[INSÉRER LOGO DE L'ENTREPRISE]

POLITIQUE DE SÉCURITÉ INFORMATIQUE

[NOM DE L'ENTREPRISE]

Version	1.0
Date d'entrée en vigueur	[DATE D'ENTRÉE EN VIGUEUR]
Date de révision prévue	[DATE DE RÉVISION]
Responsable du document	[NOM ET FONCTION DU RESPONSABLE]
Approbateur	[NOM ET FONCTION DE L'APPROBATEUR]
Classification	Document confidentiel interne

Ce document constitue la politique officielle de sécurité informatique de [NOM DE L'ENTREPRISE]. Tout collaborateur, prestataire ou partenaire ayant accès aux systèmes d'information de l'entreprise est tenu de la respecter. Source : ia-cyber-securite.fr

SOMMAIRE

SOMMAIRE 2
Article 1 - Préambule et objectifs 5
1.1 Contexte réglementaire 5
1.2 Objectifs de la politique 5
1.3 Engagement de la direction 5
1.4 Sanctions en cas de non-respect 5
Article 2 - Périmètre d'application 6
2.1 Personnes concernées 6
2.2 Systèmes couverts 6
2.3 Sites géographiques 6
Article 3 - Classification des informations et des actifs 7
3.1 Niveaux de classification 7
3.2 Règles de manipulation et de destruction 8
3.3 Inventaire des actifs informatiques 8
Article 4 - Gestion des accès et des identités (IAM) 8
4.1 Principe du moindre privilège 8
4.2 Procédures de gestion des comptes 9
4.3 Gestion des comptes administrateurs 9
4.4 Revue périodique des droits d'accès 9
4.5 Modèle de matrice des accès par rôle 10
Article 5 - Politique des mots de passe et authentification 10
5.1 Règles de complexité des mots de passe 10
5.2 Authentification multifacteur (MFA) 11
5.3 Gestionnaire de mots de passe 11
5.4 Règles d'usage 11
Article 6 - Sécurité des postes de travail et appareils mobiles 12
6.1 Configuration minimale requise 12
6.2 Politique BYOD (Bring Your Own Device) 12
6.3 Procédure en cas de perte ou de vol 12
Article 7 - Sécurité des accès distants et du télétravail 13
7.1 Obligation du VPN 13
7.2 Règles d'utilisation des réseaux Wi-Fi 13
7.3 Règles de confidentialité en espace public 13
7.4 Équipements autorisés pour le télétravail 13
Article 8 - Utilisation des services cloud et des outils d'intelligence artificielle 14
8.1 Services cloud autorisés 14
8.2 Politique sur le Shadow IT 14
8.3 Politique sur les outils d'intelligence artificielle générative 14
8.4 Hébergement des données sensibles - exigences de souveraineté 15

Article 9 - Politique de sauvegarde des données 15
9.1 Règle 3-2-1 15
9.2 Plan de sauvegarde 16
9.3 Tests de restauration obligatoires 16
Article 10 - Gestion des mises à jour et des correctifs (Patch Management) 17
10.1 Classification et délais d'application 17
10.2 Périmètre et responsabilités 17
10.3 Gestion des équipements en fin de support 17
Article 11 - Sécurité des e-mails et protection contre le hameçonnage 18
11.1 Règles d'utilisation de la messagerie professionnelle 18
11.2 Règles de vigilance - prévention du hameçonnage 18
11.3 Procédure en cas d'e-mail suspect 18
11.4 Protocoles d'authentification e-mail (SPF, DKIM, DMARC) 18
Article 12 - Gestion des incidents de sécurité 19
12.1 Définition d'un incident de sécurité 19
12.2 Niveaux de gravité des incidents 19
12.3 Procédure de signalement et de traitement 20
12.4 Obligations de notification RGPD (72 heures) 20
12.5 Cellule de crise 20
Article 13 - Sensibilisation et formation des collaborateurs 21
13.1 Formations obligatoires 21
13.2 Ressources disponibles 21
13.3 Responsabilités du management 21
Article 14 - Gestion de la sécurité des prestataires et des tiers 22
14.1 Obligations contractuelles de sécurité 22
14.2 Gestion des accès prestataires 22
14.3 Évaluation de la sécurité des fournisseurs 22
14.4 Révocation des accès en fin de contrat 23
Article 15 - Conformité réglementaire 23
15.1 RGPD - Règlement Général sur la Protection des Données 23
15.2 Directive NIS2 23
15.3 Recommandations ANSSI 23
15.4 ISO 27001:2022 23
15.5 Assurance cyber 24
Article 16 - Sanctions et application de la politique 24
16.1 Principes généraux 24
16.2 Échelle des sanctions pour les collaborateurs 24
16.3 Sanctions applicables aux prestataires et aux tiers 25
Article 17 - Révision et mise à jour de la politique 25
17.1 Fréquence de révision 25
17.2 Déclencheurs de révision anticipée 25

17.3 Processus de validation et de diffusion 25
ANNEXES 26
Annexe A - Glossaire des termes de sécurité informatique 26
Annexe B - Modèle de fiche de déclaration d'incident de sécurité 28
Annexe C - Liste des outils et services cloud autorisés 29
Annexe D - Contacts d'urgence sécurité informatique 30
Annexe E - Tableau de suivi des révisions du document 31
Annexe F - Feuille d'émargement - Attestation de prise de connaissance 32

Article 1 - Préambule et objectifs

Les systèmes d'information constituent le cœur opérationnel de [NOM DE L'ENTREPRISE]. Leur disponibilité, leur intégrité et la confidentialité des données qu'ils traitent conditionnent directement la continuité des activités, la réputation de l'entreprise et le respect de ses obligations légales.

Face à l'intensification des cybermenaces (rançongiciels, hameçonnage, compromission de comptes, attaques sur la chaîne d'approvisionnement), la mise en place d'une Politique de Sécurité Informatique (PSI) structurée n'est plus une option mais une nécessité pour toute organisation, quelle que soit sa taille.

1.1 Contexte réglementaire

La présente politique s'inscrit dans le cadre réglementaire suivant :

- Règlement Général sur la Protection des Données (RGPD - UE 2016/679) : impose des obligations strictes en matière de protection des données personnelles, de notification des violations de données et de mise en place de mesures techniques et organisationnelles appropriées.
- Directive NIS2 (UE 2022/2555) : transposée en droit français, elle renforce les obligations de cybersécurité pour les entités essentielles et importantes, élargit le périmètre aux PME sous-traitantes de ces entités, et impose des mesures de gestion des risques et de notification des incidents.
- Recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : guides de bonnes pratiques, référentiels techniques et qualification des prestataires de sécurité.
- Norme ISO 27001:2022 : cadre international de référence pour les systèmes de management de la sécurité de l'information (SMSI), auquel la présente politique s'aligne.
- Code du travail (articles L1222-9 à L1222-11) : encadre le télétravail et les droits et obligations associés.

1.2 Objectifs de la politique

La présente politique vise à :

1. Protéger les actifs informationnels de [NOM DE L'ENTREPRISE] contre les menaces internes et externes.
2. Garantir la disponibilité, l'intégrité et la confidentialité des systèmes d'information.
3. Assurer la conformité aux obligations légales et réglementaires applicables.
4. Instaurer une culture de la cybersécurité au sein de l'ensemble des équipes.
5. Réduire l'exposition aux risques cyber et limiter l'impact potentiel d'un incident.
6. Définir clairement les responsabilités de chaque acteur en matière de sécurité.

1.3 Engagement de la direction

La direction de [NOM DE L'ENTREPRISE] s'engage à allouer les ressources humaines, techniques et financières nécessaires à la mise en œuvre de cette politique, à conduire une révision annuelle du présent document, à donner l'exemple en respectant elle-même les règles édictées, et à promouvoir une culture de la sécurité à tous les niveaux de l'organisation.

La présente politique a été approuvée par [NOM ET FONCTION DE L'APPROBATEUR] le [DATE D'APPROBATION] et entre en vigueur à compter du [DATE D'ENTRÉE EN VIGUEUR].

1.4 Sanctions en cas de non-respect

Le non-respect des règles définies dans la présente politique expose son auteur à des sanctions disciplinaires proportionnelles à la gravité du manquement, pouvant aller jusqu'au licenciement pour

faute grave ou sérieuse, voire à des poursuites pénales en cas d'infraction constituée (article 323-1 et suivants du Code pénal relatifs à l'atteinte aux systèmes de traitement automatisé de données). Pour les prestataires, le non-respect peut entraîner la résiliation immédiate du contrat.

Instructions de personnalisation

Complétez cette section avec le contexte propre à votre entreprise : secteur d'activité ([SECTEUR D'ACTIVITÉ]),
taille de l'entreprise, éventuelles certifications obtenues (ISO 27001, SecNumCloud, etc.).
Si vous êtes sous-traitant d'une entité NIS2, mentionnez-le explicitement ici.

Article 2 - Périmètre d'application

2.1 Personnes concernées

La présente politique s'applique sans exception à toutes les personnes suivantes, dès lors qu'elles accèdent, directement ou indirectement, aux systèmes d'information de [NOM DE L'ENTREPRISE] :

Catégorie	Exemples	Modalités d'application
Collaborateurs permanents	CDI, CDD, dirigeants, mandataires	Application intégrale et immédiate
Collaborateurs temporaires	Intérimaires, stagiaires, alternants	Application dès le premier jour - formation obligatoire à l'accueil
Prestataires et consultants	ESN, freelances, auditeurs	Application contractuelle - clause de sécurité obligatoire
Partenaires et tiers	Fournisseurs avec accès SI, sous-traitants RGPD	Application des règles minimales - accès tracés
Télétravailleurs	Collaborateurs en travail à distance	Application intégrale avec règles spécifiques (Article 7)

2.2 Systèmes couverts

La politique couvre l'ensemble des actifs du système d'information de [NOM DE L'ENTREPRISE], incluant :

- Postes de travail fixes et portables (ordinateurs, stations de travail).
- Équipements mobiles (smartphones, tablettes, clés USB, disques durs externes).
- Serveurs physiques et virtuels, qu'ils soient hébergés en interne ou dans le cloud.
- Infrastructure réseau (routeurs, commutateurs, pare-feux, points d'accès Wi-Fi).
- Applications métier, logiciels, progiciels (ERP, CRM, comptabilité, etc.).
- Services cloud et SaaS utilisés par l'entreprise (messagerie, stockage, collaboration).
- Sauvegardes et archives de données, quelle que soit leur forme ou leur localisation.
- Systèmes industriels et objets connectés (IoT) reliés au réseau d'entreprise, le cas échéant.

2.3 Sites géographiques

Cette politique s'applique à l'ensemble des sites de [NOM DE L'ENTREPRISE], notamment :

- Siège social : [ADRESSE DU SIÈGE SOCIAL]
- Sites secondaires et agences : [LISTE DES SITES]
- Tout espace de travail utilisé en télétravail ou en nomadisme.

Instructions de personnalisation

Listez ici tous les sites physiques de votre entreprise. Si vous avez des filiales, précisez si elles sont
également couvertes par ce document ou si elles disposent de leur propre PSI.

Article 3 - Classification des informations et des actifs

La classification des informations permet d'adapter les mesures de protection à la sensibilité réelle des données. [NOM DE L'ENTREPRISE] adopte un schéma de classification à quatre niveaux.

3.1 Niveaux de classification

Niveau	Définition	Exemples concrets	Règles de partage
PUBLIC	Informations destinées à être divulguées librement	Site web, plaquettes commerciales, offres d'emploi	Diffusion libre, sans restriction
INTERNE	Informations réservées aux collaborateurs	Notes internes, organigramme, procédures internes, planning	Partage entre collaborateurs autorisés uniquement - ne pas transmettre à l'extérieur sans autorisation
CONFIDENTIEL	Informations sensibles à accès restreint	Données clients, contrats, données RH, informations financières, stratégie	Partage limité aux personnes ayant le besoin d'en connaître - chiffrement requis pour le stockage et l'envoi
SECRET	Informations hautement sensibles dont la divulgation pourrait causer un préjudice grave	Secrets industriels, brevets en cours, données de R&D, mots de passe administrateurs, clés de chiffrement	Accès nominatif uniquement - double contrôle requis - ne jamais transmettre par e-mail

3.2 Règles de manipulation et de destruction

Action	PUBLIC	INTERNE	CONFIDENTIEL	SECRET
Stockage	Non chiffré acceptable	Non chiffré acceptable	Chiffrement recommandé	Chiffrement obligatoire
Transmission e-mail	Libre	E-mail interne OK	E-mail chiffré ou lien sécurisé	Jamais par e-mail - canal dédié
Impression	Libre	Libre	Impression sécurisée - ne pas laisser sans surveillance	Impression nominative - destruction sécurisée immédiate après usage
Archivage	Standard	Standard	Durée limitée - accès restreint	Accès nominatif - journal d'accès
Destruction	Suppression standard	Suppression standard	Suppression sécurisée (écrasement)	Destruction certifiée (broyage, effacement sécurisé 7 passes)

3.3 Inventaire des actifs informatiques

Conformément aux exigences de la norme ISO 27001:2022 (contrôle 5.9) et aux recommandations ANSSI, [NOM DE L'ENTREPRISE] maintient un inventaire à jour de l'ensemble de ses actifs informatiques. Cet inventaire est tenu par [RESPONSABLE DE L'INVENTAIRE] et mis à jour au minimum annuellement, ainsi qu'à chaque modification significative du parc informatique.

Chaque actif inventorié inclut au minimum : le propriétaire de l'actif, sa classification, sa localisation, son niveau de criticité pour l'activité et les mesures de protection associées.

Instructions de personnalisation

Tenez un tableau d'inventaire séparé (fichier Excel ou outil CMDB) recensant : matériels, logiciels,
services cloud, données et leur propriétaire. Rattachez chaque actif à un niveau de classification ci-dessus.

Article 4 - Gestion des accès et des identités (IAM)

4.1 Principe du moindre privilège

Tout compte utilisateur ou de service ne doit disposer que des droits strictement nécessaires à l'exercice de ses fonctions. Ce principe s'applique à tous les niveaux : accès applicatifs, accès réseau, accès aux données, droits d'administration. Aucun compte ne doit être créé avec des droits administrateurs par défaut. Les droits élevés sont accordés nominativement, documentés et font l'objet d'une revue trimestrielle.

4.2 Procédures de gestion des comptes

Événement	Action requise	Délai	Responsable
Arrivée d'un collaborateur	Création du compte selon le profil de poste - Formation obligatoire PSI	Avant le premier jour ouvré	[RESPONSABLE IT]
Changement de poste	Révision des droits - Suppression des droits non nécessaires	Dans les 48 heures suivant le changement	[RESPONSABLE IT] + Manager
Départ (démission, licenciement)	Désactivation immédiate du compte - Révocation des accès VPN, cloud, messagerie	Le jour même du départ, avant fin de journée	[RESPONSABLE IT] + RH
Congé longue durée (> 30 jours)	Suspension temporaire du compte	Au départ en congé	[RESPONSABLE IT]
Compte inactif (> 90 jours)	Désactivation automatique et vérification	Automatique ou mensuelle	[RESPONSABLE IT]

4.3 Gestion des comptes administrateurs

Les comptes disposant de privilèges élevés font l'objet de mesures renforcées :

- Chaque administrateur dispose d'un compte nominatif dédié à l'administration, distinct de son compte standard.
- Les connexions avec des droits administrateurs sont journalisées et auditables.
- L'authentification multifacteur (MFA) est obligatoire pour tous les accès administrateurs.
- L'utilisation de comptes administrateurs génériques (admin, administrator, root) est interdite sauf urgence technique documentée.
- Les mots de passe des comptes administrateurs sont stockés dans un coffre-fort de mots de passe dédié.

4.4 Revue périodique des droits d'accès

Type de compte	Fréquence de revue	Responsable
Comptes utilisateurs standards	Semestrielle	[RESPONSABLE IT] avec validation des managers
Comptes avec droits élevés (admin, super-utilisateur)	Trimestrielle	[RESPONSABLE IT] avec validation de la direction
Comptes prestataires et tiers	À chaque renouvellement et trimestrielle	[RESPONSABLE IT] + Responsable achats
Comptes de service (applications)	Annuelle	[RESPONSABLE IT]

Tout droit non justifié identifié lors d'une revue est révoqué dans un délai de 5 jours ouvrés. Les résultats de chaque revue sont documentés et conservés pendant 3 ans.

4.5 Modèle de matrice des accès par rôle

Le tableau suivant présente une matrice d'accès type à adapter selon les applications de l'entreprise.
Légende : R = Lecture, E = Écriture, A = Administration, X = Aucun accès.

Application / Ressource	Direction	Manager	Collaborateur	Prestataire	Administrateur IT
ERP / Comptabilité	R/E	R/E (périmètre)	R (périmètre)	X	A
CRM / Base clients	R/E	R/E	R/E (périmètre)	R (contractuel)	A
Serveurs de fichiers	R/E	R/E (périmètre)	R/E (dossier propre)	X	A
Active Directory / Annuaire	R	R	X	X	A
Infrastructure réseau	X	X	X	X	A
Sauvegardes	R	X	X	X	A

Instructions de personnalisation

Adaptez cette matrice à votre organisation. Listez vos applications métier réelles et définissez les droits
pour chaque profil. Ce tableau doit être mis à jour à chaque changement organisationnel ou applicatif.

Article 5 - Politique des mots de passe et authentification

5.1 Règles de complexité des mots de passe

Critère	Exigence comptes standards	Exigence comptes privilégiés
Longueur minimale	12 caractères	16 caractères
Majuscules	Au moins 1	Au moins 2
Minuscules	Au moins 1	Au moins 2
Chiffres	Au moins 1	Au moins 2
Caractères spéciaux	Au moins 1 (! @ # $ % & * etc.)	Au moins 2
Durée de validité	365 jours maximum	90 jours maximum
Historique (réutilisation interdite)	12 derniers mots de passe	24 derniers mots de passe
Blocage après tentatives	5 tentatives - blocage 30 minutes	3 tentatives - blocage et alerte IT

Il est recommandé d'utiliser des phrases de passe (passphrase) d'au moins 4 mots, par exemple : Cheval-Montagne-2024-Ciel. Cette méthode est à la fois plus sécurisée et plus mémorisable qu'un mot de passe court complexe.

5.2 Authentification multifacteur (MFA)

L'authentification multifacteur est obligatoire pour les accès suivants :

- Accès VPN et accès distants à l'infrastructure.
- Messagerie professionnelle accessible depuis l'extérieur du réseau d'entreprise.
- Portails d'administration (Active Directory, console cloud AWS/Azure/GCP, etc.).
- Applications métier critiques (ERP, CRM, comptabilité, paie).
- Tout accès à des données classifiées CONFIDENTIEL ou SECRET.

Les méthodes MFA acceptées sont, par ordre de préférence : application d'authentification TOTP (Microsoft Authenticator, Google Authenticator, Authy), clé de sécurité physique FIDO2/WebAuthn, SMS en dernier recours uniquement (déconseillé pour les accès à haute criticité).

5.3 Gestionnaire de mots de passe

L'utilisation d'un gestionnaire de mots de passe professionnel est fortement recommandée. [NOM DE L'ENTREPRISE] met à disposition ou recommande l'outil suivant : [NOM DE L'OUTIL RETENU - exemples : Bitwarden, 1Password Business, Keeper, Dashlane Business].

5.4 Règles d'usage

- Il est strictement interdit de partager ses identifiants avec quiconque, y compris un collègue ou un prestataire IT.
- Il est interdit de noter ses mots de passe sur un support physique non sécurisé (post-it, carnet, fichier texte non protégé).
- Il est interdit d'utiliser le même mot de passe pour des usages professionnels et personnels.
- En cas de suspicion de compromission d'un mot de passe, l'utilisateur doit le changer immédiatement et en informer le responsable IT.

Instructions de personnalisation

Précisez l'outil de gestion de mots de passe retenu et les modalités de déploiement.
Indiquez la procédure de réinitialisation de mot de passe (helpdesk, self-service, etc.).

Article 6 - Sécurité des postes de travail et appareils mobiles

6.1 Configuration minimale requise

Exigence	Poste fixe / portable	Smartphone / tablette
Chiffrement du disque	Obligatoire (BitLocker, FileVault)	Obligatoire (chiffrement natif iOS/Android activé)
Antivirus / EDR	Solution d'entreprise centralisée obligatoire	Gestion MDM obligatoire
Mises à jour OS	Automatiques ou gérées centralement - délai max 7 jours après publication	Automatiques - délai max 14 jours
Pare-feu local	Activé et géré par IT	Géré par MDM
Verrouillage automatique	5 minutes maximum d'inactivité	2 minutes maximum d'inactivité
Code PIN / mot de passe	Mot de passe selon Article 5	Code PIN 6 chiffres minimum ou biométrie + code

6.2 Politique BYOD (Bring Your Own Device)

L'utilisation d'équipements personnels pour accéder aux ressources de l'entreprise est soumise à autorisation préalable du [RESPONSABLE IT]. En cas d'autorisation, les conditions suivantes s'appliquent :

- L'équipement doit satisfaire à la configuration minimale définie à l'article 6.1.
- Un cloisonnement technique entre les données personnelles et professionnelles est mis en place via une solution MDM (Mobile Device Management).
- L'entreprise peut effacer à distance les données professionnelles en cas de perte, vol ou départ du collaborateur. L'effacement est limité aux données professionnelles.
- L'installation de l'agent MDM de l'entreprise est obligatoire. Le collaborateur accepte les conditions d'utilisation par écrit.

À ce jour, la politique BYOD de [NOM DE L'ENTREPRISE] est : [AUTORISÉE / INTERDITE / AUTORISÉE POUR LES SMARTPHONES UNIQUEMENT].

6.3 Procédure en cas de perte ou de vol

Tout équipement professionnel (ou BYOD autorisé) perdu ou volé doit faire l'objet, dans les 4 heures suivant la constatation :

7. D'un signalement immédiat au responsable IT : [CONTACT IT] - Tél. urgence : [NUMÉRO D'URGENCE IT].
8. D'un effacement à distance de l'équipement si techniquement possible.
9. D'un dépôt de plainte auprès des autorités compétentes (fournir le numéro de plainte à l'IT).
10. D'une évaluation du risque de violation de données (déclenchement éventuel de la procédure de notification CNIL selon Article 12).

Instructions de personnalisation

Précisez le nom et les coordonnées de votre responsable IT. Définissez si vous autorisez ou interdisez le BYOD.
Si vous utilisez un outil MDM (Microsoft Intune, Jamf, etc.), mentionnez-le ici.

Article 7 - Sécurité des accès distants et du télétravail

7.1 Obligation du VPN

Tout accès aux ressources internes de [NOM DE L'ENTREPRISE] depuis l'extérieur du réseau d'entreprise (domicile, déplacement, espace de coworking) doit obligatoirement transiter par le réseau privé virtuel (VPN) mis à disposition par l'entreprise. Aucun accès direct aux serveurs internes depuis Internet n'est autorisé en dehors du VPN, sauf exception documentée et approuvée par [RESPONSABLE IT]. Solution VPN retenue : [NOM DE LA SOLUTION VPN].

7.2 Règles d'utilisation des réseaux Wi-Fi

Type de réseau	Règle applicable
Wi-Fi professionnel (bureau)	Utilisation normale - réseau sécurisé WPA2/WPA3 entreprise
Wi-Fi domicile (télétravail)	Autorisé avec VPN actif - chiffrement WPA2/WPA3 obligatoire sur la box - changement du mot de passe par défaut obligatoire
Wi-Fi public (café, hôtel, transport)	Interdit pour tout accès aux données d'entreprise sans VPN actif - risque d'interception élevé
Partage de connexion 4G/5G (hotspot)	Autorisé - méthode recommandée en déplacement si Wi-Fi public indisponible

7.3 Règles de confidentialité en espace public

- Utiliser un filtre de confidentialité sur l'écran dans les espaces publics (trains, avions, cafés).
- Ne jamais laisser un équipement sans surveillance dans un lieu public, même verrouillé.
- Éviter les conversations téléphoniques ou vidéo portant sur des sujets confidentiels dans des lieux publics.
- Ne pas imprimer de documents confidentiels sur des imprimantes partagées ou publiques.
- Verrouiller systématiquement la session avant de quitter son poste de travail, même brièvement.

7.4 Équipements autorisés pour le télétravail

En télétravail, seuls les équipements fournis ou expressément autorisés par [NOM DE L'ENTREPRISE] peuvent être utilisés pour accéder aux ressources professionnelles. L'accès depuis un équipement personnel non autorisé (ordinateur familial partagé, tablette personnelle non enrôlée) est interdit.

Instructions de personnalisation

Indiquez le nom de votre solution VPN et les modalités de connexion (accès web, client dédié, etc.).

Précisez si vous remboursez le matériel pour le télétravail (écran, siège ergonomique, filtre de confidentialité).

Article 8 - Utilisation des services cloud et des outils d'intelligence artificielle

8.1 Services cloud autorisés

Seuls les services cloud validés par [RESPONSABLE IT] et listés ci-dessous sont autorisés. L'utilisation de tout service non référencé (Shadow IT) est interdite.

Service	Usage autorisé	Niveau de données autorisé	Statut
[SERVICE 1 - ex. Microsoft 365]	Bureautique, messagerie, collaboration	Interne, Confidentiel	AUTORISÉ
[SERVICE 2 - ex. Google Workspace]	[USAGE]	[NIVEAU]	AUTORISÉ / INTERDIT
[SERVICE 3 - ex. Salesforce]	CRM	Confidentiel	AUTORISÉ
[SERVICE 4 - ex. Dropbox personnel]	Stockage personnel	Aucune donnée entreprise	INTERDIT
[AUTRE SERVICE]	[USAGE]	[NIVEAU]	À COMPLÉTER

8.2 Politique sur le Shadow IT

Toute demande d'utilisation d'un nouveau service cloud doit être soumise à [RESPONSABLE IT] via [CANAL DE DEMANDE - ex. ticket helpdesk]. L'évaluation prend en compte la sécurité du service, sa localisation de données (souveraineté), sa conformité RGPD et son modèle contractuel. Une réponse est apportée dans un délai de 5 jours ouvrés.

8.3 Politique sur les outils d'intelligence artificielle générative

L'utilisation des outils d'intelligence artificielle générative (IA Gen) est encadrée par les règles suivantes. Ces outils présentent des risques spécifiques de fuite de données confidentielles.

Catégorie de données	Autorisation avec IA Gen externe	Exemples d'outils
Données publiques, textes génériques	Autorisée	ChatGPT, Copilot, Claude, Gemini (usage général)
Données INTERNES non sensibles	Autorisée avec prudence - anonymiser si possible	Copilot for Microsoft 365 (données restant dans le tenant)
Données CONFIDENTIELLES (clients, contrats, RH)	INTERDITE sur outils cloud publics - utiliser uniquement des outils hébergés en interne ou dans un environnement maîtrisé	Environnement Azure OpenAI privé, solution on-premise
Données SECRÈTES ou soumises à secret professionnel	STRICTEMENT INTERDITE	Aucun outil externe

Il est notamment interdit de saisir dans un outil d'IA externe : des données personnelles de clients ou de collaborateurs, des informations financières non publiques, des données couvertes par un NDA, des secrets industriels, des identifiants de connexion, des extraits de code source propriétaire.

8.4 Hébergement des données sensibles - exigences de souveraineté

Les données classifiées CONFIDENTIEL et SECRET doivent être hébergées dans des environnements offrant des garanties de souveraineté compatibles avec les exigences réglementaires françaises et européennes. Les certifications à privilégier : SecNumCloud (ANSSI), ISO 27001, HDS (pour les données de santé). Pour les données les plus sensibles, un hébergement en France ou dans l'UE est obligatoire. Solutions retenues : [SOLUTIONS RETENUES].

Instructions de personnalisation

Dressez la liste de tous vos services cloud utilisés. Vérifiez pour chacun : localisation des données,
accord de traitement des données (DPA/ATD) signé, politique de rétention.
Pour les outils IA, définissez une liste positive des outils autorisés et formez vos équipes.

Article 9 - Politique de sauvegarde des données

9.1 Règle 3-2-1

[NOM DE L'ENTREPRISE] applique la règle de sauvegarde 3-2-1, reconnue comme standard de référence par l'ANSSI :

- 3 copies des données (1 copie de production + 2 copies de sauvegarde).
- 2 supports ou technologies différents (par exemple : serveur local NAS + cloud).
- 1 copie hors site ou hors ligne (air-gap), protégée contre les rançongiciels.

Cette règle garantit qu'aucun sinistre unique (incendie, rançongiciel, défaillance matérielle) ne puisse détruire simultanément toutes les copies des données critiques.

9.2 Plan de sauvegarde

Type de données	Fréquence	Rétention	Support 1	Support 2 (hors site)	Responsable
Données métier critiques (ERP, CRM, compta)	Quotidienne (nuit)	90 jours	NAS interne	Cloud [FOURNISSEUR]	[RESPONSABLE IT]
Fichiers utilisateurs (serveur de fichiers)	Quotidienne	30 jours	NAS interne	Cloud [FOURNISSEUR]	[RESPONSABLE IT]
Messagerie professionnelle	Continue (réplication)	1 an	Hébergement prestataire	Archive cloud	[RESPONSABLE IT]
Bases de données applicatives	Quotidienne + hebdomadaire	1 an	Serveur dédié	Cloud chiffré	[RESPONSABLE IT]
Configuration infrastructure réseau	Après chaque modification	5 versions	Coffre-fort local	Cloud sécurisé	[RESPONSABLE IT]

9.3 Tests de restauration obligatoires

Toute sauvegarde non testée ne peut être considérée comme fiable. [NOM DE L'ENTREPRISE] impose les tests de restauration suivants :

Type de test	Fréquence minimale	Procédure	Documentation
Restauration partielle (fichier isolé)	Mensuelle	Restaurer un fichier ou répertoire aléatoire et vérifier son intégrité	Rapport de test daté et signé
Restauration complète (base de données)	Trimestrielle	Restaurer une base de données sur un environnement de test	Rapport avec temps de restauration mesuré
Test de reprise d'activité complet	Annuelle	Simuler une perte totale et mesurer le RTO/RPO réel	Rapport de PRA signé par la direction

Les résultats des tests de restauration sont conservés pendant 3 ans et communiqués à la direction. Un test de restauration échoué doit déclencher une action corrective immédiate.

Instructions de personnalisation

Définissez votre RTO (Recovery Time Objective - durée maximale d'indisponibilité acceptable) et votre RPO
(Recovery Point Objective - perte de données maximale acceptable). Pour une PME : RTO de 4 à 24h et
RPO de 24h sont des cibles raisonnables. Adaptez le tableau à vos applications réelles.

Article 10 - Gestion des mises à jour et des correctifs (Patch Management)

10.1 Classification et délais d'application

L'application des correctifs de sécurité est une des mesures les plus efficaces pour réduire l'exposition aux cyberattaques. Les délais ci-dessous sont des maximums à respecter impérativement :

Criticité (CVSS)	Score CVSS	Délai maximum d'application	Procédure
CRITIQUE	9,0 - 10,0	48 heures	Application immédiate après test minimal - dérogation direction requise si dépassement
ÉLEVÉE	7,0 - 8,9	7 jours ouvrés	Application en fenêtre de maintenance prioritaire
MODÉRÉE	4,0 - 6,9	30 jours calendaires	Application lors du cycle de maintenance mensuel
FAIBLE	0,1 - 3,9	90 jours calendaires	Application lors du cycle de maintenance trimestriel

10.2 Périmètre et responsabilités

Le périmètre du patch management couvre : systèmes d'exploitation (Windows, macOS, Linux), applications bureautiques (Office, navigateurs web), logiciels métier, équipements réseau (firmware des routeurs, commutateurs, pare-feux), systèmes d'exploitation mobiles.

Responsable du suivi des vulnérabilités et de la planification des correctifs : [RESPONSABLE IT]. Les avis de sécurité sont suivis via : CERT-FR (cert.ssi.gouv.fr), bulletins constructeurs, flux CVE. La veille est effectuée [FRÉQUENCE - ex. hebdomadaire].

10.3 Gestion des équipements en fin de support

- Maintenir un inventaire des dates de fin de support de tous les composants critiques.
- Initier une démarche de remplacement au moins 12 mois avant la date de fin de support.
- En cas d'impossibilité de remplacement immédiat, mettre en place des mesures compensatoires documentées (isolation réseau, surveillance renforcée) approuvées par la direction.
- Interdire formellement la connexion à Internet d'équipements dont le système d'exploitation n'est plus maintenu (ex. Windows 7, Windows XP).

Instructions de personnalisation

Utilisez un outil de gestion de parc (GLPI, Lansweeper, etc.) pour suivre les dates de fin de support.
Établissez un budget prévisionnel de renouvellement des équipements sur 3 à 5 ans.

Article 11 - Sécurité des e-mails et protection contre le hameçonnage

11.1 Règles d'utilisation de la messagerie professionnelle

- La messagerie professionnelle ([DOMAINE E-MAIL]) est réservée aux usages professionnels. Un usage personnel occasionnel et raisonnable est toléré.
- Il est strictement interdit d'utiliser une messagerie personnelle (Gmail, Hotmail, Yahoo, etc.) pour transmettre des données professionnelles.
- Toute pièce jointe de taille supérieure à [LIMITE - ex. 10 Mo] doit être transmise via un lien de téléchargement sécurisé depuis la plateforme de partage autorisée.
- Les données classifiées CONFIDENTIEL ou SECRET ne doivent jamais être transmises par e-mail non chiffré.

11.2 Règles de vigilance - prévention du hameçonnage

- Vérifier l'adresse e-mail de l'expéditeur (pas seulement le nom affiché) avant d'ouvrir une pièce jointe ou de cliquer sur un lien.
- En cas de doute sur un e-mail prétendant venir d'un fournisseur, d'un client ou d'un collaborateur, le confirmer par téléphone ou via un autre canal, sans utiliser les coordonnées figurant dans l'e-mail suspect.
- Ne jamais saisir ses identifiants sur une page web atteinte via un lien dans un e-mail. Accéder directement aux services via les marque-pages ou l'URL habituelle.
- Traiter avec une vigilance particulière toute demande urgente de virement, de modification de coordonnées bancaires ou de transfert de fichiers sensibles.
- Ne jamais activer les macros d'un document Office reçu par e-mail, sauf si le document provient d'une source interne vérifiée.

11.3 Procédure en cas d'e-mail suspect

11. Ne pas cliquer, ne pas ouvrir les pièces jointes, ne pas répondre à l'e-mail.
12. Signaler immédiatement l'e-mail à [RESPONSABLE IT] via [CANAL DE SIGNALEMENT - ex. bouton « Signaler » dans Outlook, ticket helpdesk].
13. Conserver l'e-mail en attente d'analyse (ne pas le supprimer avant accord IT).
14. Si un lien a déjà été cliqué ou des identifiants saisis : changer immédiatement le mot de passe et alerter l'IT en urgence.

11.4 Protocoles d'authentification e-mail (SPF, DKIM, DMARC)

Pour protéger le domaine de [NOM DE L'ENTREPRISE] contre l'usurpation d'identité (spoofing), les protocoles suivants doivent être configurés et maintenus par le responsable technique :

- SPF (Sender Policy Framework) : définit les serveurs autorisés à envoyer des e-mails pour le domaine.
- DKIM (DomainKeys Identified Mail) : appose une signature cryptographique sur les e-mails sortants.
- DMARC (Domain-based Message Authentication, Reporting and Conformance) : définit la politique de traitement des e-mails non authentifiés (politique p=quarantine ou p=reject recommandée).

État actuel : SPF : [CONFIGURÉ/NON CONFIGURÉ] - DKIM : [CONFIGURÉ/NON CONFIGURÉ] - DMARC : [CONFIGURÉ/NON CONFIGURÉ] - Politique DMARC : [NONE/QUARANTINE/REJECT]

Instructions de personnalisation

Demandez à votre prestataire ou hébergeur e-mail de vérifier et configurer SPF, DKIM et DMARC.

L'outil MXToolbox (mxtoolbox.com/SuperTool.aspx) permet de vérifier gratuitement votre configuration.

Article 12 - Gestion des incidents de sécurité

12.1 Définition d'un incident de sécurité

Constitue un incident de sécurité informatique tout événement susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des systèmes d'information ou des données. À titre d'exemples non exhaustifs :

- Infection par un virus, un rançongiciel ou un logiciel malveillant.
- Accès non autorisé à des données ou des systèmes.
- Perte ou vol d'un équipement contenant des données d'entreprise.
- Violation de données personnelles (fuite, accès non autorisé, destruction accidentelle).
- Tentative d'intrusion détectée sur le réseau ou les systèmes.
- Indisponibilité prolongée et inexpliquée d'un service critique.
- Réception d'un e-mail de hameçonnage ayant conduit à la saisie d'identifiants.

12.2 Niveaux de gravité des incidents

Niveau	Critères	Exemples	Délai de réponse initiale	Escalade
P1 - CRITIQUE	Impact sur des données personnelles sensibles ou arrêt complet d'activité	Rançongiciel bloquant tous les postes, fuite de base clients	Immédiate (H+1 maximum)	Direction + RSSI + Cellule de crise
P2 - ÉLEVÉ	Impact significatif sur un service ou des données confidentielles	Compromission d'un compte e-mail, accès non autorisé avéré	2 heures ouvrées	Responsable IT + Direction
P3 - MODÉRÉ	Impact limité ou incident contenu rapidement	Logiciel malveillant détecté et isolé, tentative de hameçonnage non aboutie	8 heures ouvrées	Responsable IT

12.3 Procédure de signalement et de traitement

15. DÉTECTER : Tout collaborateur suspectant ou constatant un incident signale immédiatement via [CANAL DE SIGNALEMENT - ex. e-mail security@entreprise.fr, tél. urgence IT : [NUMÉRO], ticket helpdesk].
16. NE PAS AGIR seul : ne pas tenter de corriger ou d'effacer des éléments sans instruction IT.
17. ISOLER si possible : sur instruction IT, déconnecter l'équipement compromis du réseau (débrancher le câble ou désactiver le Wi-Fi) sans l'éteindre.
18. DOCUMENTER : noter l'heure de détection, les symptômes observés, les actions déjà effectuées.
19. ANALYSER ET REMÉDIER avec l'équipe IT ou le prestataire de sécurité.
20. CLÔTURER : rédiger un rapport d'incident et conduire un retour d'expérience.

12.4 Obligations de notification RGPD (72 heures)

En cas de violation de données personnelles, [NOM DE L'ENTREPRISE] est soumise aux obligations suivantes, conformément à l'article 33 du RGPD :

- Notification à la CNIL dans un délai de 72 heures suivant la prise de connaissance de la violation, si elle est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. La notification s'effectue sur le portail notifications.cnil.fr.
- Si la violation est susceptible d'engendrer un risque élevé pour les personnes, information directe des personnes concernées dans les meilleurs délais (article 34 RGPD).
- Documentation systématique de toute violation dans le registre des violations de données, même si la notification à la CNIL n'est pas requise.

Responsable de la notification CNIL : [NOM DU DPO OU RESPONSABLE RGPD] - Contact : [E-MAIL/TÉL.].

12.5 Cellule de crise

Rôle	Nom	Contact
Directeur de la cellule de crise (décision)	[NOM DU DIRIGEANT]	[CONTACT]
Responsable technique (IT/RSSI)	[NOM RESPONSABLE IT]	[CONTACT]
Responsable communication	[NOM]	[CONTACT]
Prestataire de sécurité	[NOM DU PRESTATAIRE]	[CONTACT D'URGENCE]
DPO / Responsable RGPD	[NOM DU DPO]	[CONTACT]

Un modèle de fiche de déclaration d'incident figure en Annexe B du présent document.

Instructions de personnalisation

Définissez impérativement le canal de signalement des incidents (e-mail dédié, ticket, numéro d'astreinte).

Réalisez un exercice de simulation d'incident au moins une fois par an pour tester cette procédure.

Article 13 - Sensibilisation et formation des collaborateurs

13.1 Formations obligatoires

La sécurité informatique est l'affaire de tous. La grande majorité des incidents de sécurité (plus de 80 % selon les études sectorielles) implique une dimension humaine. La formation et la sensibilisation des collaborateurs constituent des investissements prioritaires.

Formation	Public cible	Fréquence	Contenu minimal	Validation
Formation initiale PSI	Tout nouveau collaborateur, stagiaire, prestataire avec accès SI	À l'arrivée (dans les 5 jours)	Lecture et signature de la PSI, règles essentielles, procédures d'incident	Feuille d'émargement (Annexe F) + quiz de validation
Sensibilisation annuelle	Tous les collaborateurs	Annuelle	Actualité des menaces, rappel des règles, cas pratiques, retours d'expérience	Attestation de suivi
Test de hameçonnage simulé	Tous les collaborateurs	2 fois par an minimum	E-mail de hameçonnage simulé - mesure du taux de clic - formation corrective	Rapport de taux de réussite
Formation approfondie	Responsables IT, managers	Annuelle	Techniques d'attaque avancées, gestion de crise, réglementation	Certification ou attestation

13.2 Ressources disponibles

- Portail de sensibilisation interne : [URL DU PORTAIL OU « À CRÉER »].
- Ressources ANSSI gratuites : www.cybermalveillance.gouv.fr (guides, fiches réflexes).
- Kit de sensibilisation SecNumAcadémie (ANSSI) : gratuit et disponible en ligne.
- Contact pour toute question de sécurité : [E-MAIL SÉCURITÉ INTERNE].

13.3 Responsabilités du management

- S'assurer que tout nouveau collaborateur de son équipe suit la formation initiale PSI dans les délais.
- Promouvoir les bonnes pratiques au quotidien et donner l'exemple.
- Signaler au responsable IT tout comportement contraire à la présente politique.
- Informer le responsable IT de tout changement dans son équipe (arrivée, départ, changement de poste).

Instructions de personnalisation

Choisissez une plateforme de sensibilisation (Terranova, KnowBe4, Proofpoint, ou solution interne).

Planifiez les campagnes de hameçonnage simulé dans le calendrier annuel des formations.

Article 14 - Gestion de la sécurité des prestataires et des tiers

14.1 Obligations contractuelles de sécurité

Tout contrat avec un prestataire ayant accès, même ponctuel, aux systèmes d'information ou aux données de [NOM DE L'ENTREPRISE] doit inclure une clause de sécurité informatique obligatoire couvrant a minima :

- L'obligation de respecter la présente PSI lors des interventions sur le SI de l'entreprise.
- L'obligation de signaler immédiatement tout incident de sécurité détecté ou susceptible d'affecter les données de l'entreprise.
- L'interdiction de sous-traiter les accès ou les données sans accord préalable écrit de [NOM DE L'ENTREPRISE].
- L'obligation de restituer ou de détruire de façon certifiée les données en fin de mission.
- Le droit d'audit de [NOM DE L'ENTREPRISE] sur les mesures de sécurité du prestataire.

Pour tout prestataire traitant des données à caractère personnel, la signature d'un Accord de Traitement des Données (ATD / DPA) conforme au RGPD est obligatoire avant tout début de traitement (article 28 RGPD).

14.2 Gestion des accès prestataires

- Les accès accordés aux prestataires sont nominatifs, limités dans le temps et au périmètre strictement nécessaire.
- Aucun compte générique ou partagé ne doit être créé pour des prestataires.
- Les sessions d'intervention à distance des prestataires sont idéalement enregistrées via un outil de supervision des accès à privilèges (PAM - Privileged Access Management).
- Un accès accompagné est préférable pour les interventions sensibles (présence d'un collaborateur IT interne).

14.3 Évaluation de la sécurité des fournisseurs

Critère d'évaluation	Niveau requis (données CONFIDENTIELLES)	Niveau requis (données SECRÈTES)
Certifications / qualifications	ISO 27001 ou équivalent souhaité	ISO 27001 obligatoire ou qualification ANSSI
Localisation des données	UE ou France préféré	France ou UE obligatoire
Politique de sécurité documentée	Obligatoire	Obligatoire + audit possible
Réponse aux incidents	Procédure documentée requise	SLA d'incident contractualisé
Formation des équipes	Sensibilisation de base	Formation avancée certifiée

14.4 Révocation des accès en fin de contrat

À la fin de toute relation contractuelle, dans un délai maximum de 24 heures après la fin effective du contrat :

21. Révocation de tous les accès logiques (comptes, VPN, applications, messagerie si applicable).
22. Récupération des équipements prêtés (badge, matériel).
23. Confirmation écrite de la suppression ou de la restitution des données par le prestataire.
24. Archivage des journaux d'accès du prestataire pendant une durée minimale de 1 an.

Instructions de personnalisation

Dressez un registre des prestataires avec accès SI (nom, accès accordés, DPA signé, date de fin de contrat).

Vérifiez que tous vos prestataires actuels ont signé une clause de sécurité et, si applicable, un DPA RGPD.

Article 15 - Conformité réglementaire

15.1 RGPD - Règlement Général sur la Protection des Données

- Délégué à la Protection des Données (DPO) : [NOM DU DPO - OBLIGATOIRE POUR LES ORGANISMES PUBLICS ET CERTAINS ACTEURS PRIVÉS - contact : [E-MAIL DPO]]. Pour les PME sans DPO obligatoire, nommer un référent RGPD interne.
- Registre des activités de traitement : [NOM DE L'ENTREPRISE] tient et maintient à jour son registre des traitements conformément à l'article 30 du RGPD. Responsable : [NOM].
- Droits des personnes concernées : toute demande d'exercice des droits (accès, rectification, effacement, portabilité, opposition) est traitée dans un délai d'un mois. Contact : [E-MAIL RGPD].
- Analyses d'impact (AIPD/DPIA) : réalisées avant tout nouveau traitement susceptible d'engendrer un risque élevé pour les personnes physiques.

15.2 Directive NIS2

La directive NIS2 (transposée en France) s'applique aux entités essentielles et importantes dans des secteurs définis. [NOM DE L'ENTREPRISE] [EST / N'EST PAS] directement concernée par NIS2 en tant qu'[ENTITÉ ESSENTIELLE / IMPORTANTE / SOUS-TRAITANT D'UNE ENTITÉ NIS2].

Le cas échéant, les obligations spécifiques applicables sont : [LISTE DES OBLIGATIONS NIS2 APPLICABLES]. Pour vérifier votre assujettissement, consulter : cyber.gouv.fr ou l'ANSSI.

15.3 Recommandations ANSSI

La présente politique s'appuie sur les guides et recommandations publiés par l'ANSSI, notamment : le Guide d'hygiène informatique (42 mesures essentielles), les recommandations pour la sécurisation des systèmes d'information, le guide de gestion des incidents de sécurité, et le Référentiel Général de Sécurité (RGS) pour les interactions avec les administrations publiques.

15.4 ISO 27001:2022

[NOM DE L'ENTREPRISE] [EST CERTIFIÉE ISO 27001 / VISE UNE CERTIFICATION ISO 27001 / S'INSPIRE DES BONNES PRATIQUES ISO 27001 SANS VISER LA CERTIFICATION]. Les contrôles de sécurité applicables sont sélectionnés et documentés dans la Déclaration d'Applicabilité (SOA) tenue par [RESPONSABLE].

15.5 Assurance cyber

La mise en œuvre effective de la présente politique contribue à renforcer la position de [NOM DE L'ENTREPRISE] vis-à-vis de son assureur cyber. Lors de la souscription ou du renouvellement d'une police d'assurance cyber, le respect des mesures définies dans cette politique est susceptible d'influer positivement sur les conditions tarifaires et les garanties accordées. Assureur cyber actuel : [NOM DE L'ASSUREUR] - Contrat n° [NUMÉRO] - Contact sinistres : [CONTACT].

Instructions de personnalisation

Si votre entreprise n'a pas encore de DPO ni de registre des traitements, c'est une priorité légale. Pour NIS2, vérifiez votre secteur sur cyber.gouv.fr/nis2 pour déterminer si vous êtes concerné.

Article 16 - Sanctions et application de la politique

16.1 Principes généraux

Le non-respect de la présente politique est traité avec le sérieux que requiert la protection des actifs de l'entreprise, des données des clients et des collaborateurs. Les sanctions sont proportionnelles à la gravité du manquement, à son caractère intentionnel ou non, et à ses conséquences réelles ou potentielles.

16.2 Échelle des sanctions pour les collaborateurs

Niveau de manquement	Exemples	Sanction applicable
Mineur (négligence sans conséquence)	Non-respect du verrouillage de session, partage involontaire d'un fichier interne, mot de passe non conforme	Rappel à l'ordre oral, formation corrective obligatoire
Modéré (négligence avec risque potentiel)	Utilisation d'une messagerie personnelle pour des données confidentielles, connexion sans VPN répétée	Avertissement écrit, formation obligatoire, signalement au manager
Grave (faute caractérisée)	Clic sur un lien de hameçonnage avec compromission, installation d'un logiciel non autorisé ayant causé une infection	Mise à pied, procédure disciplinaire formelle
Très grave ou intentionnel	Vol ou destruction intentionnelle de données, installation délibérée d'un logiciel espion, revente d'informations confidentielles	Licenciement pour faute grave ou sérieuse, dépôt de plainte pénale

Toute sanction disciplinaire respecte les procédures prévues par le Code du travail et la convention collective applicable à [NOM DE L'ENTREPRISE].

16.3 Sanctions applicables aux prestataires et aux tiers

- La résiliation immédiate du contrat aux torts du prestataire, sans indemnité.
- L'activation des clauses de responsabilité et de pénalités contractuelles.
- Le dépôt d'une plainte pénale en cas d'infraction constituée.
- La signalisation aux autorités compétentes (CNIL, ANSSI) en cas de violation de données.

Article 17 - Révision et mise à jour de la politique

17.1 Fréquence de révision

La présente politique fait l'objet d'une révision formelle au minimum une fois par an, idéalement au cours du premier trimestre de chaque année civile. Cette révision est conduite par [RESPONSABLE DE LA RÉVISION] avec la participation des parties prenantes concernées (direction, RH, responsables métier).

17.2 Déclencheurs de révision anticipée

Une révision anticipée peut être déclenchée par l'un des événements suivants :

- Incident de sécurité majeur (P1) ayant mis en évidence des lacunes dans la politique.
- Évolution significative du cadre réglementaire (nouvelle directive, modification RGPD, etc.).
- Changement organisationnel majeur (fusion, acquisition, changement de direction, croissance rapide).
- Migration vers une nouvelle infrastructure ou adoption d'une technologie majeure.
- Résultat d'un audit de sécurité révélant des non-conformités substantielles.
- Recommandation d'un prestataire de sécurité suite à un test d'intrusion.

17.3 Processus de validation et de diffusion

25. Rédaction de la révision par [RESPONSABLE IT] avec prise en compte des retours d'expérience.
26. Relecture et validation juridique si des modifications concernent les obligations légales.
27. Approbation formelle par [NOM ET FONCTION DE L'APPROBATEUR].
28. Diffusion à l'ensemble des collaborateurs via [CANAL - ex. intranet, e-mail à tous, réunion d'équipe].
29. Mise à jour du tableau de révision (Annexe E) et archivage de la version précédente.
30. Formation ou communication spécifique si les modifications sont substantielles.
31. Signature de la nouvelle feuille d'émargement par les collaborateurs (Annexe F).

ANNEXES

Annexe A - Glossaire des termes de sécurité informatique

Terme	Définition
Actif informatique	Tout élément ayant de la valeur pour l'organisation : données, logiciels, matériels, infrastructures réseau.
Antivirus / EDR	Logiciel détectant et neutralisant les programmes malveillants. L'EDR (Endpoint Detection and Response) est une version avancée avec capacités d'analyse comportementale.
APT (Advanced Persistent Threat)	Attaque informatique ciblée, furtive et persistante menée par des acteurs sophistiqués (États, groupes criminels organisés).
Authentification multifacteur (MFA)	Mécanisme de vérification d'identité combinant au moins deux facteurs : quelque chose que l'on sait (mot de passe), possède (téléphone) ou est (biométrie).
BEC (Business Email Compromise)	Fraude consistant à usurper l'identité d'un dirigeant ou d'un fournisseur pour obtenir un virement frauduleux.
BYOD (Bring Your Own Device)	Politique autorisant les collaborateurs à utiliser leurs équipements personnels à des fins professionnelles.
Chiffrement	Transformation cryptographique des données les rendant illisibles sans la clé de déchiffrement correspondante.
CVSS (Common Vulnerability Scoring System)	Système de notation standardisé de la criticité des vulnérabilités informatiques, de 0 (aucun risque) à 10 (critique).
DMZ (Zone démilitarisée)	Sous-réseau physique ou logique séparant un réseau interne d'un réseau non fiable (Internet), hébergeant les services accessibles publiquement.
DPO (Data Protection Officer)	Délégué à la Protection des Données, responsable du suivi de la conformité RGPD au sein de l'organisation.
Pare-feu (Firewall)	Système de sécurité réseau filtrant le trafic entrant et sortant selon des règles définies.
FIDO2 / WebAuthn	Standard d'authentification forte sans mot de passe, utilisant des clés cryptographiques (clés de sécurité physiques, biométrie).
Ingénierie sociale	Manipulation psychologique visant à obtenir des informations confidentielles ou à pousser une victime à réaliser une action nuisible.
ISO 27001	Norme internationale définissant les exigences d'un Système de Management de la Sécurité de l'Information (SMSI).
MDM (Mobile Device Management)	Solution permettant de gérer et sécuriser à distance les appareils mobiles du parc informatique.
NIS2	Directive européenne sur la sécurité des réseaux et des systèmes d'information, renforçant les obligations de cybersécurité depuis 2024.

Hameçonnage (Phishing)	Technique d'attaque par e-mail, SMS ou appel téléphonique imitant une entité de confiance pour soutirer des identifiants ou déclencher un paiement frauduleux.
Rançongiciel (Ransomware)	Logiciel malveillant chiffrant les données de la victime et exigeant une rançon en échange de la clé de déchiffrement.
RPO (Recovery Point Objective)	Perte de données maximale acceptable en cas de sinistre, exprimée en durée (ex. : 24 h signifie qu'on accepte de perdre au maximum 24 h de données).
RTO (Recovery Time Objective)	Durée maximale d'interruption acceptable avant reprise d'activité après un sinistre.
SMSI	Système de Management de la Sécurité de l'Information : ensemble de politiques, processus et systèmes permettant de gérer les risques liés à la sécurité de l'information de façon structurée.
Hameçonnage ciblé (Spear phishing)	Variante ciblée du hameçonnage, personnalisée pour une victime spécifique en utilisant des informations la concernant.
VPN (Virtual Private Network)	Réseau privé virtuel permettant de créer un tunnel chiffré entre un poste distant et le réseau d'entreprise.
Vulnérabilité	Faiblesse dans un système, une application ou un processus pouvant être exploitée par un attaquant pour compromettre la sécurité.
Vulnérabilité zero-day	Vulnérabilité inconnue du fabricant et donc sans correctif disponible, pouvant être exploitée immédiatement par des attaquants.

Annexe B - Modèle de fiche de déclaration d'incident de sécurité

Champ	À renseigner
Date et heure de détection	
Déclarant (nom, fonction, contact)	
Date et heure de signalement au responsable IT	
Description de l'incident	
Systèmes / données potentiellement affectés	
Niveau de gravité estimé (P1 / P2 / P3)	
Actions déjà réalisées par le déclarant	
Équipements concernés (modèle, numéro de série)	
Impact métier estimé (activités interrompues)	
Présence de données personnelles concernées (OUI / NON)	
Si OUI : catégories de personnes et volume estimé	
Notification CNIL requise (OUI / NON - délai 72 h)	
Prestataire externe notifié (OUI / NON - lequel)	

Ce formulaire doit être transmis à [RESPONSABLE IT] par [CANAL - ex. e-mail security@entreprise.fr].

Conserver une copie de cette fiche dans le registre des incidents de sécurité de l'entreprise.

Annexe C - Liste des outils et services cloud autorisés

Ce tableau est à compléter et à maintenir à jour par [RESPONSABLE IT]. Toute demande d'ajout doit suivre la procédure définie à l'Article 8.2.

Outil / Service	Éditeur	Usage	Niveau max autorisé	Localisation données	DPA signé	Date validation
[SERVICE 1]	[ÉDITEUR]	[USAGE]	[ ]	[PAYS/RÉGION]	O / N	[DATE]
[SERVICE 2]	[ÉDITEUR]	[USAGE]	[ ]	[PAYS/RÉGION]	O / N	[DATE]
[SERVICE 3]	[ÉDITEUR]	[USAGE]	[ ]	[PAYS/RÉGION]	O / N	[DATE]
[SERVICE 4]	[ÉDITEUR]	[USAGE]	[ ]	[PAYS/RÉGION]	O / N	[DATE]
[SERVICE 5]	[ÉDITEUR]	[USAGE]	[ ]	[PAYS/RÉGION]	O / N	[DATE]

Annexe D - Contacts d'urgence sécurité informatique

Rôle	Nom	Téléphone	E-mail	Disponibilité
Responsable IT interne	[NOM]	[TÉL.]	[E-MAIL]	Heures ouvrées
Astreinte IT (hors heures ouvrées)	[NOM]	[TÉL. ASTREINTE]	[E-MAIL]	24 h/24 - 7 j/7
Prestataire de sécurité (MSSP)	[NOM SOCIÉTÉ]	[TÉL.]	[E-MAIL]	[HORAIRES]
DPO / Référent RGPD	[NOM]	[TÉL.]	[E-MAIL]	Heures ouvrées
Assureur cyber - déclaration sinistre	[ASSUREUR]	[TÉL. SINISTRES]	[E-MAIL]	[HORAIRES]
CERT-FR (ANSSI)	cert.ssi.gouv.fr	+33 1 71 75 84 68	cert-fr@ssi.gouv.fr	24 h/24 - 7 j/7
Cybermalveillance.gouv.fr	cybermalveillance.gouv.fr	-	Formulaire en ligne	En ligne
CNIL (notification violations de données)	cnil.fr	01 53 73 22 22	notifications.cnil.fr	Heures ouvrées

Annexe E - Tableau de suivi des révisions du document

Version	Date	Auteur	Nature des modifications	Approbateur
1.0	[DATE]	[AUTEUR]	Version initiale	[APPROBATEUR]

Annexe F - Feuille d'émargement - Attestation de prise de connaissance

Je soussigné(e), _____ (nom et prénom), en qualité de _____ (fonction), au sein de [NOM DE L'ENTREPRISE], atteste avoir pris connaissance de la Politique de Sécurité Informatique de l'entreprise dans sa version _____ du _____.

Je m'engage à respecter l'ensemble des règles et procédures qui y sont définies, dans le cadre de mes activités professionnelles. Je reconnais avoir été informé(e) que tout manquement est susceptible d'entraîner des sanctions disciplinaires, telles que définies à l'Article 16 du présent document.

Fait à _____, le _____

Signature :

Nom	Prénom	Fonction	Date	Signature

Ce modèle a été élaboré par ia-cyber-securite.fr. Adaptez-le à votre contexte.