Politique de Sécurité des Systèmes d'Information (PSSI)

1. Introduction

E1 : La présente Politique de Sécurité des Systèmes d'Information (PSSI) définit les règles et bonnes pratiques pour garantir la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'organisation.

E2 : Cette politique s'applique à l'ensemble des employés, prestataires et partenaires accédant aux systèmes d'information.

---

2. Gouvernance de la Sécurité

E3 : Un Responsable de la Sécurité des Systèmes d'Information (RSSI) est désigné pour piloter la mise en œuvre de la PSSI.

E4 : Une analyse des risques est réalisée périodiquement afin d'identifier les menaces pesant sur le SI.

E5 : Les incidents de sécurité doivent être signalés immédiatement au RSSI pour investigation et remédiation.

---

3. Gestion des Accès

E6 : L'accès aux systèmes d'information est accordé selon le principe du moindre privilège.

E7 : L'authentification multi-facteurs (MFA) est obligatoire pour les accès sensibles.

E8 : Tout compte inactif depuis plus de 90 jours est désactivé.

E9 : Les mots de passe doivent respecter un niveau de complexité défini (minimum 12 caractères, mélange de majuscules, minuscules, chiffres et caractères spéciaux).

---

4. Protection des Données

E10 : Les données sensibles doivent être chiffrées en transit et au repos.

E11 : Les sauvegardes des données critiques sont réalisées quotidiennement et testées régulièrement.

E12 : L'accès aux données personnelles est strictement restreint aux personnes autorisées.

---

5. Sécurité des Systèmes et Réseaux

E13 : Tout équipement connecté au réseau doit être à jour et disposer d'une protection antivirus.

E14 : Un pare-feu est mis en place pour filtrer le trafic réseau entrant et sortant.

E15 : L'usage de réseaux Wi-Fi publics pour accéder aux systèmes d'information est interdit sans VPN.

---

6. Sécurité Physique

E16 : L'accès aux locaux contenant des équipements critiques est restreint aux personnes autorisées.

E17 : Les supports de stockage amovibles (clés USB, disques durs externes) doivent être chiffrés et approuvés avant utilisation.

---

7. Sensibilisation et Conformité

E18 : Tous les utilisateurs doivent suivre une formation annuelle sur la cybersécurité.

E19 : Un audit de sécurité est réalisé au moins une fois par an pour vérifier la conformité à la PSSI.

E20 : Le non-respect de la PSSI peut entraîner des sanctions disciplinaires.

Cette politique doit être révisée et mise à jour annuellement.