Politiques relatives à la gestion des actifs

Modèle

Contenu

[Utilisation de ce document 3](#_Toc169269375)

[Autorité et révision 3](#_Toc169269376)

[Contrôle et révision des documents 3](#_Toc169269377)

[Gestion des versions 3](#_Toc169269378)

[Cible 4](#_Toc169269379)

[Définitions 4](#_Toc169269380)

[Responsabilités 4](#_Toc169269381)

[Propriétaires de biens 4](#_Toc169269382)

[Personnel 4](#_Toc169269383)

[Cycle de vie des actifs 5](#_Toc169269384)

[Inventaire des actifs 6](#_Toc169269386)

[Actifs primaires 6](#_Toc169269387)

[Actifs secondaires 7](#_Toc169269388)

[Matériel (virtuel) 7](#_Toc169269389)

[logiciel 7](#_Toc169269390)

[Utilisation et entretien 8](#_Toc169269391)

[Utilisation 8](#_Toc169269392)

[Maintenance préventive 8](#_Toc169269393)

[Maintenance corrective 8](#_Toc169269394)

[Sécurité des actifs 8](#_Toc169269395)

[Sécurité physique 8](#_Toc169269396)

[Sécurité du réseau 8](#_Toc169269397)

[Gestion de l'accès 9](#_Toc169269398)

[Protection des données 9](#_Toc169269399)

[Enlèvement et destruction des biens en toute sécurité 9](#_Toc169269400)

[Enlèvement contrôlé 9](#_Toc169269401)

[Élimination incontrôlée 10](#_Toc169269402)

[Gestion des incidents 10](#_Toc169269403)

[Formation et sensibilisation 10](#_Toc169269404)

[Conformité et audit 10](#_Toc169269405)

[Changements et écarts 10](#_Toc169269406)

# Utilisation de ce document

Ce document contient des lignes directrices et des exemples que les organisations peuvent suivre pour soutenir le développement de leurs propres politiques en matière de gestion du patrimoine d'infrastructure. Le modèle n'est pas exhaustif. La politique de gestion du patrimoine de chaque organisation doit être adaptée à son environnement opérationnel, à ses priorités, à ses ressources et à ses engagements. Ce texte n'est donné qu'à titre d'exemple et ne doit pas servir de base à votre propre politique de gestion du patrimoine d'infrastructure.

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents** |  |
| Auteur |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date d'approbation** | **Approuvé par** | **Description du changement** |
|  |  |  |  |

# Cible

L'objectif de cette politique est d'établir des lignes directrices et des procédures pour la gestion des biens de [l'**organisation], conformément aux** normes ISO 27002, CIS Controls version 8 et IEC 62443. Cette politique vise à garantir la disponibilité, l'intégrité et la confidentialité de tous les actifs physiques et numériques de [l'**organisation]**. Une bonne politique de gestion des actifs est le fondement de la sécurité, de l'efficience et de l'efficacité d'une organisation. Elle fournit une approche structurée de la gestion de tous les actifs, ce qui permet de réaliser des économies, d'améliorer la sécurité, d'assurer la conformité aux réglementations et de mieux gérer les risques. Tout cela contribue à la santé et à la réussite globales de l'organisation.

La présente politique s'applique à tous les employés, contractants et tiers impliqués dans l'utilisation, la gestion, la maintenance ou la sécurité des actifs (informationnels) et des systèmes d'automatisation et de contrôle industriels (IACS) de **[l'organisation].**

Le présent document d'orientation fait partie d'un ensemble de documents d'orientation destinés à aider **[l'organisation]** à mettre en place une stratégie solide en matière de cybersécurité.

# Définitions

|  |  |
| --- | --- |
| **Actifs** | Toutes les données, informations et systèmes d'information détenus ou exploités par **[l'organisation], y compris le** matériel, les logiciels, les bases de données, les réseaux, les noms de domaine, la documentation (physique),... |
| **Actifs critiques** | Les actifs critiques sont des ressources ou des éléments d'une organisation qui sont essentiels à son fonctionnement et à sa réussite. |
| **Actifs du SIGC** | Ensemble du matériel, des logiciels, des composants de réseau et des informations faisant partie des systèmes d'automatisation et de contrôle industriels **[de l'organisme].** |
| **Propriétaire d'actifs** | Personne ou équipe désignée responsable de la gestion d'informations spécifiques et des actifs du SIGC au sein de l'organisation. |
| **Les médias** | Tous les appareils physiques qui stockent des données, tels que les disques durs, les disques SSD, les clés USB, les CD/DVD, les cassettes et les appareils mobiles,... |
| **Données sensibles** | Informations confidentielles, personnellement identifiables ou critiques pour l'entreprise, qui doivent être protégées contre tout accès non autorisé. |

# Responsabilités

Propriétaires de biens   
Ils sont chargés de maintenir l'exactitude des registres des biens, d'identifier les exigences en matière de sécurité et de coordonner l'entretien et les réparations.

Personnel Responsable de l'utilisation et de la maintenance correctes des informations et des actifs du SIGC qui lui sont attribués et de la notification de tout problème ou incident conformément aux politiques en matière de cybersécurité.

# Cycle de vie des actifs

L'identification et le suivi des actifs est un processus important. Pour protéger un réseau, une entreprise doit d'abord savoir ce qui s'y trouve. En outre, de nombreux autres contrôles de sécurité dépendent de l'inventaire des actifs, tels que la gestion des données, la configuration sécurisée des actifs, le contrôle d'accès, etc. La figure ci-dessous présente les principales "étapes" du cycle de vie des actifs.

# 

**Acquisition/développement**

* Acquisition et/ou développement de nouveaux actifs ou acquisition de nouveaux actifs par transfert d'une autre unité opérationnelle.

**Découverte / surveillance / inventaire**

* Identifier les nouveaux actifs en recherchant activement les systèmes connectés au réseau de l'entreprise. Ce processus se déroule en continu tout au long du cycle de vie d'un bien.

**Utilisation**

* L'utilisation autorisée des biens par les utilisateurs. Dans le présent document, les utilisateurs peuvent être des employés (sur site ou à distance), des fournisseurs externes, des contractants, des prestataires de services, des consultants ou d'autres utilisateurs utilisant des biens.

**Enlèvement contrôlé**

* Mettre les biens hors d'usage en toute sécurité.

**Élimination incontrôlée**

* les actifs perdus, volés ou inexpliqués. Au fur et à mesure que l'entreprise se développe, cette question devient récurrente et il vaut la peine de discuter des procédures à suivre avant qu'elle ne devienne un problème

# Inventaire des actifs

Il doit y avoir un inventaire de tous les actifs primaires et auxiliaires (secondaires) pertinents. Les dépendances ou les relations entre les actifs primaires et secondaires sont également identifiées et mises à jour. L'inventaire peut être automatisé ou manuel.

## Actifs primaires

Les actifs primaires sont les données, les informations et les connaissances dont **[l'organisation] a besoin** pour mener à bien ses activités et prendre des décisions. Ils sont toujours stockés, traités ou disponibles quelque part par le biais d'un logiciel, sur papier ou dans l'esprit des gens. Si les actifs primaires sont perturbés, [l'**organisation]** ne peut pas fonctionner, les décisions ne peuvent pas être prises et des problèmes de gestion se posent.

*\*Chaque organisation dispose d'une liste d'actifs primaires différente, en fonction de son secteur d'activité. La liste suivante peut être une source d'inspiration :*

* les données de votre entreprise, les commandes, les contrats, les données relatives aux projets, etc.
* vos coordonnées de client
* les données personnelles de vos employés
* votre expertise spécifique
* les données relatives à vos produits ou technologies (par exemple, le code source)
* les données de connexion (pour les services bancaires, d'autres systèmes)
* toutes les informations marquées comme confidentielles
* processus d'entreprise

La liste doit comporter au moins les informations suivantes pour chaque actif :

* Nom
* Description
* Propriétaire
* Classification de la confidentialité, de l'intégrité et de la disponibilité
* Registres de l'existence de données à caractère personnel
* Géré par
* Fournisseur (le cas échéant)

Les actifs primaires pertinents hébergés ou conservés à l'extérieur doivent également faire partie de l'inventaire et avoir un propriétaire interne. Il s'agit généralement du service responsable du contrat (d'externalisation). Les coordonnées de ce fournisseur doivent être documentées afin qu'il puisse être contacté en cas de besoin.

## Actifs secondaires

Les actifs informationnels de soutien (secondaires) sont les logiciels, le matériel, l'infrastructure physique telle que les salles de serveurs ou d'autres installations, le personnel et les services achetés. Il s'agit de toutes les technologies de l'information et de la communication, de tous les sites ou services dont dépendent les actifs primaires.

En d'autres termes, si un élément de soutien tombe en panne, l'élément principal est également indisponible.

Les moyens de soutien sont censés soutenir les moyens principaux.

### Matériel (virtuel)

Il doit exister un inventaire de tout le matériel (virtuel) nécessaire aux systèmes d'information concernés. Cet inventaire comprend les ordinateurs fixes et portables, les serveurs, les tablettes, les téléphones mobiles, les automates programmables, les capteurs, les actionneurs, les robots, les machines-outils, les commutateurs de réseau, les routeurs et les autres composants ou dispositifs de réseau. L'inventaire doit comprendre au moins les aspects suivants :

* Identifiant de l'actif
* Date d'achat/dépréciation
* Description
* Fabricant
* Numéro de modèle
* Numéro de série
* Version du micrologiciel si disponible
* Nom du propriétaire du bien (par exemple, administrateur, utilisateur), rôle ou unité opérationnelle, le cas échéant.
* Localisation physique des actifs de l'entreprise, le cas échéant
* Adresse physique (Media Access Control (MAC))
* Date d'expiration de la garantie

Il convient d'accorder une attention particulière aux actifs virtuels. Ceux-ci font partie de plateformes Cloud externes (publiques). Il est conseillé d'enregistrer également les spécifications techniques, les informations d'assistance, les informations sur les clients et les fournisseurs, le cas échéant. Le matériel géré en externe (par exemple, le matériel en nuage) doit répondre aux mêmes exigences et la gestion des données doit être garantie par contrat.

**Veillez à ce que les éléments administratifs - tels que les noms de domaine, les clés privées pour les certificats et autres cryptomonnaies - ne soient pas oubliés dans cet inventaire.**

### logiciel

Il convient de dresser un inventaire de tous les logiciels nécessaires aux systèmes d'information concernés. L'inventaire doit comprendre au moins les aspects suivants :

* Nom
* Description
* Propriétaire
* Version
* Informations sur la licence (y compris la durée du contrat, le nombre de licences,...)
* Coordonnées du fournisseur.
* Numéro de contrat.
* En option, vous pouvez également spécifier les dates que le logiciel traite
* Il convient de faire la distinction entre les logiciels non pris en charge et les logiciels non autorisés.

Il est conseillé d'enregistrer également les spécifications techniques et les informations d'assistance, le cas échéant. Les administrateurs externes (SaaS) doivent répondre aux mêmes exigences et cela doit faire partie de l'accord contractuel avec l'administrateur externe.

**[Le service responsable] doit vérifier l'inventaire des biens tous les six mois ou plus souvent.**

# Utilisation et entretien

## Utilisation

* Les utilisateurs doivent manipuler tous les actifs avec précaution.
* Des inspections **[semestrielles]** ou plus fréquentes de chaque actif doivent être effectuées en personne ou à distance, sauf exception autorisée par la direction du contrôle.
* Il incombe au propriétaire de l'actif de.. :
* Garder le contrôle du bien.
* Contactez [le service compétent] en cas de problèmes tels que des dysfonctionnements, des réparations nécessaires, des équipements sous-utilisés ou la perte d'équipements.

## Maintenance préventive

* Une maintenance et des mises à jour régulières des terminaux (ordinateurs portables, ordinateurs de bureau, stations de travail, serveurs, ....) doivent être effectuées pour garantir la sécurité et les performances des actifs, comme décrit dans la [politique relative à la gestion des vulnérabilités et des correctifs.](https://atwork.safeonweb.be/sites/default/files/2024-03/Beleid%20rond%20het%20beheer%20van%20kwetsbaarheden%20en%20patches.docx)
* Tous les travaux d'entretien doivent être documentés. Cette documentation peut être conservée dans un registre séparé ou dans l'inventaire déjà existant.

## Maintenance corrective

* Tout défaut ou incident de sécurité lié aux actifs doit être traité et documenté immédiatement.
* Les incidents doivent être analysés et des mesures correctives appropriées doivent être prises pour éviter qu'ils ne se reproduisent.

# Sécurité des actifs

Sécurité physique

Les actifs doivent être protégés physiquement contre l'accès non autorisé, le vol et les dommages par des mesures telles que le contrôle d'accès, les serrures et les zones de stockage sécurisées.

Sécurité du réseau Il convient de segmenter le réseau afin de séparer les composants critiques du SIGC des autres segments du réseau. Des pare-feu, des systèmes de notification d'intrusion (IDS) et d'autres mesures de sécurité du réseau doivent être mis en œuvre, conformément à [la politique de sécurité du réseau](https://atwork.safeonweb.be/sites/default/files/2024-04/Netwerkbeveiligingsbeleid.docx), afin de protéger l'intégrité et la disponibilité des réseaux.

## Gestion de l'accès

L'accès aux biens doit être géré conformément à la [politique d'accès de l](https://atwork.safeonweb.be/sites/default/files/2024-03/Toegangsbeleid_0.docx)'organisation et aux responsabilités des utilisateurs. Les mécanismes d'authentification et d'autorisation doivent être appliqués conformément à la [politique de l](https://atwork.safeonweb.be/sites/default/files/2024-03/Wachtwoordenbeleid.docx)'organisation en [matière de mots de passe](https://atwork.safeonweb.be/sites/default/files/2024-03/Wachtwoordenbeleid.docx).

## Protection des données

Les données sensibles doivent être cryptées lors de leur transfert et de leur stockage afin d'en garantir la confidentialité. Des sauvegardes des données critiques doivent être effectuées régulièrement, conformément à la [politique de sauvegarde et de récupération.](https://atwork.safeonweb.be/sites/default/files/2024-04/Backup-%20en%20herstelbeleid.docx)

# Enlèvement et destruction des biens en toute sécurité

Les actifs obsolètes, non réparables ou économiquement non viables doivent être éliminés conformément aux procédures établies. Toutes les données contenues dans les appareils numériques doivent être effacées ou détruites en toute sécurité avant d'être éliminées.

## Enlèvement contrôlé

* Les biens (matériels, logiciels) qui sont mis hors service doivent être restitués au **[service responsable]**.
* **[Le service responsable]** doit faire une copie des données de l'utilisateur si nécessaire.
* **[Le service responsable]** est chargé d'effacer en toute sécurité la mémoire primaire du bien, le cas échéant. (cryptage, déchiquetage selon la norme DIN-66399, démagnétiseur,...)
* Supprimez les anciens documents, les notes de politique, les procédures opérationnelles standard, les manuels, ... et conservez un registre de ces documents.
* **[Le service responsable] est** chargé de mettre à jour l'état du bien dans tous les systèmes de gestion de l'entreprise.
* Documenter la sortie de l'actif de l'entreprise dans l'inventaire des actifs.
* Supprimer d'anciens noms de domaine

Même si les noms de domaine ne sont plus utilisés, ils peuvent encore poser problème.

Il existe un risque de détournement de domaine, lorsque des domaines expirés sont achetés par des tiers, souvent des escrocs ou des cybercriminels. Ces derniers peuvent utiliser le domaine à des fins malveillantes telles que des campagnes d'hameçonnage ou la publication de contenus inappropriés. Bon nombre de ces domaines de messagerie électronique reçoivent encore des courriels contenant des informations sensibles (sur les citoyens) et sont souvent liés à des comptes en nuage (tels que Dropbox, OneDrive, iCloud, Google Drive,...) qui peuvent être réinitialisés par le nouveau propriétaire du domaine, en interceptant des liens de récupération de mot de passe.   
Lorsque les noms de domaine ne sont plus utilisés activement, il est fortement recommandé de les conserver sous votre propre contrôle pendant une période de transition.

***N'oubliez pas que le coût d'enregistrement d'un nom de domaine ne s'élève généralement qu'à quelques dizaines d'euros par an - le coût de ce renouvellement supplémentaire ne compense pas les dommages que vous pourriez subir.***

**Pour plus d'informations sur la gestion des anciens noms de domaine, consultez le site de DNS Belgique.**

<https://www.dnsbelgium.be/nl/beheren-domeinnaam/niet-laten-vervallen>

<https://www.dnsbelgium.be/nl/je-domeinnaam-beheren/verwijderen>

## Élimination incontrôlée

* Tous les biens perdus ou volés doivent être immédiatement signalés à **[Le service responsable].**
* Les actifs de l'entreprise doivent également être retirés de l'inventaire.

# Gestion des incidents

Tous les incidents (de sécurité) liés aux actifs doivent être immédiatement signalés et documentés conformément au [plan d'intervention en cas d'incident cybernétique](https://atwork.safeonweb.be/sites/default/files/2024-03/Cyber%20Incident%20Response%20Plan_0.docx) **[de** l'**organisation**]**.**

Les incidents doivent être analysés et des mesures correctives appropriées doivent être prises pour éviter qu'ils ne se reproduisent.

# Formation et sensibilisation

Tous les employés devraient recevoir une formation sur leurs responsabilités en matière de gestion et de sécurité des actifs. Des campagnes de sensibilisation doivent être organisées régulièrement pour souligner l'importance de la sécurité de l'information. Il y aura **4** occasions de formation par an.

Le contenu des [10 règles d'or de la cybersécurité](https://atwork.safeonweb.be/sites/default/files/2024-03/10%20gouden%20regels%20voor%20cyberveiligheid_0.docx) et les enseignements tirés d'un cyber incident seront toujours pris en compte lors de la conception des formations.

Des campagnes de sensibilisation supplémentaires seront préparées si nécessaire.

# Conformité et audit

Des contrôles internes réguliers doivent être mis en place pour garantir le respect de la présente politique et des normes applicables. Toutes les parties prenantes doivent se conformer aux lois et règlements applicables en matière de sécurité de l'information et du SIGC.

# Changements et écarts

Les modifications apportées à cette politique doivent être approuvées par la direction de **[organisation].**

Des dérogations à cette politique ne peuvent être accordées qu'avec l'accord écrit de la **[Fonction]**