| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P12S | | | | | Titre du document :<br>**Politique de gestion des actifs** | | | | | | | |
| Version :<br>1.0 | | Date d'entrée en vigueur :<br>01.01.2025 | | | Propriétaire du document : | | | | | | | |
| X | Politique | | Norme | | Procédure | | Formulaire | | Registre | | Autre | |

| **Historique des révisions** | | | | |
|---|---|---|---|---|
| **Numéro de révision** | **Date de révision** | **Modifications** | **Revu par** | **Propriétaire du processus** |
| | | | | |
| | | | | |

| **Approbations** | | | |
|---|---|---|---|
| **Nom** | **Fonction** | **Date** | **Signature** |
| | | | |
| | | | |

**Mentions légales (droits d'auteur et restrictions d'utilisation)**

(C) 2025 Clarysec LLC. All rights reserved.

Le présent document est la propriété intellectuelle de Clarysec LLC. Aucune partie de ce document ne peut être copiée, réutilisée, distribuée ou modifiée à des fins commerciales ou de mise en œuvre sans autorisation écrite expresse préalable.

Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.

Pour toute demande de licence, contactez : info@clarysec.com

Alignement sur les normes et réglementations

| Norme/Réglementation | Clause/Article | Commentaire |
|---|---|---|
| ISO/IEC 27001:2022 | Clause 8 | Exigences relatives à la gestion des actifs |
| ISO/IEC 27002:2022 | Mesure 5 | Contrôles de gestion des actifs |
| NIST SP 800-53 Rev.5 | CM-8 | Inventaire des composants des systèmes |
| NIS2 de l'UE | Article 21(2)(a) | Suivi des actifs pour la protection des systèmes d'information et des réseaux |
| DORA de l'UE | Article 5(8) | Exigences relatives à l'inventaire des actifs TIC |
| COBIT 2019 | BAI | Cycle de vie de la gestion des actifs informatiques |
| RGPD de l'UE | Article 30 | Inventaire des activités de traitement des données |

**1. Objet**

1.1 La présente politique définit la manière dont l'organisation identifie, suit, protège et retire du service ses actifs informationnels, y compris leurs composantes physiques et numériques.

1.2 Elle vise à réduire les risques opérationnels et de sécurité en assurant la visibilité, l'attribution des responsabilités et le traitement sécurisé de l'information pour l'ensemble des actifs métier tout au long de leur cycle de vie.

1.3 Un inventaire des actifs fiable contribue à la conformité réglementaire, à la réponse aux incidents, à la planification de la continuité d'activité et à la gestion des risques.

1.4 La présente politique soutient également la certification ISO/IEC 27001 et démontre l'alignement avec les obligations juridiques, financières et de cybersécurité prévues par des référentiels tels que le RGPD, NIS2 et DORA.

1.5 Pour les petites et moyennes entreprises (PME), une approche simple mais systématique de la gestion des actifs est essentielle afin d'éviter les équipements non gérés, les pertes de données ou les échecs d'audit, en particulier lorsque les ressources techniques sont limitées.

**2. Champ d'application**

**2.1 La présente politique s'applique à tous les actifs détenus, loués ou autrement gérés par l'organisation, y compris ceux utilisés dans les contextes suivants :**

2.1.1 Activités réalisées dans les bureaux

2.1.2 Équipements utilisés en télétravail ou en mode hybride

2.1.3 Opérations sur le terrain ou mobiles

2.1.4 Environnements cloud et externalisés

**2.2 Les catégories d'actifs couvertes comprennent notamment :**

2.2.1 Matériel : ordinateurs portables, postes fixes, écrans, téléphones, tablettes, clés USB, routeurs, imprimantes, supports de sauvegarde

2.2.2 Logiciels : applications installées, services SaaS, systèmes d'exploitation, antivirus, licences

2.2.3 Actifs informationnels : dépôts de données métier, feuilles de calcul, dossiers clients, code source

2.2.4 Identifiants et services numériques : noms de domaine, certificats numériques, clés API, comptes de messagerie, accès aux services cloud

2.2.5 Moyens d'accès : clés, cartes à puce, badges d'accès, jetons biométriques

2.3 Tous les employés, prestataires et fournisseurs tiers qui manipulent des actifs de l'organisation entrent dans le champ d'application de la présente politique.

2.4 La politique couvre également les actifs à court terme (par exemple, les ordinateurs portables affectés à un projet) et les actifs à long terme, ainsi que les actifs partagés utilisés par plusieurs membres du personnel.

**3. Objectifs**

3.1 Établir et maintenir un inventaire des actifs complet et exact pour l'ensemble des actifs pertinents, tenu à jour en continu.

3.2 Veiller à ce que chaque actif ait un propriétaire désigné responsable de son utilisation, de son stockage et de sa restitution.

3.3 Classer les actifs en fonction de leur sensibilité, de leur impact sur l'activité ou de leur pertinence réglementaire, afin de permettre des niveaux de protection différenciés.

3.4 Définir des procédures claires pour l'attribution, la réaffectation, la maintenance, le signalement des pertes et le retrait des actifs.

3.5 Veiller à ce que les actifs soient gérés de manière sécurisée tout au long de leur cycle de vie et à ce que les informations qu'ils stockent soient protégées ou supprimées de manière sécurisée lors de leur élimination.

3.6 Réduire la probabilité des incidents de sécurité causés par des ressources de l'organisation non suivies, non restituées ou utilisées à mauvais escient.

3.7 Soutenir la conformité aux lois applicables (par exemple, le principe de responsabilité du RGPD) et aux normes de certification en cybersécurité.

**4. Rôles et responsabilités**

**4.1 Directeur général (DG)**

4.1.1 Est propriétaire de la présente politique et veille à ce que les pratiques de gestion des actifs soient mises en œuvre et appliquées dans l'ensemble de l'organisation.

4.1.2 Revoit et approuve les mises à jour de l'inventaire des actifs, et autorise, lorsque nécessaire, le retrait du service ou le transfert des actifs.

4.1.3 Doit être informé de toute perte, de tout vol ou de tout usage abusif significatif d'actifs.

**4.2 Responsable informatique ou dépositaire des actifs désigné**

4.2.1 Tient à jour l'inventaire des actifs (par exemple dans une feuille de calcul, un système de tickets ou un outil léger de gestion des actifs).

4.2.2 Attribue les propriétaires des actifs et suit les changements de statut (par exemple : nouveau, en service, en réparation, retiré).

4.2.3 Vérifie que tous les actifs attribués sont documentés et rattachés à une personne ou à une unité métier.

4.2.4 Veille à ce que les niveaux de classification soient appliqués et respectés (par exemple : Interne, Confidentiel).

4.2.5 Coordonne la récupération des actifs, leur assainissement et leur désactivation lors du départ ou du retrait.

4.2.6 Signale au DG tout écart non résolu dans l'inventaire des actifs.

[ ... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ... ]

## 9. Exigences de revue et de mise à jour

### 9.1 La présente politique doit faire l’objet d’une revue au moins une fois par an, et chaque fois que :

9.1.1 De nouveaux types de technologies ou d’actifs sont introduits

9.1.2 Les procédures de suivi des actifs évoluent (par exemple : adoption de nouveaux outils ou plateformes)

9.1.3 De nouvelles obligations réglementaires affectent la traçabilité ou l’élimination des actifs

9.1.4 Un incident ou un audit identifie une lacune dans les pratiques actuelles de gestion des actifs

9.2 Les revues doivent associer le DG et le responsable informatique et inclure les mises à jour des procédures de gestion des actifs, des modèles d’inventaire et des consignes de classification.

9.3 Toutes les mises à jour doivent être documentées et communiquées au personnel concerné. Un journal des modifications soumis à gestion de version doit être conservé.

## 10. Politiques associées et articulations

10.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue la responsabilité liée à la propriété des politiques et aux opérations informatiques.

10.2 P4S – Politique de contrôle d’accès : articule l’utilisation des actifs (par exemple : ordinateurs portables, équipements mobiles) avec les droits d’accès des utilisateurs et la gestion des identités.

10.3 P7S – Politique d’intégration et de départ : veille à ce que l’attribution et la récupération des actifs soient intégrées aux processus liés au cycle de vie du personnel.

10.4 P13S – Politique de classification et d’étiquetage des données : définit les règles permettant de déterminer si un actif doit être classé comme Interne ou Confidentiel.

10.5 P30S – Politique de réponse aux incidents : encadre les procédures de réponse lorsqu’un événement lié à un actif entraîne un incident de sécurité ou une violation de la vie privée.

## 11. Normes et référentiels de référence

### 11.1 ISO/IEC 27001

11.1.1 Clause 8.1 : exige des contrôles opérationnels pour gérer les actifs et les protéger tout au long de leur utilisation.

### 11.2 ISO/IEC 27002

11.2.1 Mesure 5.9 : détaille la manière d’identifier, d’attribuer un propriétaire, de classer et de gérer les actifs de manière sécurisée.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8 : exige des organisations qu’elles élaborent et maintiennent un inventaire des composants des systèmes, y compris le matériel, les logiciels et les actifs virtuels.

### 11.4 RGPD de l’UE

11.4.1 Article 30 : exige la documentation des activités de traitement des données, ce qui suppose de savoir où les données sont stockées et sur quels actifs.

### 11.5 NIS2 de l’UE

11.5.1 Article 21(2)(a) : impose des mesures techniques et organisationnelles, y compris le suivi des actifs, pour protéger les systèmes d'information et les réseaux.

### 11.6 DORA de l’UE

11.6.1 Article 5(8) : les entités financières doivent maintenir des inventaires détaillés des actifs TIC dans le cadre de la gestion des risques liés aux TIC.

### 11.7 COBIT 2019

11.7.1 BAI09 : précise que les actifs informatiques doivent être gérés tout au long de leur cycle de vie, de l’acquisition au retrait, avec une propriété clairement définie et des contrôles appropriés.