# Politique de Sécurité des Systèmes d’Information (PSSI)

## 1. Préambule et champ d’application

La présente politique définit les principes et les règles encadrant la sécurité des systèmes d’information (SI) de l’organisation. Elle s’applique à l’ensemble des utilisateurs internes (collaborateurs, stagiaires) et externes (prestataires, sous-traitants) ayant accès aux ressources numériques de l’entreprise.

## 2. Engagement de la direction

La direction reconnaît que la sécurité des informations constitue un enjeu stratégique pour protéger les actifs de l’entreprise, garantir la continuité d’activité, et répondre aux exigences réglementaires et contractuelles. Elle s’engage à mettre en œuvre les moyens nécessaires à la bonne application de cette politique.

## 3. Principes généraux de sécurité

- Garantir la confidentialité, l’intégrité et la disponibilité des informations.
- Gérer les droits d’accès aux systèmes et aux données selon le principe du moindre privilège.
- Mettre en place des sauvegardes régulières et des solutions de restauration fiables.
- Protéger les postes de travail et équipements mobiles contre les logiciels malveillants.
- Journaliser les accès et opérations sensibles.
- Sensibiliser régulièrement les utilisateurs aux bonnes pratiques de sécurité.
- Contrôler l’accès physique aux locaux et aux équipements sensibles.

## 4. Règles de comportement attendues

- Ne jamais partager ses identifiants ou mots de passe.
- Verrouiller son poste en cas d’absence.
- Utiliser uniquement les outils et supports autorisés pour le traitement des données professionnelles.
- Signaler immédiatement tout incident ou comportement suspect au service informatique.
- Utiliser les ressources numériques de manière conforme et responsable.

## 5. Responsabilités

- La direction définit les objectifs et valide les moyens associés.
- Le DSI ou référent sécurité pilote la mise en œuvre des mesures techniques et organisationnelles.
- Les responsables métiers veillent au respect des règles dans leurs équipes.
- Le service RH prend en compte les aspects sécurité dans les processus RH (embauche, départ, sanctions).
- Chaque utilisateur est responsable de l’utilisation conforme des ressources mises à sa disposition.

## 6. Conformité et sanctions

Tout manquement à la présente politique pourra faire l’objet de sanctions disciplinaires, conformément au règlement intérieur et à la législation en vigueur. La sécurité est une responsabilité collective.

## 7. Mise à jour, diffusion et application

Cette politique est revue annuellement ou à l’occasion de tout changement majeur impactant la sécurité. Elle est diffusée via l’intranet, remise à chaque nouvel arrivant, et accessible à tout moment par les utilisateurs. Elle est approuvée par la direction générale.

Fait à [lieu], le [date]

Nom et signature de la direction : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_