Charte d'utilisation des ressources informatiques de *WELCOME*

Cette Charte graphique doit être annexée
au Règlement intérieur de WELCOME

INTRODUCTION

WELCOME met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Il met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de WELCOME. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de la société.

Cette Charte informatique comporte deux annexes :

- Les dispositions légales applicables
- Quelques astuces de cybersécurité proposées par le GHR

PROTECTION DES DONNEES A CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés et le Règlement général de Protection des données en vigueur le 25 mai 2018 définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.
WELCOME désigné un correspondant à la protection des données à caractère personnel. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.
Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.
Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de WELCOME au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande**.** Elle est également diffusée sur l'intranet de *WELCOME***.**
Le correspondant veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition).

LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de WELCOME pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service. .

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet. Elle est systématiquement remise à tout nouvel arrivant.
Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Quelques définitions :

On désignera sous le terme « **utilisateur »** toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de *WELCOME* et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....
Cette Charte informatique ne concerne cependant pas l'usage des outils informatiques mis à disposition par *WELCOME* aux clients. Un autre document pourra être spécifiquement communiqué à ces utilisateurs spécifiques.
Les termes "**outils informatiques et de communication**" recouvrent tous les équipements informatiques, de télécommunications et de reprographie de *WELCOME*.

LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION DE *WELCOME*

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par *WELCOME*.

1. Les modalités d'intervention du service de l'informatique interne

WELCOME assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication par *un service interne*. Ces agents/personnels disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.
Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.
Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

2. L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte (identifiant) fourni à l'utilisateur lors de son arrivée à/chez WELCOME. Un mot de passe personnel est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels.
Le mot de passe doit être composé de 12 caractères minimum combinant chiffres, lettres et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement et à chaque événement critique de sécurité (hacking, phishing…).
Dans le cadre d'une adresse nominative (ou faisant office) : le mot de passe doit être changé par défaut tous les 6 mois minimum.
Dans le cadre d'une adresse générique partagée entre plusieurs collaborateurs : le mot de passe doit être changé par défaut tous les 3 mois.
Dans le cadre d'une adresse générique transmise à chaque collaborateur gérant ce service : le mot de passe doit être changé par défaut tous les 3 mois mais également à chaque nouveau collaborateur.

3. Les règles de sécurité

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne de *WELCOME* toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.

- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés d*e WELCOME* .
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute utilisation d'un support numérique externe (disque dur, clé USB ect…) est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par *WELCOME* dans ce document.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de *WELCOME* sans l'accord préalable de la société.
Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre WELCOME et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

Voir l'Annexe 2 de cette Charte informatique sur la sensibilisation à la cybersécurité.

LES MOYENS INFORMATIQUES

1. Configuration du poste de travail

WELCOME met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. L''utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord du responsable informatique.

2. Equipements nomades et procédures spécifiques aux matériels de prêt.

Equipements nomades

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc.. ..).
Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.
Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, cet ordinateur doit être physiquement attaché à l'aide de l'antivol prévu à cet effet (sauf quand l'utilisateur est physiquement présent dans son bureau).
L'utilisation de smartphones ou BlackBerry pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils

doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

3. Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

4. Usage de l'intelligence artificielle générative

*WELCOME t*olère l'usage de l'intelligence artificielle générative sous les conditions suivantes :

- uniquement pour un **usage professionnel et en lien avec le poste** occupé par l'agent ;
- Et uniquement pour des raisons linguistique et/ou pour fournir une aide à la rédaction de documents (Rédaction de mail, Rédaction de compte-rendu ect…)
- Avec une **interdiction formelle** de donner à l'intelligence artificielle générative :
    - Des données personnelles,
    - Des informations sensibles sur l'activité de la société,
    - Des éléments de propriété intellectuelle.

5. Messagerie électronique

Conditions d'utilisation

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de *WELCOME*.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

WELCOME s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'agent.

Consultation de la messagerie

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, le service informatique interne de *WELCOME* peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf conditions d'utilisation).

Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un agent (longue maladie), le chef de service peut demander au service informatique, après accord de son directeur, le transfert des messages reçus.

Courriel non sollicité

WELCOME Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel. Les utilisateurs ne cliqueront pas sur des liens provenant de mail tant que le destinataire n'est pas considéré comme fiable par l'un des responsable du SI

6. Téléphone

WELCOME met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.
Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.
WELCOME s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.
WELCOME s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service informatique ou administratif, WELCOME se réserve le droit d'accéder aux numéros complets des relevés individuels.

L'ADMINISTRATION DU SYSTEME D'INFORMATION
Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de la Commission, différents dispositifs sont mis en place.

1. Les systèmes automatiques de filtrage
A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour la WELCOME et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée....).

2. Les systèmes automatiques de traçabilité
Le service informatique de la WELCOME opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.
Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement.
Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de trois mois.

3. Gestion du poste de travail
A des fins de maintenance informatique, le service informatique interne de *WELCOME* peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.
Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR
Lors de son départ, l'utilisateur doit restituer au service de l'informatique interne les matériels mis à sa disposition.
Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le chef de service.
Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

Concernant les adresses mails génériques, l'ensemble des échanges seront disponibles aux utilisateurs suivants. Les utilisateurs partants doivent donc s'assurer d'avoir effacé tous les échanges personnels et au bon classement des échanges dans les dossiers correspondants.

RESPONSABILITES- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre. Des sanctions en interne peuvent être prononcées, elles consistent :

- dans un premier temps, en un rappel à l'ordre émanant du service informatique ou administratif interne, après avis du directeur de *WELCOME* , en cas de non-respect des règles énoncées par la charte ;

- dans un second temps, et en cas de renouvellement, après *WELCOME* et du supérieur hiérarchique de l'agent, en des sanctions disciplinaires adoptées après saisine du comité consultatif paritaire restreint.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

ANNEXE 1

DISPOSITIONS LEGALES APPLICABLES

Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiées par la loi n°2004-801 du 6 août 2004.

Dispositions Pénales :

- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.

Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.

Disposition pénale : art L.335-2 du Code pénal.

ANNEXE 2

LA SECURITE DES OBJETS CONNECTES

1. **Bien choisir les mots de passe**

Un mot de passe doit comporter au moins 12 caractères avec des majuscules, des minuscules, des chiffres et si possible un caractère non-alphanumérique. Autant que possible il faut un mot de passe par utilisateur (et non pas uniquement par type de poste), et le changer régulièrement (2 fois par an) et au départ de la personne. Il faut également un mot de passe par type de connexion (pas le même pour le logiciel X et le réseau social !) Parmi les mots de passe les plus importants, **celui de la boite mail est le plus sensible**.

2. **Verrouiller les objets connectés**

Ordinateurs fixes ou portables, tablettes ou smartphones doivent être verrouillés manuellement dès que la personne qui l'utilise s'en éloigne. Pour s'assurer que ce verrouillage est effectué automatiquement, ces outils peuvent être paramétrés :

- 5 minutes sans activité pour un ordinateur fixe ;
- 5 minutes sans activité pour un ordinateur portable ou une tablette ;
- 3 minutes sans activité pour un smartphone.

3. **Bien entretenir son système informatique**

Mettre régulièrement à jour les logiciels car des corrections sont apportées régulièrement aux failles de sécurité.

4. **Régulièrement effectuer des sauvegardes des données**

ET s'assurer qu'elles fonctionnent en les restaurant de temps en temps. Enfin toute nouvelle connexion, par exemple avec une clef USB, doit être analysée avec un anti-virus.

5. **Sécuriser ses objets connectés**

Un smartphone, une tablette, un ordinateur portable doivent être autant protégés qu'un ordinateur fixe. A minima **paramétrer un verrouillage automatique avec demande de mot de passe.** De même **un antivirus et un pare-feu** sont des éléments essentiels pour ces mini-ordinateurs qui comportent directement ou indirectement de nombreuses données confidentielles.

6. **Etre vigilent lors de l'utilisation de la messagerie**

Vérifier les expéditeurs, ne pas ouvrir les pièces jointes ou cliquer sur les liens automatiquement sans s'assurer du contenu. En cas de doute sur un mail reçu demandant des informations, chercher à joindre l'expéditeur pour s'assurer de la véracité du mail.

7. **Limiter les discussions d'éléments confidentiels dans les espaces publics**

Les établissements HCR sont des lieux recevant du public. Dans les espaces communs, les collaborateurs doivent veiller à ne pas évoquer des éléments confidentiels.

8. **Séparer les usages personnels et professionnels**

Ne pas avoir un seul téléphone, une messagerie personnelle avec toutes les redirections des autres adresses mails professionnelles (ou inversement), ne pas connecter automatiquement les comptes personnels sur un outil (téléphone, ordinateur) professionnel…