Modèle PSSI — Politique de Sécurité du SI

Template personnalisable | Conforme ISO 27001:2022 | Ayi NEDJIMI Consultants

Organisation	*[Nom de votre entreprise]*
Version	*[1.0]*
Date d'approbation	*[JJ/MM/AAAA]*
Approuvé par	*[Direction Générale]*
Prochaine revue	*[JJ/MM/AAAA — annuelle]*
Classification	Interne

1. Objet et champ d'application

La présente Politique de Sécurité du Système d'Information (PSSI) définit les principes directeurs, les objectifs de sécurité et le cadre organisationnel mis en place par *[Entreprise]* pour protéger son patrimoine informationnel.

Elle s'applique à :

- L'ensemble des collaborateurs (CDI, CDD, stagiaires, alternants)
- Les prestataires et sous-traitants ayant accès au SI
- Tous les actifs informationnels (données, systèmes, réseaux, applications)
- Tous les sites et environnements (locaux, cloud, télétravail)

2. Engagement de la Direction

La Direction Générale de *[Entreprise]* s'engage à :

- Allouer les ressources nécessaires à la sécurité de l'information
- Soutenir l'amélioration continue du SMSI
- Promouvoir une culture de sécurité à tous les niveaux
- Respecter les exigences légales et réglementaires (NIS2, RGPD, DORA)

3. Objectifs de sécurité

- **Confidentialité** — Garantir que l'information n'est accessible qu'aux personnes autorisées
- **Intégrité** — Assurer l'exactitude et l'exhaustivité de l'information
- **Disponibilité** — Garantir l'accès à l'information en temps voulu
- **Traçabilité** — Permettre l'imputation des actions à leur auteur

4. Organisation de la sécurité

4.1 Rôles et responsabilités

- **Direction Générale** — Sponsor du SMSI, allocation des ressources
- **RSSI** — Pilotage opérationnel de la sécurité, reporting
- **DSI** — Mise en œuvre technique des contrôles

- **DPO** — Protection des données personnelles
- **Managers** — Application locale des politiques
- **Collaborateurs** — Respect des règles, signalement des incidents

4.2 Comité de sécurité

Un comité SSI se réunit *[trimestriellement]* pour :

- Revoir les indicateurs de sécurité
- Valider les plans d'action et les budgets
- Traiter les incidents majeurs
- Arbitrer les risques résiduels

5. Gestion des risques

L'organisation met en œuvre une démarche d'analyse de risques basée sur *[EBIOS RM / ISO 27005]*, comprenant :

- Identification et classification des actifs
- Analyse des menaces et vulnérabilités
- Évaluation des risques (probabilité × impact)
- Plan de traitement (réduction, transfert, acceptation, évitement)
- Revue périodique (au minimum annuelle)

6. Règles de sécurité

6.1 Contrôle d'accès

- Principe du moindre privilège appliqué systématiquement
- Authentification forte (MFA) obligatoire pour les accès sensibles
- Revue des droits d'accès trimestrielle
- Désactivation immédiate des comptes lors des départs

6.2 Protection des données

- Classification obligatoire (Public, Interne, Confidentiel, Secret)
- Chiffrement des données sensibles au repos et en transit
- Politique de rétention et de destruction sécurisée

6.3 Gestion des incidents

- Procédure de signalement obligatoire (< 4h pour les incidents critiques)
- Équipe de réponse identifiée et joignable 24/7
- Notification aux autorités selon NIS2 (< 24h alerte, < 72h rapport)
- Capitalisation systématique (lessons learned)

6.4 Continuité d'activité

- PCA/PRA documenté et testé annuellement
- Sauvegardes 3-2-1 vérifiées mensuellement
- RTO/RPO définis par processus métier

7. Sensibilisation et formation

- Formation à l'intégration pour tous les nouveaux arrivants
- Campagnes de sensibilisation trimestrielles (phishing, etc.)
- Formation technique annuelle pour les équipes IT

8. Conformité et contrôle

- Audit interne annuel du SMSI
- Tests d'intrusion annuels (périmètre défini)
- Veille réglementaire continue (NIS2, RGPD, sectorielle)
- Sanctions en cas de non-respect (processus disciplinaire)

9. Revue et amélioration continue

Cette politique est révisée au minimum une fois par an ou lors de changements significatifs (nouvelle réglementation, incident majeur, évolution du périmètre).

> **Note :** Ce modèle est un point de départ. Il doit être adapté à votre contexte, votre taille et votre secteur d'activité. Un accompagnement expert garantit une PSSI opérationnelle et conforme.