المندوبية السامية للتخطيط

ⵜⴰⵡⵙⵙⴰⵏⵜ ⵜⴰⵎⵙⵜⴰⵡⵜ ⵏ ⵜⵣⵔⴼⵜ

HAUT-COMMISSARIAT AU PLAN

Politique de la sécurité du système d'information

Charte d'utilisation du système d'information du HCP

2015

SOMMAIRE

I. Etat d'art……3

I.1. Préambule……3

I.2. Domaine d'application de la Charte……3

II. Dispositions générales d'application……3

III. **Principes fondamentaux……3**

III.1. Les principes de base de son élaboration……3

III.2. Les règles de déontologie……4

III.3. Responsabilité de l'utilisateur……4

IV. **Sécurité et Protection des données……5**

V. Règles d'utilisation des outils informatiques……5

V.1. Matériels, réseaux et production informatique……6

V.2. Accès aux ressources informatiques……6

V.3. Logiciels applicatifs, progiciels et bureautique……6

V.3.1. Détention & Installation de logiciels…… ..6

V.3.2. Progiciels et logiciels applicatifs……7

V.4. Messagerie électronique……7

V.5. Utilisation d'Internet……8

VI. Activités Interdites……8

VII. Règles Générales……9

VII.1. Sanctions……9

VII.2. Modification de la charte……9

VII.3. Engagement et acceptation……9

I. Etat d'art

I.1. Préambule

La présente 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.

C'est un code de conduite dont l'objet est de définir les conditions générales d'utilisation des moyens de communication et 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'il soit agent du HCP ou prestataire ayant un contrat avec le HCP.

On désigne par système d'information (SI) l'ensemble des outils, progiciels, logiciels et tout autre matériel informatique mis à la disposition des utilisateurs pour répondre à leurs besoins professionnels en matière de traitement des données, de circulation et de diffusion de l'information visant à améliorer la qualité de travail et de la prise de décision au sein du HCP.

I.2. Domaine d'application de la charte

Les dispositions de la présente charte s'imposent de plein droit à tous les utilisateurs de moyens ou de ressources informatiques du HCP. Elle est destinée, impérativement, à tout le personnel du HCP, les consultants, les stagiaires, les agents de sécurité, les agents chargés de la maintenance et toutes personnes ayant un accès direct ou à distance aux systèmes d'information du HCP.

II. Principes fondamentaux

II.1. Les principes de base de son élaboration

- L'objectif recherché par la charte est de sensibiliser et de responsabiliser les utilisateurs sur l'utilisation de l'information au sein du HCP, notamment pour les informations confidentielles ;
- Tous les moyens informatiques et de communication du HCP sont vérifiés et contrôlés par les services concernés au niveau de chaque entité administrative ;
- Les moyens informatiques et de communication sont à usage professionnel ;
- Le HCP se réserve le droit d'utiliser tout moyen de vérification et de contrôle concernant tout usage fait des systèmes d'information par les utilisateurs. L'utilisateur fautif est passible d'une action disciplinaire conformément à la réglementation de l'administration en vigueur, si le HCP constate une violation des dispositions de la présente charte.

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 notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- De masquer sa véritable identité (un utilisateur doit, par exemple, indiquer sa véritable identité dans les correspondances de courrier électronique. Les pseudonymes sont exclus) ;
- De s'approprier le mot de passe d'un autre utilisateur ;
- De modifier ou de détruire des informations ne lui appartenant pas sur un des systèmes informatiques ;
- D'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation ;
- De porter atteinte à l'intégrité d'un autre utilisateur, notamment par l'intermédiaire de messages, textes ou images provocants ;
- D'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ou non au réseau.

II.3. Responsabilité de l'utilisateur

L'utilisateur est responsable des outils informatiques mis à sa disposition. Il est responsable de la sécurité physique des ressources qui lui sont affectées ou qu'il utilise. Il doit contribuer à la sécurité du système d'information et ne pas effectuer d'opérations pouvant nuire au bon fonctionnement du système et à son intégrité. Il doit :

- Protéger l'accès à ses données et au réseau ;
- Respecter les consignes retranscrites dans la présente charte (par exemple celles liées à l'utilisation des mots de passe) ;
- Signaler tout incident ou tout dysfonctionnement du système (apparition de virus, présence ou disparition inopinée de fichiers, etc.) au service concerné de chaque entité du HCP;
- S'interdire de consulter, charger, stocker, publier ou diffuser via les moyens informatiques et de communication, des documents, informations, programmes, images, et fichiers multimédia, … contraire à la loi ou à l'ordre public ou portant atteinte aux ressources du HCP et plus particulièrement à l'intégrité et à la conservation des données du HCP, ou portant atteinte à la confidentialité des informations et données du HCP et/ou de ses utilisateurs ou contraire aux bonnes mœurs ou susceptibles 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, informations, logiciels, progiciels, fichiers, bases de données, et fichiers Multimédia, ainsi que de les transmettre à des tiers sans l'autorisation préalable du responsable concerné. Si l'utilisateur est amené à recevoir de tels éléments, il est tenu de les détruire aussitôt après identification;
- Agir en toutes circonstances avec responsabilité, respecter les règles et procédures en vigueur, agir pour le bien du HCP et de ses partenaires ;
- Respecter toutes les mesures de précaution, voir de confidentialité, si cela est demandé, pour l'utilisation des informations afin de protéger les intérêts du HCP ;
- Alerter leur hiérarchie s'ils sont témoins d'un événement de non-respect de la charte.

II.4. Sécurité et protection du système d'information

L'objectif de la protection du système d'information est de maintenir la continuité des services offerts à l'utilisateur en garantissant l'intégrité et la confidentialité des données.

Ainsi, il est formellement interdit :

- d'installer des logiciels contournant la sécurité directement ou indirectement ;
- d'utiliser des programmes qui saturent les ressources ou inondent la bande passante ;
- d'introduire des programmes nuisibles (virus ou autres) ;
- d'effectuer des actes de piratage ou d'espionnage ;
- de modifier la configuration des machines ;
- d'utiliser, ou essayer d'utiliser, des comptes autres que le sien ou de masquer sa véritable identité.

L'utilisateur doit aussi protéger l'accès au matériel informatique (PC, PC Portable, etc.) qui lui est affecté. Il doit fermer les sessions ouvertes à son nom avant de quitter les lieux, ou activer la mise en veille automatique (protégée par mot de passe) après une courte période d'inactivité.

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

Le Comité de Pilotage du HCP, désigné par le Haut Commissaire au Plan, est chargé de faire :

- Etablir un plan d'action annuel par chaque direction centrale ou régionale du HCP en conformité avec les dispositions de cette charte, tout en inventoriant les incidents et risques encourus et indiquant les mesures à prendre ;
- Assurer le suivi de la mise en œuvre de cette politique de sécurité du SI du HCP par un comité de pilotage afin de :
    a. Etudier les plans d'actions de chaque entité,
    b. Assurer une optimisation du SI du HCP à travers une convergence des politiques et outils de sécurité de ses sous-systèmes d'information (matériel et logiciels de sécurité, les moyens financiers et humains disponibles) ;
    c. Proposer des directives complémentaires tout en prenant en compte les dernières évolutions technologiques et les nouveautés réglementaires en la matière,
- Mettre à jour cette charte.

IV. Règles d'utilisation des outils informatiques

Les données et le patrimoine documentaire du HCP sont confidentiels et ont parfois un caractère très sensible. L'accès à certaines ressources informatiques (Bases de données, résultats des enquêtes

et études avant publication officielle, dossiers RH, …) est soumis à l'autorisation du Haut Commissaire au Plan.

De plus, Leur utilisation doit obéir aux règles suivantes :

IV.1. Matériels, Réseaux et production informatique

Les règles d'utilisation du matériel informatique sont présentées dans ce qui suit :

- L'utilisateur s'interdit de déplacer tout matériel informatique sans le contrôle et l'autorisation préalable écrite par le service concerné au sein de chaque Direction ;
- Toute réaffectation de matériel informatique et des logiciels correspondants doit obligatoirement s'opérer en coordination avec le service concerné ;
- Chaque utilisateur s'engage à prendre soin des matériels informatiques mis à sa disposition. Il informe le responsable l'entité informatique de toute anomalie constatée,
- Les activités risquant d'occuper fortement les ressources informatiques (impression de gros documents, utilisation intensive du réseau,...) devront être effectuées après concertation avec l'entité informatique aux moments qui pénalisent le moins le reste des utilisateurs.

IV.2. Accès aux ressources informatiques

- Chaque utilisateur ayant ouvert une session sur un PC, une station de travail, un portable ou un serveur doit obligatoirement la fermer avant de quitter les lieux (notamment au niveau des espaces ouverts). Si toutefois l'utilisateur compte s'absenter pour une courte durée sans fermer sa session, il est fortement conseillé de la verrouiller par un mot de passe ;
- L'accès au parc par les stagiaires et les visiteurs doit être placé sous le contrôle et la responsabilité de l'encadrant ;
- L'assignation des profils d'administrateurs est soumise à une étude et autorisée par le Haut-Commissaire au Plan ou son délégataire ;
- Les mots de passe utilisés par les administrateurs sont confidentiels et ne peuvent en aucun cas être divulgués ;
- L'accès des personnes étrangères aux locaux de l'entité informatique, ne peut se faire qu'en présence du personnel de cette entité,
- Chaque entité administrative doit veiller à contrôler l'accès aux locaux contenant des équipements informatiques mis à sa disposition.

IV.3. Logiciels applicatifs, progiciels et bureautique

IV.3.1. Détention et installation de logiciels

- L'installation de logiciels de production bureautique est du ressort exclusif du personnel de l'entité informatique de chaque direction ;
- L'installation des logiciels spécifiques doit se faire sous la supervision du personnel de l'entité informatique de chaque direction ;

- Les utilisateurs sont tenus de signaler tout problème pouvant nuire à la sécurité du système informatique (mauvaise gestion des protections, faille système, logiciel suspect, …).

IV.3.2. Progiciels et logiciels applicatifs

Les utilisateurs doivent :

- Respecter les consignes communiquées par les responsables des progiciels ou logiciels installés ;
- S'interdire d'installer ou d'utiliser un logiciel à des fins non conformes aux missions du HCP ;
- Assumer leur responsabilité totale par rapport à l'intégrité des données gérées par le logiciel.

Les utilisateurs s'interdisent :

- d'installer des logiciels et outils autres que ceux mis en œuvre par le (HCP) ;
- de modifier les logiciels mis en place ;
- d'installer des logiciels susceptibles de modifier la configuration des machines ;
- d'effectuer toute opération pouvant nuire au bon fonctionnement du système (supprimer des répertoires ou fichiers nécessaires au fonctionnement d'un logiciel, changement d'adresses IP, …).

IV.4. Messagerie électronique et services Google Apps

L'utilisateur doit faire usage de la messagerie électronique du HCP dans le cadre exclusif de ses activités professionnelles dans le respect de 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 interdit de lire ou de prendre connaissance de tout message électronique appartenant ou destiné à une autre personne ;
- Ne doit pas se connecter ou essayer de se connecter sur un serveur que par les dispositions prévues ;
- Ne doit pas se livrer à des actions mettant en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Ne doit pas s'approprier l'identité d'une autre personne et il ne doit pas intercepter des communications entre tiers ;
- Ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,

- Doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques ;

- Doit éviter de faire circuler des messages e-mails non professionnelles ou portant atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par les messages comportant des images provocantes ou à caractère injurieux, raciste, …

- Pour éviter la saturation du réseau par les messages inutiles, l'utilisateur doit s'abstenir d'envoyer des messages non directement liés à sa fonction et doit limiter la liste des destinataires aux utilisateurs directement concernés par ce message.

Il est à noter que dans le cadre de l'utilisation des services Google Apps /HCP

- Votre compte Google Apps vous permet d'accéder à la plupart des produits Google en utilisant l'adresse e-mail qui vous est attribuée par l'administrateur @hcp.ma .
- L'administrateur @hcp.ma peut accéder à toutes les données que vous stockez dans ce compte, y compris à vos e-mails selon l'Avis de confidentialité de Google Apps.
- L'administrateur de domaine @hcp.ma est en mesure de désactiver certains services ou limiter votre capacité à déplacer des données vers ou depuis votre compte professionnel.
- Si vous accédez à des produits Google avec une adresse e-mail qui vous est attribuée par un administrateur@hcp.ma, votre contrat ou votre accord juridique avec celui-ci peut avoir un impact sur les points suivants :
    - Le détenteur des données ou du contenu que vous envoyez ou que vous téléchargez via votre compte
    - Les conditions dans lesquelles vous pouvez accéder à votre compte ou les moments où il peut être désactivé
    - Les personnes habilitées à accéder à votre compte ou à en supprimer les données
    - Votre compte est actuellement géré par un administrateur au Centre National de Documentation (HCP) pour domaine @hcp.ma .

IV.5. Utilisation d'internet

Les agents, explicitement autorisés, ont accès à Internet. L'usager l'utilise dans un cadre professionnel et à titre d'information personnelle.

Les règles d'utilisation en vigueur sont :

- L'usage du réseau Internet est réservé à des activités répondant aux exigences professionnelles. Sont interdits en particulier la consultation des sites pornographiques, les sites présentant toute forme cynique (crime, racisme, ...), les sites appelant à la haine raciale, les sites de conversations et d'une manière générale tout site qui s'oppose aux principes moraux et à l'opinion commune,

- Les données publiées sur le net doivent être obtenues licitement sans porter atteinte au droit tiers et sans impliquer le HCP dans des poursuites judiciaires ;

- Ne pas fournir des informations personnelles liées au HCP, comme l'adresse Email, lors de l'accès à des sites à des fins personnelles ou créer des comptes de téléchargement d'applications sans l'autorisation du responsable informatique ;
- Ne pas utiliser abusivement Internet quand l'accès n'est pas purement professionnel ;
- Il est formellement interdit d'utiliser l'accès donné à Internet par le HCP pour porter atteinte, par n'importe quel moyen, à toute autre institution ou tiers notamment à son patrimoine informationnel et/ou physique ;
- Ne pas ouvrir de liens inconnus et dont le contenu n'est pas sûr ;
- Ne pas télécharger ni installer les données douteuses.

V. Activités interdites

- Violer des droits (copyright, propriété intellectuelle, ...) de toute personne physique ou morale notamment la distribution ou l'installation des versions "piratées" de tout produit distribué sous format électronique (logiciel, musique, magazine, ouvrage, …) soumis à des droits de licence d'utilisation que le HCP n'a pas acquis ;
- Introduire des codes malicieux (virus, vers, cheval de Troie, e-mail bombs, ...) sur l'infrastructure réseau du HCP ;
- Dévoiler, partager ou rendre accessible l'identité électronique (compte et mot de passe) d'autres utilisateurs,
- Inscrire les mots de passe sur un papier ou dans un fichier en claire (non crypté),
- Utiliser des ressources informatiques et des services réseau du HCP pour transmettre des documents dont la circulation est en contradiction avec les lois en vigueur ou pouvant porter préjudice à autrui,
- Utiliser tout programme, script, commande ou envoi de messages dans le but d'interférer ou désactiver les sessions des utilisateurs via le réseau local ou Internet,
- Divulguer des informations sur tout ou une partie du réseau du HCP qui risquerait de compromettre la sécurité du système d'information.

VI.Règles générales

VI.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.

VI.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.

VII. Engagement et acceptation

Tout agent du HCP ou utilisateur 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)

- ☐ Agent titulaire du HCP
- ☐ Agent temporaire ou stagiaire au HCP
- ☐ Prestataire externe, travaillant pour l'employeur ……

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

Fait à ……, le …../……/……

(Signature)