur, et œuvrer dans l'intérêt du HCP et de ses partenaires.
- Respecter toutes les mesures de précaution, y compris les mesures de confidentialité, si cela est requis, lors de l'utilisation des informations, dans le but de protéger les intérêts du HCP.
- Informer leur hiérarchie en cas de constatation d'une violation de la charte.

- Éviter de communiquer son adresse e-mail professionnelle sur des sites Internet non professionnels.
- S'abstenir de modifier les logiciels installés ou la configuration de leur poste de travail.
- Veiller à ce que l'accès à l'extérieur depuis l'infrastructure du HCP se fasse par l'intermédiaire des dispositifs sécurisés mis en place. Toute autre connexion de télécommunication avec l'extérieur doit être expressément approuvée et contrôlée par le service compétent de chaque entité du HCP. L'installation d'un modem ou de tout autre moyen de communication avec l'extérieur doit être autorisée et contrôlée par le service compétent de chaque entité du HCP.

III.2. Sécurité et protection des systèmes d'information

L'objectif de la protection des systèmes d'information est de garantir la continuité des services offerts aux utilisateurs en assurant l'intégrité et la confidentialité des données. Par conséquent, les actions suivantes sont strictement interdites :

- Installer des logiciels visant à contourner directement ou indirectement les mesures de sécurité.
- Utiliser des programmes qui surchargent les ressources ou perturbent la bande passante.
- Introduire des programmes nuisibles tels que des virus ou tout autre type de logiciel malveillant.
- Effectuer des actes de piratage ou d'espionnage.
- Utiliser ou tenter d'utiliser des comptes appartenant à d'autres personnes ou dissimuler sa véritable identité.

L'utilisateur est également tenu de protéger l'accès au matériel informatique qui lui est assigné, que ce soit un ordinateur de bureau, un ordinateur portable, etc. Avant de quitter les lieux, il doit fermer toutes les sessions ouvertes à son nom ou activer la mise en veille automatique (protégée par un mot de passe) après une courte période d'inactivité.

III.3. Sauvegarde et protection des données

Les données stockées sur les serveurs communs sont sauvegardées par le service compétent de chaque entité du HCP et sont placées sous sa responsabilité. La fréquence des sauvegardes, la durée de conservation des sauvegardes et la rotation des supports sont déterminées et affichées dans le cadre d'une politique de sauvegarde établie en accord avec les utilisateurs, tout en respectant les contraintes techniques et de sécurité.

En cas de panne ou de perte de données, les informations sauvegardées lors de la dernière sauvegarde seront entièrement récupérées et restaurées. Il incombe à l'utilisateur de reconstituer les données introduites depuis la dernière sauvegarde.

Les données stockées sur les postes de travail, y compris les données archivées de la messagerie, sont placées sous la responsabilité des utilisateurs. Dans certains cas, si l'infrastructure technique le permet, le service compétent de chaque entité du HCP peut prendre en charge la sauvegarde des données spécifiquement désignées par l'utilisateur.

IV. Dispositions générales d'application de la charte :

IV.1. Respect des procédures

Chaque utilisateur doit veiller au respect des procédures en vigueur. Par conséquent, tout incident doit être signalé au service compétent de chaque entité du HCP. De même, toute demande d'évolution ou de modification concernant le matériel ou les logiciels doit être soumise en respectant ces procédures.

IV.2. Engagements du personnel des entités informatiques

En plus de la discipline exigée de l'ensemble du personnel du HCP, le personnel des services informatiques des différentes entités du HCP doit prendre en compte la sensibilité du système d'information et son rôle transversal et critique dans la vie quotidienne du HCP, à tous les niveaux.

La configuration, la maintenance de la sécurité, le contrôle et l'analyse des performances de l'infrastructure nécessitent l'utilisation de comptes à privilèges. Ces comptes sont accordés au personnel clairement identifié, afin de mener et/ou d'effectuer des tâches spécifiques sur le réseau et les serveurs.

L'analyse statistique ou l'accès aux ressources du système d'information par le personnel explicitement autorisé ne peut être effectué que dans le seul but de garantir la sécurité et d'analyser les performances de l'infrastructure informatique et de télécommunication.

En cas de besoin d'accéder aux postes de travail des utilisateurs, le personnel désigné par l'entité informatique, et autorisé à accéder à distance, doit se conformer aux exigences suivantes :

- L'outil utilisé doit être documenté et approuvé par l'entité informatique de la direction.
- L'accès à distance ne doit être effectué qu'à la demande du propriétaire et en sa présence (dans le cas d'une assistance à distance). L'utilisateur doit confirmer son besoin et autoriser l'informaticien à prendre le contrôle à distance du poste lorsque cela est nécessaire.
- L'accès à distance par le biais de logiciels d'administration réseau pour des besoins de numérisation ou d'inventaire automatique est autorisé pour le personnel désigné. Cependant, cet accès ne concerne pas le contenu des fichiers.

L'entité informatique est autorisée à mettre en œuvre les moyens nécessaires pour observer, analyser et optimiser le trafic des données et de la voix. À cette fin, l'entité informatique se réserve le droit de :

- Vérifier le trafic entrant et sortant ainsi que le trafic transitant sur le réseau interne.
- Effectuer des audits pour vérifier l'application des consignes d'utilisation et des règles de sécurité.
- Contrôler les logiciels installés.
- Filtrer les adresses électroniques (URL) des sites non autorisés.
- Tracer et auditer tous les accès aux services Intranet et Internet.

Les messages contenant des virus identifiés seront automatiquement bloqués par le système. Les intervenants externes utilisés par l'entité informatique interviennent sous sa responsabilité.

V. Confidentialité du patrimoine informationnel et données du HCP

Les données et le patrimoine documentaire du HCP sont confidentiels et peuvent parfois revêtir un caractère très sensible.

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 soumis à l'autorisation du Haut-Commissaire au Plan.

De plus, leur utilisation doit respecter les consignes suivantes :

- La communication des données ou des documents en dehors du HCP engage la responsabilité de l'utilisateur. Elle doit se faire dans le cadre d'un projet et avec la validation de l'instance responsable du projet.
- La communication des données ou des rapports techniques vers l'extérieur doit être effectuée conformément aux procédures en vigueur, en impliquant l'entité chargée du Patrimoine Documentaire et Informationnel, et avec l'accord de l'entité métier propriétaire des données.

Pour favoriser l'archivage et la sécurisation du patrimoine documentaire et informationnel, il convient de prendre les précautions suivantes :

- Éviter de conserver des documents non utilisés, qu'ils soient sous forme papier ou électronique, dans le bureau ou sur les postes de travail.

- Lors des déplacements à l'extérieur, il est préférable de ne pas charger les ordinateurs portables ou les supports de stockage avec des documents ou des données sensibles, dans la mesure du possible. L'utilisateur doit prendre les mesures nécessaires pour éviter tout risque de divulgation ou de perte de données confidentielles sensibles ou critiques.
- Toujours veiller à la protection du matériel informatique et des documents en sa possession.

V.1. Utilisation de l'infrastructure et de la messagerie électronique

L'infrastructure (serveurs, réseau, internet) et la messagerie sont des outils de travail mis à la disposition des utilisateurs pour leurs activités professionnelles. Par conséquent, l'utilisation de ces ressources doit être rationnelle.

- L'utilisateur doit utiliser la messagerie électronique du HCP exclusivement dans le cadre de ses activités professionnelles, en respectant la législation en vigueur. En particulier, l'utilisateur :
- Est responsable du contenu qu'il insère ou envoie par le biais de la messagerie électronique du HCP.
- Est strictement interdit de lire ou prendre connaissance de tout message électronique appartenant à une autre personne ou destiné à une autre personne.
- Ne doit se connecter ou tenter de se connecter à un serveur que selon les dispositions prévues.
- Ne doit pas entreprendre d'actions mettant en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.
- Doit faire preuve de la plus grande courtoisie envers ses interlocuteurs dans les échanges électroniques.
- Doit éviter de faire circuler des messages électroniques non professionnels ou portant atteinte à l'intégrité ou à la sensibilité d'un autre utilisateur, notamment en envoyant des messages comportant des images provocantes ou à caractère injurieux, raciste, etc.
- Doit éviter de saturer le réseau en envoyant des messages inutiles. L'utilisateur doit s'abstenir d'envoyer des messages qui ne sont pas directement liés à sa fonction et doit limiter la liste des destinataires aux utilisateurs directement concernés par le message.

Il est à noter que pour l'utilisation des services de messagerie et des outils collaboratifs au sein du HCP, certaines informations sont importantes à prendre en compte :

- Votre compte professionnel vous permet d'accéder à diverses fonctionnalités et produits fournis par le HCP.
- L'administration des comptes est gérée par l'équipe compétente au sein du HCP.

- L'utilisation de la messagerie et des outils collaboratifs doit être conforme à la politique et aux directives internes du HCP.
- Le respect de la confidentialité et des règles de communication professionnelle est primordial lors de l'utilisation de ces outils.
- Tout incident ou dysfonctionnement lié à la messagerie ou aux outils collaboratifs doit être signalé au service concerné de chaque entité du HCP.

VI. Règles générales

VI.1 Sanctions

Toute violation de la présente charte expose la personne concernée à des conséquences légales, notamment des sanctions pénales conformément au code pénal, ainsi qu'à des sanctions disciplinaires prévues dans le cadre du statut de la fonction publique.

VI.2 Révision de la charte

La présente charte a été rédigée dans l'intérêt de tous les utilisateurs du SI HCP. Elle sera régulièrement mise à jour par le HCP afin de prendre en compte l'évolution constante des technologies de l'information et de l'environnement au sein du HCP.

VI.3 Entrée en vigueur

La présente version de la charte sera mise en vigueur dès sa diffusion.

VI.4. Engagement et acceptation

Tout agent du HCP ou utilisateur doit attester avoir pris connaissance de la charte d'utilisation du système d'information et s'engager à l'appliquer dans le cadre d'une utilisation professionnelle de toutes les ressources informatiques. Toute personne en violation des dispositions de la présente charte s'expose aux sanctions prévues par la loi.