					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P12					Titre du document : **Politique de gestion des actifs**							
Version : 1.0		Date d'entrée en vigueur : 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**

1. Objet

1.1 La présente politique définit les exigences organisationnelles obligatoires relatives à l'identification, à la classification, à la gestion et à la protection des actifs informationnels tout au long de leur cycle de vie. Elle soutient la gouvernance à l'échelle de l'organisation des actifs matériels, logiciels, des données, cloud et des actifs informationnels immatériels, y compris dans les environnements mobiles, distants et opérés par des tiers.

1.2 La présente politique a pour objet d'assurer une visibilité complète sur le patrimoine informationnel de l'organisation, afin de permettre la mise en œuvre de mesures de sécurité efficaces, l'attribution de la propriété, l'alignement en matière de conformité ainsi qu'une mise hors service ou une élimination responsable.

1.3 La politique est alignée sur la mesure A.5.9 de l'ISO/IEC 27001:2022 en imposant le maintien d'un inventaire centralisé des informations et des autres actifs associés. Elle garantit la responsabilisation en rattachant chaque actif à un propriétaire et en appliquant une protection fondée sur la classification, selon la sensibilité métier et les exigences réglementaires.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel, aux prestataires, aux fournisseurs tiers et aux prestataires de services managés qui gèrent, utilisent, consultent, stockent ou traitent des actifs informationnels détenus ou contrôlés par l'organisation.

2.2 Le champ d'application couvre toutes les catégories d'actifs, notamment :

2.2.1 Actifs physiques : ordinateurs portables, postes de travail, appareils mobiles, supports amovibles, imprimantes, équipements réseau

2.2.2 Actifs numériques : logiciels, applications, images système, bases de données, données de sauvegarde, clés de chiffrement

2.2.3 Actifs informationnels : données structurées et non structurées, rapports, courriels, propriété intellectuelle

2.2.4 Actifs cloud et virtuels : environnements IaaS, SaaS, PaaS, machines virtuelles, conteneurs

2.2.5 Actifs logiques : noms de domaine, licences, comptes utilisateurs, configurations de référence

2.3 La politique régit également les actifs utilisés dans des environnements de télétravail, hybrides ou externalisés, afin de garantir leur protection et leur visibilité même lorsqu'ils ne sont pas physiquement situés dans les locaux de l'organisation.

3. Objectifs

3.1 Maintenir un inventaire des actifs complet, exact et à jour de l'ensemble des actifs informationnels de l'organisation, avec des attributs définis de propriété, de classification et de localisation.

3.2 Désigner des propriétaires d'actifs chargés de la classification, du traitement et de la protection des actifs placés sous leur responsabilité, conformément aux politiques de gouvernance des données et de sécurité.

3.3 Appliquer une classification et un étiquetage appropriés à tous les actifs sur la base de la sensibilité, de la criticité et des exigences réglementaires.

3.4 Protéger les actifs conformément à leur classification et à l'exposition au risque associée, y compris pour le stockage, l'accès, la transmission et l'élimination.

3.5 Imposer des procédures de restitution des actifs et d'élimination sécurisée lors du départ d'un employé, de la fin d'un contrat ou de la clôture du cycle de vie d'un actif.

3.6 Soutenir la conformité réglementaire avec des référentiels tels que l'ISO/IEC 27001, le RGPD, NIS2, DORA et COBIT 2019 au moyen d'une gestion structurée des actifs et de la traçabilité d'audit.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve la Politique de gestion des actifs et veille à l'allocation des ressources nécessaires à sa pleine mise en œuvre.

4.1.2 Assume la responsabilité ultime de la protection et de la gestion des actifs de l'organisation conformément aux obligations réglementaires et contractuelles.

4.2 Responsable de la sécurité des systèmes d'information (RSSI)

4.2.1 Est responsable de la Politique de gestion des actifs et veille à son intégration dans le système de management de la sécurité de l'information (SMSI) de l'organisation.

4.2.2 Examine les exceptions et les écarts à la présente politique et impose des stratégies d'atténuation fondées sur les risques.

4.2.3 Supervise les audits périodiques relatifs à la classification des actifs, à l'intégrité de l'inventaire et à la conformité du cycle de vie 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, ou en réponse à :

9.1.1 des changements dans les obligations légales ou réglementaires affectant la classification des actifs ou les exigences d'inventaire

9.1.2 l'introduction de nouvelles catégories d'actifs ou de nouvelles plateformes de gestion (par exemple, CMDB cloud natives)

9.1.3 des constats d'audit interne ou des incidents de sécurité impliquant une mauvaise gestion des actifs

9.1.4 une restructuration organisationnelle affectant la propriété ou les contrôles du cycle de vie

9.2 Le processus de revue doit être initié par le Responsable des actifs informatiques et coordonné avec le RSSI, les achats, les affaires juridiques et les responsables de département concernés.

9.3 Des revues intermédiaires peuvent également être déclenchées par :

9.3.1 l'acquisition ou la cession d'unités d'activité

9.3.2 des changements de fournisseur affectant les actifs gérés par des tiers

9.3.3 des renouvellements technologiques impliquant une mise hors service ou une attribution d'accès en masse

9.4 Toute révision de la présente politique doit :

9.4.1 faire l'objet d'une gestion de versions et être conservée dans le référentiel du SMSI

9.4.2 être approuvée par la haute direction

9.4.3 inclure un résumé des modifications et leur justification

9.4.4 être communiquée à l'ensemble des parties prenantes concernées, y compris avec mise à jour des procédures ou de la formation aux systèmes lorsque cela est applicable

10. Politiques associées et articulations

10.1 La présente politique s'applique conjointement avec les politiques associées ci-dessous et en soutient l'application :

10.1.1 P4 - Politique de contrôle d'accès : garantit que la visibilité sur les actifs est alignée sur les droits d'accès et les mécanismes de contrôle dans les systèmes et environnements de données.

10.1.2 P7 - Politique d'intégration et de départ : régit l'attribution en temps utile et la restitution des actifs physiques et logiques lors des transitions de personnel.

10.1.3 P13 - Politique de classification et d'étiquetage des données : établit les règles obligatoires de classification des actifs, qui déterminent les procédures d'étiquetage, de traitement et d'élimination.

10.1.4 P14 - Politique de conservation et d'élimination des données : définit les délais et méthodes d'élimination sécurisée des actifs physiques et numériques contenant des informations.

10.1.5 P22 - Politique de journalisation et de surveillance : permet la traçabilité de l'accès aux actifs et de leur usage grâce à la journalisation des systèmes, à la visibilité sur les terminaux et à l'analyse comportementale.

10.1.6 P30 - Politique de réponse aux incidents : soutient le confinement rapide et l'investigation des violations liées aux actifs, telles que la perte d'ordinateurs portables ou de supports de stockage non tracés.

10.2 Ces politiques forment un dispositif de gouvernance cohérent garantissant que les actifs sont gérés de manière sécurisée, inventoriés avec exactitude et traités de manière appropriée tout au long de leur cycle de vie.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des normes de sécurité de l'information et des cadres réglementaires reconnus à l'international qui imposent une gestion robuste des actifs sur l'ensemble du cycle de vie.

11.2 ISO/IEC 27001 :

11.2.1 Clause 8.1 - Exige des organisations qu'elles planifient, mettent en œuvre et maîtrisent les processus nécessaires pour satisfaire aux exigences de sécurité de l'information, y compris celles liées à la gestion du cycle de vie des actifs.

11.3 ISO/IEC 27002:2022 - Mesures 5.9 à 5.11

11.3.1 Mesure 5.9 - Inventaire des informations et autres actifs associés : exige un inventaire à jour et complet de tous les actifs pertinents pour le traitement de l'information.

11.3.2 Mesure 5.10 - Utilisation acceptable des informations et des actifs : soutenue par des règles d'utilisation, des processus de propriété et de restitution.

11.3.3 Mesure 5.11 - Restitution des actifs : mise en œuvre au moyen de procédures formelles de remise et de mise hors service.

11.3.4 Ces mesures établissent des exigences structurées pour identifier, étiqueter, maintenir et suivre les actifs de l'organisation, avec des responsabilités correspondantes pour les propriétaires et les dépositaires tout au long du cycle de vie.

11.4 NIST SP 800-53 Rev.5 :

11.4.1 CM-8 - Inventaire des composants du système : reflété par une gestion centralisée des actifs, une visibilité en temps réel et un rattachement aux configurations opérationnelles.

11.4.2 RA-3 - Évaluation des risques : les inventaires des actifs servent d'éléments de base pour la modélisation des menaces et l'évaluation des risques.

11.4.3 MP-6 - Assainissement des supports : appliqué au moyen des méthodes d'élimination sécurisée définies dans les contrôles du cycle de vie des actifs et dans la politique d'élimination des données.

11.5 RGPD de l'UE (2016/679) :

11.5.1 Article 30 - Registres des activités de traitement : exige que les organisations documentent les systèmes, équipements et référentiels qui stockent ou traitent des données à caractère personnel.

11.5.2 Article 32 - Sécurité du traitement : s'aligne sur l'évaluation des risques fondée sur les actifs et sur des mesures de protection adaptées aux actifs classifiés et aux infrastructures critiques.

11.6 Directive NIS2 de l'UE (2022/2555) :

11.6.1 Article 21(2)(a, b) : impose la visibilité et l'inventaire des actifs comme fondements de l'analyse des risques, de la protection et de la réponse aux incidents de cybersécurité.

11.6.2 Article 21(3) : renforce la nécessité d'une gouvernance structurée des actifs dans le cadre d'une culture organisationnelle de sécurité.

11.7 DORA de l'UE (2022/2554) :

11.7.1 Article 5 - Gouvernance des TIC et contrôle interne : exige des entités financières qu'elles maîtrisent leurs actifs TIC au moyen d'exigences claires d'inventaire, de propriété et de protection.

11.7.2 Article 9 - Cadre de gestion des risques liés aux TIC : établit que les processus de gestion des actifs doivent soutenir l'atténuation des menaces, la planification de la continuité d'activité et la résilience des services.

11.8 COBIT 2019 :

11.8.1 BAI09 - Gérer les actifs : directement aligné sur l'identification structurée, la classification, l'utilisation et l'élimination des actifs de l'entreprise.

11.8.2 DSS01 - Opérations gérées : soutient la mise en œuvre de contrôles garantissant la protection des actifs et une gouvernance opérationnelle continue.

11.8.3 MEA03 - Surveiller, évaluer et apprécier la conformité : garantit l'audit régulier des contrôles de gestion des actifs et de leur efficacité au regard de l'alignement réglementaire.