POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION

[NOM DE L'ENTREPRISE]

[Secteur d'activité] — [Ville]

Version	[X.X]
Date de création	[JJ/MM/AAAA]
Dernière mise à jour	[JJ/MM/AAAA]
Rédacteur	[Prénom NOM], [Titre]
Approbateur	[Prénom NOM], Direction générale
Classification	CONFIDENTIEL — Diffusion restreinte

Sommaire

(Mettre à jour via Word : Références > Mettre à jour la table)

1. Objet et domaine d'application

La présente Politique de Sécurité du Système d'Information (PSSI) constitue le document fondateur de la démarche de sécurité de [Nom de l'entreprise]. Elle traduit les orientations stratégiques de la direction en matière de protection du système d'information et fixe les règles que l'ensemble des parties prenantes s'engagent à respecter.

Les informations que [Nom de l'entreprise] traite, stocke et transmet constituent un actif stratégique à part entière. Les systèmes d'information qui les supportent sont exposés à une gamme étendue de menaces : accidents techniques, erreurs humaines, actes malveillants internes ou externes. Ces menaces ne sont pas statiques ; elles évoluent en permanence en sophistication et en volume, tandis que les systèmes eux-mêmes gagnent en complexité, en ouverture et en interdépendance. Chaque nouveau besoin de connectivité, chaque projet de transformation numérique, chaque prestataire intégré au périmètre élargit mécaniquement la surface d'exposition.

Le domaine d'application couvre l'ensemble du système d'information de [Nom de l'entreprise] : ses matériels, ses logiciels, ses données, ses réseaux et ses locaux, qu'ils soient hébergés en propre ou confiés à des tiers. Elle s'impose à tous les utilisateurs du SI — collaborateurs permanents, stagiaires et alternants, mais aussi prestataires et sous-traitants ayant accès, même ponctuellement, aux ressources de l'entreprise.

2. Cadre réglementaire et normatif

La présente PSSI s'inscrit dans un ensemble de référentiels dont [Nom de l'entreprise] s'inspire pour structurer sa démarche. Sans prétendre à une certification immédiate, l'organisation aligne ses pratiques sur les normes ISO/IEC 27001:2022 et ISO/IEC 27002:2022, qui constituent aujourd'hui la référence internationale en matière de management de la sécurité de l'information.

Sur le plan réglementaire, le Règlement Général sur la Protection des Données (RGPD, UE 2016/679) impose des obligations directes en matière de protection des données personnelles traitées par l'organisation. La directive NIS 2, transposée en droit national, renforce les exigences de cybersécurité pour un nombre croissant d'entités. Les recommandations de l'ANSSI, notamment son guide PSSI à destination des PME et ETI, ont par ailleurs guidé la structuration du présent document.