

Politique de sécurité de l'information

Trame à adapter. Les passages *en italique entre crochets* sont à compléter. Chaque section renvoie aux contrôles de l'Annexe A d'ISO 27001:2022 qu'elle couvre, pour alimenter directement votre déclaration d'applicabilité.

Ce qu'un auditeur regardera en premier

La date et la signature d'approbation, la preuve de diffusion, et la cohérence entre ce que dit la politique et ce que fait réellement l'organisation. Une politique de cinq pages appliquée vaut mieux qu'une de quarante que personne n'a lue.

1. Objet et périmètre

La présente politique définit les principes de sécurité de l'information de *[NOM DE L'ORGANISATION]* et s'applique à *[PÉRIMÈTRE : entités, sites, systèmes, personnels, prestataires]*.

Elle est approuvée par *[ORGANE]* le *[DATE]* et revue au moins annuellement.

Contrôles ISO 27001:2022 concernés

5.1 Politiques de sécurité de l'information

2. Engagement de la direction

La direction s'engage à allouer les ressources nécessaires, à arbitrer les risques résiduels et à examiner la performance du dispositif au moins *[FRÉQUENCE]*.

Point d'attention : l'article 32 de la loi belge engage la responsabilité personnelle des membres de l'organe de direction. L'absence de trace d'implication est un risque juridique, pas seulement normatif.

Contrôles ISO 27001:2022 concernés

5.4 Responsabilités de la direction

3. Rôles et responsabilités

Responsable de la sécurité : *[NOM]* — suppléant : *[NOM]*.

Les rôles de sécurité figurent dans les fiches de poste et sont revus annuellement. Les tâches incompatibles sont séparées ; à défaut, un contrôle compensatoire est documenté.

Contrôles ISO 27001:2022 concernés

5.2 Rôles et responsabilités en matière de sécurité de l'information

5.3 Séparation des tâches

4. Gestion des risques

Méthode retenue : *[ISO 27005 / EBIOS RM / autre]*. Réévaluation au moins annuelle et à chaque changement significatif. Les risques résiduels sont acceptés formellement par *[ORGANE]*.

Relève des chapitres 6 et 8 d'ISO 27001, pas de l'Annexe A.

5. Classification et manipulation

Niveaux retenus : [2 à 4 niveaux]. Chaque niveau est assorti de règles de manipulation, de transfert et de conservation.

Contrôles ISO 27001:2022 concernés

- | | |
|------|---|
| 5.12 | Classification de l'information |
| 5.13 | Étiquetage de l'information |
| 5.10 | Utilisation acceptable de l'information et des actifs |

6. Contrôle des accès

Les droits sont attribués par rôle et validés par le propriétaire de la ressource. Revue des accès : [FRÉQUENCE]. Authentification à plusieurs facteurs imposée sur les accès distants, les comptes à privilèges et les applications critiques.

Contrôles ISO 27001:2022 concernés

- | | |
|------|---------------------------------|
| 5.15 | Contrôle d'accès |
| 5.16 | Gestion des identités |
| 5.17 | Informations d'authentification |
| 5.18 | Droits d'accès |
| 8.2 | Droits d'accès privilégié |
| 8.5 | Authentification sécurisée |

7. Sécurité des opérations

Configurations de référence, gestion des vulnérabilités avec délais par criticité ([critique : X j / élevé : Y j]), journalisation centralisée et surveillance.

Contrôles ISO 27001:2022 concernés

- | | |
|------|---------------------------------------|
| 8.7 | Protection contre les malwares |
| 8.8 | Gestion des vulnérabilités techniques |
| 8.9 | Gestion de la configuration |
| 8.15 | Journalisation (Logging) |
| 8.16 | Activités de surveillance |

8. Continuité et sauvegardes

Objectifs par processus : [RTO / RPO]. Sauvegardes selon la règle 3-2-1 avec une copie hors ligne ou immuable, et test de restauration [FRÉQUENCE].

Contrôles ISO 27001:2022 concernés

- | | |
|------|---|
| 5.29 | Sécurité de l'information pendant les perturbations |
| 5.30 | Préparation des TIC pour la continuité d'activité |
| 8.13 | Sauvegarde de l'information |
| 8.14 | Redondance des installations de traitement de l'information |

9. Gestion des incidents

Tout événement suspect est signalé à [CANAL]. Les incidents significatifs sont notifiés au CCB selon les délais 24 h / 72 h / 1 mois.

Contrôles ISO 27001:2022 concernés

- | | |
|------|---|
| 5.24 | Planification et préparation de la gestion des incidents de sécurité de l'information |
| 5.25 | Évaluation et décision sur les événements de sécurité de l'information |
| 5.26 | Réponse aux incidents de sécurité de l'information |

- 5.27 Tirer les leçons des incidents de sécurité de l'information
- 6.8 Rapports d'événements de sécurité de l'information

10. Fournisseurs

Les fournisseurs sont inventoriés et classés par criticité. Les exigences de sécurité figurent au contrat, avec un délai de notification d'incident compatible avec le nôtre.

Contrôles ISO 27001:2022 concernés

- 5.19 Sécurité de l'information dans les relations avec les fournisseurs
- 5.20 Traiter la sécurité de l'information dans les accords avec les fournisseurs
- 5.21 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC
- 5.22 Surveillance, revue et gestion du changement des services fournisseurs
- 5.23 Sécurité de l'information pour l'utilisation de services cloud

11. Personnel

Vérifications à l'embauche proportionnées au poste, engagements contractuels, sensibilisation *[FRÉQUENCE]* dirigeants compris, et procédure de départ tracée.

Contrôles ISO 27001:2022 concernés

- 6.1 Sélection
- 6.2 Termes et conditions d'emploi
- 6.3 Sensibilisation, éducation et formation à la sécurité de l'information
- 6.5 Responsabilités après la cessation ou le changement d'emploi

12. Contrôle de l'application

Programme d'audit interne pluriannuel fondé sur le risque, mené par une personne indépendante du domaine audité. Les écarts font l'objet d'un plan daté.

Contrôles ISO 27001:2022 concernés

- 5.35 Revue indépendante de la sécurité de l'information
- 5.36 Conformité aux politiques, règles et normes de sécurité de l'information

13. Approbation

RÔLE	NOM	DATE	SIGNATURE
Rédacteur			
Responsable sécurité			
Organe de direction			