CHARTE INFORMATIQUE

Utilisation des Systèmes d'Information

Version 1.0 **Siba KOIVOGUI** **OPSIE M2 Lyon 2**

NOTE D'UTILISATION

Ce modèle de charte est à adapter au nom et contexte de la structure. Elle doit être signée par chaque utilisateur (salarié, agent, bénévole, stagiaire) avant tout accès aux systèmes d'information. Conserver l'exemplaire signé dans le dossier individuel. Mise à jour recommandée : annuelle ou après tout incident significatif.

PAGE D'EN-TÊTE — À COMPLÉTER

CHARTE D'UTILISATION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

[NOM DE LA STRUCTURE] **[Adresse — Ville]**

Applicable à compter du	**[DATE D'ENTRÉE EN VIGUEUR]**
Version	**1.0**
Approuvée par	**[NOM DU DIRIGEANT / DG / PRÉSIDENT]**

PRÉAMBULE

[NOM DE LA STRUCTURE] met à la disposition de ses collaborateurs, agents, bénévoles et stagiaires des outils informatiques et des accès à des systèmes d'information dans le cadre de l'exercice de leurs fonctions.

Ces outils constituent des ressources professionnelles dont l'utilisation doit respecter les règles légales et les politiques internes de la structure. La présente charte définit les règles d'utilisation acceptable de ces ressources et les responsabilités de chaque utilisateur.

Elle s'inscrit dans le cadre : - Du Règlement Général sur la Protection des Données (RGPD — UE 2016/679) - De la loi Informatique et Libertés (loi n° 78-17 modifiée) - Du Code du travail

(ou statut de la fonction publique territoriale) - Des recommandations de l'ANSSI en matière de sécurité informatique

Le non-respect de cette charte peut entraîner des sanctions disciplinaires et, le cas échéant, des poursuites judiciaires.

ARTICLE 1 — CHAMP D'APPLICATION

La présente charte s'applique à toute personne ayant accès aux systèmes d'information de **[NOM DE LA STRUCTURE]**, notamment :

- Les salariés (CDI, CDD, temps partiel)
- Les agents titulaires et contractuels (collectivités)
- Les stagiaires et apprentis
- Les bénévoles disposant d'un accès informatique
- Les prestataires et intervenants extérieurs (pour la durée de leur mission)

Les systèmes d'information concernés comprennent : - Les postes de travail fixes et portables - Les équipements mobiles (smartphones, tablettes professionnels) - Le réseau informatique et les accès Internet - La messagerie électronique professionnelle - Les applications métier et logiciels - Les espaces de stockage (serveurs, cloud, disques partagés) - Les imprimantes et scanners connectés

ARTICLE 2 — ACCÈS AUX SYSTÈMES D'INFORMATION

2.1 Comptes utilisateurs

• Chaque utilisateur dispose d'un compte nominatif personnel. • Les identifiants et mots de passe sont strictement personnels et confidentiels. Ils ne doivent jamais être communiqués à un tiers, y compris un supérieur hiérarchique ou un technicien informatique. • En cas de suspicion de compromission du compte, l'utilisateur doit le signaler immédiatement à **[RESPONSABLE INFORMATIQUE / RSSI]**.

2.2 Règles de gestion des mots de passe

• Longueur minimale : **[12 / 14]** caractères • Composition : majuscules, minuscules, chiffres et caractères spéciaux • Interdiction d'utiliser : prénom, date de naissance, nom de la structure • Renouvellement obligatoire tous les **[90 / 180]** jours • Utilisation d'un gestionnaire de mots de passe recommandée **[ex : Bitwarden, KeePass]** • Interdiction de réutiliser un mot de passe sur plusieurs services

2.3 Authentification renforcée

• L'authentification à deux facteurs (MFA) est obligatoire pour : [lister les systèmes : VPN, messagerie, ERP, accès distants…] • L'utilisateur doit conserver en sécurité son second facteur (code SMS, application d'authentification, clé physique).

2.4 Verrouillage des postes

• Tout poste de travail doit être verrouillé lors d'une absence, même de courte durée (raccourci Windows + L ou Cmd + Ctrl + Q sur Mac). • Le verrouillage automatique est configuré à **[5 / 10]** minutes d'inactivité.

ARTICLE 3 — UTILISATION DES RESSOURCES INFORMATIQUES

3.1 Usage professionnel

Les ressources informatiques sont mises à disposition à des fins professionnelles. Une utilisation personnelle raisonnable est tolérée dans les conditions suivantes : • En dehors des heures de travail (ou pauses) • Sans impact sur les performances du système • Dans le respect des lois en vigueur et de la présente charte

Sont strictement interdits : ✖ Stocker des fichiers personnels volumineux sur les serveurs partagés ✖ Installer des logiciels non autorisés sur les postes professionnels ✖ Accéder à des contenus illicites (piratage, contenu illégal) ✖ Utiliser les ressources à des fins commerciales personnelles

3.2 Messagerie électronique

• La messagerie professionnelle est réservée aux échanges professionnels. • L'utilisateur est responsable des courriels envoyés depuis son compte. • Règles de vigilance obligatoires : → Ne jamais ouvrir une pièce jointe inattendue sans vérification → Ne jamais cliquer sur un lien suspect sans validation → Signaler tout courriel suspect à **[CONTACT SÉCURITÉ]** → Ne pas transférer de données confidentielles par messagerie non chiffrée vers des adresses externes

3.3 Internet et réseaux sociaux

• La navigation Internet depuis les postes professionnels est tracée. • Sont interdits : ✖ Le téléchargement de logiciels ou fichiers non autorisés ✖ L'utilisation de services de partage de fichiers non approuvés ✖ La connexion à des réseaux Wi-Fi publics sans VPN ✖ La publication d'informations confidentielles de la structure sur des réseaux sociaux ou forums publics

3.4 Supports amovibles

• L'utilisation de clés USB ou disques externes personnels est [interdite / soumise à autorisation préalable]. • Tout support amovible fourni par la structure doit être chiffré. • En cas de perte ou vol d'un support contenant des données professionnelles, le signalement immédiat est obligatoire.

ARTICLE 4 — PROTECTION DES DONNÉES PERSONNELLES (RGPD)

4.1 Obligations générales

• Tout utilisateur traitant des données personnelles agit en tant que mandataire de la structure et engage sa responsabilité personnelle. • Les principes suivants doivent être respectés : → Finalité : utiliser les données uniquement pour l'objectif déclaré → Minimisation : ne collecter que ce qui est strictement nécessaire → Confidentialité : ne pas divulguer les données à des tiers non autorisés → Durée de conservation : respecter les durées définies dans le registre

4.2 Données sensibles

Les données sensibles (santé, opinions politiques, données d'enfants, informations bancaires...) font l'objet de précautions renforcées : → Accès restreint aux seules personnes habilitées → Transmission uniquement via des canaux sécurisés (chiffrement) → Interdiction de les stocker sur des supports non sécurisés

4.3 Droits des personnes concernées

En cas de demande d'exercice des droits (accès, rectification, effacement, opposition) formulée par une personne concernée, l'utilisateur doit : → Transmettre immédiatement la demande à **[RESPONSABLE RGPD / DPO]** → Ne pas traiter lui-même la demande sans coordination → Ne pas ignorer ou retarder la transmission

4.4 Interdictions spécifiques

✖ Envoyer des données personnelles sur des messageries non professionnelles (WhatsApp, Gmail personnel, Messenger...) ✖ Stocker des données personnelles sur des services cloud non approuvés (Google Drive personnel, Dropbox personnel...) ✖ Imprimer des données personnelles et laisser les impressions sans surveillance ✖ Communiquer des données de tiers à d'autres tiers sans base légale

ARTICLE 5 — TÉLÉTRAVAIL ET ACCÈS DISTANTS

5.1 Connexion à distance

• L'accès aux systèmes d'information depuis l'extérieur doit se faire exclusivement via [VPN fourni / solution approuvée par la structure]. • L'utilisation de connexions Wi-Fi publiques sans VPN est interdite. • L'utilisateur en télétravail est responsable de la sécurité physique de son poste de travail.

5.2 Environnement de travail

• Les écrans ne doivent pas être visibles par des tiers non autorisés. • Les documents confidentiels imprimés à domicile doivent être déchiquetés. • Les équipements professionnels ne doivent pas être utilisés par des membres de la famille ou des tiers.

ARTICLE 6 — SIGNALEMENT DES INCIDENTS

Tout utilisateur qui constate ou suspecte : ✔ Un accès non autorisé à son compte ou aux systèmes ✔ La perte ou le vol d'un équipement professionnel ✔ Un comportement anormal d'un système (ransomware, ralentissement...) ✔ La réception d'un courriel suspect (phishing) ✔ Une fuite ou divulgation accidentelle de données

DOIT IMMÉDIATEMENT contacter :

Responsable informatique / RSSI	**[NOM]** — **[TÉLÉPHONE]** — **[EMAIL]**
En cas d'indisponibilité	**[NOM SUPPLÉANT]** — **[TÉLÉPHONE]**
En dehors des heures ouvrées	**[PROCÉDURE D'ASTREINTE]**

⚠ En cas d'incident impliquant des données personnelles, la CNIL doit être notifiée dans les 72 heures. L'utilisateur NE DOIT PAS attendre pour signaler en interne.

Bon réflexe en cas de suspicion de ransomware : 1. NE PAS éteindre le poste 2. DÉBRANCHER le câble réseau immédiatement 3. APPELER le responsable informatique 4. NE PAS tenter de résoudre soi-même

ARTICLE 7 — CONFIDENTIALITÉ ET PROPRIÉTÉ INTELLECTUELLE

7.1 Confidentialité

• Les informations de la structure (données clients, contrats, stratégie, données financières) sont confidentielles. • L'obligation de confidentialité s'applique pendant et après la relation avec la structure. • Les informations ne doivent pas être divulguées à des tiers, même après départ de la structure, sans autorisation expresse.

7.2 Propriété intellectuelle

• Les créations réalisées dans le cadre professionnel appartiennent à la structure, sauf accord contraire. • L'utilisation de logiciels ou contenus protégés sans licence valide est interdite et engage la responsabilité de l'utilisateur.

ARTICLE 8 — CONTRÔLE ET SANCTIONS

8.1 Traçabilité et contrôle

La structure se réserve le droit de surveiller et journaliser : • Les connexions aux systèmes d'information (logs d'accès) • La messagerie professionnelle (en cas de procédure disciplinaire) • L'utilisation d'Internet (sites visités, volumes téléchargés) • Les opérations réalisées sur les données sensibles

Ces contrôles sont effectués dans le respect du cadre légal applicable et après information du Comité Social et Économique (CSE) le cas échéant.

8.2 Sanctions

Le non-respect de la présente charte peut entraîner : • Un avertissement oral ou écrit • Une sanction disciplinaire (avertissement, mise à pied, licenciement) • Des poursuites judiciaires en cas d'infraction pénale (accès frauduleux à un système — Art. 323-1 du Code pénal, violation du secret professionnel, atteinte à la vie privée)

8.3 Responsabilité

L'utilisateur est responsable des actions effectuées depuis son compte. En cas de partage de ses identifiants ayant conduit à un incident, sa responsabilité personnelle pourra être engagée.

ARTICLE 9 — ENTRÉE EN VIGUEUR ET RÉVISION

La présente charte entre en vigueur à compter de sa signature. Elle est remise à chaque nouvel utilisateur lors de son arrivée et doit être signée avant tout accès aux systèmes d'information.

Elle est révisée annuellement ou après tout incident significatif. Toute modification est portée à la connaissance des utilisateurs.

ATTESTATION DE PRISE DE CONNAISSANCE ET D'ENGAGEMENT

Je soussigné(e) :

Nom et Prénom : _____

Fonction / Rôle : _____

Structure : _____

Déclare avoir pris connaissance de la Charte d'Utilisation des Systèmes d'Information de **[NOM DE LA STRUCTURE]** dans sa version du **[DATE]**, en avoir compris les dispositions et m'engage à les respecter.

Je reconnais que : ✔ Mes identifiants sont personnels et ne seront jamais communiqués ✔ J'ai l'obligation de signaler tout incident ou suspicion d'incident ✔ Le non-respect de cette charte peut entraîner des sanctions

Fait à _____, le _____

Signature :

_____ **[Nom et Prénom]**

Pour la structure — Accusé de remise :

Remis par : _____ le _____

Fonction : _____

Signature :

_____

ANNEXE — CONTACTS UTILES EN CAS D'INCIDENT

Contact interne

Responsable informatique / RSSI	**[NOM]** — **[TÉL]** — **[EMAIL]**
Direction / DG	**[NOM]** — **[TÉL]** — **[EMAIL]**

Contacts externes

Cybermalveillance.gouv.fr Assistance en cas d'incident CERT-FR (ANSSI) cert.ssi.gouv.fr — urgences@ssi.gouv.fr CNIL cnil.fr — 01 53 73 22 22 Gendarmerie / Police 17 (urgence) ou commissariat local

FIN DE LA CHARTE