LANCEL
PARIS 1876

CHARTE CYBERSÉCURITÉ
LANCEL SOGEDI

---

1. Objet

La présente charte cybersécurité a pour objectif de définir les règles et bonnes pratiques permettant de protéger les systèmes d'information, les réseaux, les données et les utilisateurs de LANCEL SOGEDI.

Elle complète la Charte d'utilisation du système d'information et s'impose à toute personne accédant aux ressources numériques de la Société, y compris via le réseau Wi-Fi invité.

---

2. Principes généraux

La cybersécurité repose sur la responsabilité collective et individuelle de chaque utilisateur. Toute négligence peut exposer la Société à des risques majeurs : fuite de données, interruption d'activité, atteinte à l'image de marque.

Chaque utilisateur s'engage à adopter un comportement prudent, vigilant et conforme aux règles définies ci-après.

---

3. Accès réseau et Wi-Fi (siège et boutiques)

3.1 Réseaux Wi-Fi

La Société met à disposition :

- Un réseau Wi-Fi interne réservé aux collaborateurs et prestataires autorisés,
- Un réseau Wi-Fi invité (« Guest ») destiné aux visiteurs, partenaires ou clients.

Chaque réseau est logiquement séparé afin de garantir la sécurité du système d'information interne.

3.2 Conditions d'utilisation du Wi-Fi

Tout utilisateur du Wi-Fi s'engage à :

- Utiliser le réseau conformément à sa destination,
- Ne pas tenter d'accéder aux ressources internes depuis le réseau invité,
- Ne pas contourner les dispositifs de sécurité (filtrage, portail captif, authentification),

- Respecter les lois et règlements en vigueur.

Toute utilisation illicite, frauduleuse ou abusive du Wi-Fi est interdite.

3.3 Traçabilité

Les connexions aux réseaux Wi-Fi peuvent être journalisées à des fins de sécurité, de conformité légale et de prévention des abus.

---

4. Sécurité des équipements

Les équipements connectés au système d'information ou au Wi-Fi de la Société doivent :

- Être protégés par un mot de passe ou un mécanisme équivalent,
- Disposer de mises à jour de sécurité,
- Ne pas être volontairement compromis (root, jailbreak, logiciels malveillants).

Tout équipement jugé non conforme peut être exclu du réseau.

---

5. Phishing et menaces numériques

Les utilisateurs doivent faire preuve d'une vigilance particulière face :

- Aux courriels suspects,
- Aux liens ou pièces jointes inattendus,
- Aux demandes urgentes ou inhabituelles d'informations.

Toute tentative de phishing ou d'ingénierie sociale doit être signalée sans délai au service informatique.

---

6. Authentification et mots de passe

Les identifiants sont strictement personnels et confidentiels.

L'authentification multifacteur (MFA) est obligatoire lorsque la Société la met en place.

Il est interdit de partager ses identifiants ou de les réutiliser sur des services non professionnels.

---

7. Télétravail et mobilité

En situation de télétravail ou de mobilité, l'utilisateur doit :

- Utiliser les moyens de connexion sécurisés fournis par la Société,
- Éviter les réseaux Wi-Fi publics non sécurisés,

- Protéger les écrans contre les regards indiscrets,
- Signaler immédiatement toute perte ou vol de matériel.

---

8. Signalement des incidents

Tout incident de sécurité (virus, ransomware, accès suspect, perte de données, vol d'équipement) doit être signalé immédiatement au service informatique.

Un signalement rapide permet de limiter les impacts pour la Société et les utilisateurs.

---

9. Contrôles et sanctions

La Société se réserve le droit de mettre en œuvre des contrôles de sécurité et de suspendre l'accès au réseau en cas de non-respect de la présente charte.

Toute violation peut entraîner des sanctions disciplinaires et, le cas échéant, des poursuites judiciaires.

---

10. Accès aux chartes

La Charte d'utilisation du système d'information et la présente Charte cybersécurité sont mises à disposition des utilisateurs via des supports dématérialisés, notamment par QR code affiché dans les locaux et sur le portail Wi-Fi invité.

Fait à Paris, le 17/12/2025

Le Mandataire Social