#

#

#

# POLITIQUE DE SÉCURITÉ INFORMATIQUE

##

##

## Politique de sécurité du système d'information

[Nom de l’entreprise]
[Adresse] — [Téléphone] — [Email]

*Ce document définit le cadre de gestion de la sécurité informatique au sein de l’entreprise. Il fixe les principes, responsabilités et règles permettant de protéger les systèmes d’information, les données et les utilisateurs. Il doit être adapté en fonction des réalités organisationnelles, juridiques et techniques de chaque structure.*

## Tableau de suivi des versions

| **Version** | **Date** | **Modifications apportées** | **Validé par** |
| --- | --- | --- | --- |
| 1.0 | [Date] | Création du document | [Nom du valideur] |

##

## Contexte réglementaire

Dans un contexte de digitalisation croissante et de menaces cyber de plus en plus sophistiquées, la mise en place d’une politique de sécurité informatique est une obligation stratégique et réglementaire. L’article 32 du RGPD impose notamment aux responsables de traitement de mettre en œuvre des mesures de sécurité appropriées. De plus, l’ANSSI recommande des dispositifs adaptés à la taille, aux risques et aux enjeux propres à chaque organisation. Cette politique s’inscrit dans cette logique de conformité et de protection proactive.

## 1. Objectifs de la politique

L’objectif principal de cette politique est de garantir la **confidentialité**, l’**intégrité** et la **disponibilité** des systèmes d'information et des données de [Nom de l’entreprise]. Elle permet de réduire les risques liés à l’utilisation des technologies numériques, qu’ils soient d’origine humaine (erreurs, négligences), technique (panne, faille) ou malveillante (intrusion, vol, fraude). Elle fixe un cadre clair pour responsabiliser les collaborateurs, harmoniser les pratiques et anticiper les crises potentielles.

## 2. Champ d’application

Cette politique s’applique à l’ensemble des utilisateurs internes et externes qui accèdent ou manipulent les ressources informatiques de l’entreprise. Sont concernés :

* Les employés, quelle que soit leur fonction ou ancienneté
* Les sous-traitants et prestataires techniques
* Les partenaires accédant aux systèmes via des interfaces dédiées
* Les équipements informatiques (ordinateurs, serveurs, smartphones, imprimantes)
* Les infrastructures réseau (LAN, VPN, Wi-Fi…)
* Les données, systèmes applicatifs et plateformes cloud utilisés dans le cadre professionnel

## 3. Rôles et responsabilités

La sécurité informatique est une responsabilité partagée. Sa mise en œuvre repose sur une gouvernance claire :

* **Le Responsable de la Sécurité des Systèmes d’Information (RSSI)** définit la politique, coordonne les actions, pilote les audits et veille à la conformité.
* **La Direction des Systèmes d’Information (DSI)** applique les mesures techniques, supervise les infrastructures et intervient en cas d’incident.
* **Les managers** sont garants de l’application des règles par leurs équipes et relais des messages de sensibilisation.
* **Chaque utilisateur** est responsable de ses actes numériques et doit signaler toute situation suspecte.

## 4. Contrôle des accès

L'accès aux ressources informatiques doit être strictement encadré selon le principe du **moindre privilège**. Cela implique :

* L’attribution des droits en fonction des besoins réels des utilisateurs
* L’utilisation d’identifiants nominatifs et de mots de passe robustes
* La mise en place d’une authentification à deux facteurs (MFA) sur les accès sensibles
* La désactivation immédiate des comptes inactifs ou en cas de départ d’un collaborateur

Des journaux de connexion sont conservés à des fins de traçabilité et d’analyse en cas d’incident.

## 5. Protection des équipements

Les équipements informatiques, qu’ils soient fixes ou mobiles, doivent être sécurisés pour éviter toute compromission :

* Installation et mise à jour régulière d’un antivirus et d’un pare-feu
* Chiffrement des disques durs des ordinateurs portables et mobiles
* Blocage des ports USB non autorisés
* Mises à jour automatiques des systèmes d’exploitation et logiciels installés

Toute connexion d’un matériel personnel (BYOD) doit être validée par la DSI.

## 6. Sécurité des données

La protection des données, notamment à caractère personnel ou stratégique, est une priorité :

* Des **sauvegardes automatiques et chiffrées** sont effectuées quotidiennement
* Les données sensibles sont stockées sur des serveurs sécurisés, avec accès restreint
* Toute transmission externe (email, cloud, transfert) est soumise à des règles strictes
* La conservation des données est limitée dans le temps et encadrée par des procédures de suppression sécurisée

L’ensemble est conforme aux exigences du RGPD et aux engagements contractuels de l’entreprise.

## 7. Utilisation acceptable

L’usage des outils informatiques mis à disposition doit rester professionnel, responsable et conforme à la présente politique :

* Il est interdit d’installer des logiciels non validés par la DSI
* Le téléchargement de contenus illégaux ou non professionnels est prohibé
* Les e-mails doivent être traités avec précaution (attention aux pièces jointes douteuses)
* La navigation sur internet doit respecter les règles éthiques et sécuritaires

Les comportements à risque peuvent entraîner des mesures disciplinaires.

## 8. Gestion des incidents

Un **incident de sécurité informatique** est tout événement susceptible de compromettre la sécurité des systèmes (ex. : perte d’équipement, virus, fuite de données).

* Tout incident doit être signalé immédiatement au RSSI ou à la DSI
* Un **plan de réponse** est déclenché : analyse, containment, remédiation, communication
* Si nécessaire, l’entreprise notifie l’incident aux autorités compétentes (CNIL, clients…)
* Un retour d’expérience est documenté pour éviter toute récurrence

La réactivité est essentielle pour limiter les impacts.

## 9. Sensibilisation et formation

Les utilisateurs sont la première ligne de défense. La sécurité passe donc par la **connaissance des bonnes pratiques** :

* Une formation cybersécurité est intégrée au parcours d’onboarding
* Des sessions annuelles de rappel sont organisées, en présentiel ou e-learning
* Des campagnes de faux phishing sont menées pour tester la vigilance
* Des supports de type fiches pratiques sont mis à disposition

La sensibilisation est une démarche continue.

## 10. Suivi et révision

Cette politique est un document **vivant** : elle est révisée chaque année, ou plus fréquemment en cas :

* d’incident majeur
* de modification réglementaire
* de changement d’organisation ou d’infrastructure

Un rapport annuel de conformité est transmis à la direction. Des audits internes ou externes peuvent être réalisés à tout moment.

## Approbation

Nom : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Fonction : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_