Richtlinie zur vermögensverwaltung

Vorlage

Inhalt

[Verwendung dieses Dokuments 3](#_Toc169270233)

[Behörde und Überprüfung 3](#_Toc169270234)

[Dokumentenkontrolle und -prüfung 3](#_Toc169270235)

[Versionsverwaltung 3](#_Toc169270236)

[Ziel 4](#_Toc169270237)

[Definitionen 4](#_Toc169270238)

[Zuständigkeiten 4](#_Toc169270239)

[Eigentümer von Vermögenswerten 4](#_Toc169270240)

[Personal 4](#_Toc169270241)

[Lebenszyklus von Vermögenswerten 5](#_Toc169270242)

[Inventar der Vermögenswerte 6](#_Toc169270244)

[Primäre Vermögenswerte 6](#_Toc169270245)

[Sekundäres Vermögen 7](#_Toc169270246)

[(Virtuelle) Hardware 7](#_Toc169270247)

[Software 7](#_Toc169270248)

[Nutzung und Wartung 8](#_Toc169270249)

[Verwenden Sie 8](#_Toc169270250)

[Vorbeugende Wartung 8](#_Toc169270251)

[Korrigierende Wartung 8](#_Toc169270252)

[Sicherheit der Vermögenswerte 8](#_Toc169270253)

[Physische Sicherheit 8](#_Toc169270254)

[Netzsicherheit Durch 8](#_Toc169270255)

[Verwaltung des Zugangs 8](#_Toc169270256)

[Datenschutz 9](#_Toc169270257)

[Sichere Entfernung und Vernichtung von Vermögenswerten 9](#_Toc169270258)

[Kontrollierte Entfernung 9](#_Toc169270259)

[Unkontrollierte Entfernung 10](#_Toc169270260)

[Management von Zwischenfällen 10](#_Toc169270261)

[Schulung und Sensibilisierung 10](#_Toc169270262)

[Einhaltung der Vorschriften und Prüfung 10](#_Toc169270263)

[Änderungen und Abweichungen 10](#_Toc169270264)

# Verwendung dieses Dokuments

Dieses Dokument enthält Leitlinien und Beispiele, an denen sich Organisationen orientieren können, um die Entwicklung ihrer eigenen Richtlinien für die Vermögensverwaltung zu unterstützen. Die Vorlage ist nicht erschöpfend. Die Richtlinien jeder Organisation im Bereich der Vermögensverwaltung sollte auf ihr einzigartiges Betriebsumfeld, ihre Prioritäten, Ressourcen und Verpflichtungen zugeschnitten sein. Dieser Text ist nur als Beispiel gedacht und sollte nicht als Grundlage für Ihre eigene vermögensverwaltungsrichtlinie verwendet werden.

# Behörde und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung** |  |
| Autor |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von |  |
| Datum der letzten Überarbeitung |  |

.

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum der Genehmigung** | **Genehmigt durch** | **Beschreibung der Änderung** |
|  |  |  |  |

# Ziel

Zweck dieser Richtlinie ist es, Richtlinien und Verfahren für die Verwaltung von Vermögenswerten bei **[Organisation] in Übereinstimmung mit den** Standards ISO 27002, CIS Controls Version 8 und IEC 62443 festzulegen. Diese Richtlinie soll die Verfügbarkeit, Integrität und Vertraulichkeit aller physischen und digitalen Assets von **[Organisation]** sicherstellen. Eine gute Vermögensverwaltungspolitik ist eine Grundlage für die Sicherheit, Effizienz und Effektivität einer Organisation. Sie bietet einen strukturierten Ansatz für die Verwaltung aller Vermögenswerte, der zu Kosteneinsparungen, höherer Sicherheit, Einhaltung von Vorschriften und besserem Risikomanagement führt. All dies trägt zur allgemeinen Gesundheit und zum Erfolg der Organisation bei.

Diese Politik gilt für alle Mitarbeiter, Auftragnehmer und Dritte, die an der Nutzung, Verwaltung, Wartung oder Sicherheit der (Informations-)Vermögenswerte und der industriellen Automatisierungs- und Steuerungssysteme (ICS) **der [Organisation]** beteiligt sind**.**

Dieses Strategiedokument ist Teil einer Reihe von Strategiedokumenten, die **[Organisation]** bei der Entwicklung einer soliden Cybersicherheitsstrategie unterstützen.

# Definitionen

|  |  |
| --- | --- |
| **Vermögenswerte** | Alle Daten, Informationen und Informationssysteme, die Eigentum von **[Organisation]** sind oder von ihr betrieben werden**, einschließlich** Hardware, Software, Datenbanken, Netzwerke, Domänennamen, (physische) Dokumentation,... |
| **Kritische Vermögenswerte** | Kritische Vermögenswerte sind Ressourcen oder Teile einer Organisation, die für deren Betrieb und Erfolg unerlässlich sind. |
| **InVeKoS-Vermögenswerte** | Alle Hardware-, Software-, Netzkomponenten und Informationen, die zu den industriellen Automatisierungs- und Steuerungssystemen **der [Organisation]** gehören**.** |
| **Eigentümer des Vermögens** | Eine Person oder ein Team, das für die Verwaltung bestimmter Informationen und ICS-Vermögenswerte innerhalb der Organisation zuständig ist. |
| **Medien** | Alle physischen Geräte, die Daten speichern, wie Festplatten, SSDs, USB-Sticks, CDs/DVDs, Bänder und mobile Geräte,... |
| **Sensible Daten** | Informationen, die vertraulich, persönlich identifizierbar oder geschäftskritisch sind und vor unbefugtem Zugriff geschützt werden müssen. |

# Zuständigkeiten

Eigentümer von Vermögenswerten   
Verantwortlich für die Richtigkeit der Vermögensregister, die Ermittlung von Sicherheitsanforderungen und die Koordinierung von Wartung und Reparatur.

Personal Verantwortlich für die ordnungsgemäße Nutzung und Pflege der zugewiesenen Informationen und ICS-Vermögenswerte sowie für die Meldung von Problemen oder Vorfällen im Einklang mit den Cybersicherheitsrichtlinien.

# Lebenszyklus von Vermögenswerten

Die Identifizierung und Verfolgung von Vermögenswerten ist ein wichtiger Prozess. Um ein Netzwerk zu schützen, muss ein Unternehmen zunächst wissen, was sich im Netzwerk befindet. Darüber hinaus hängen viele andere Sicherheitskontrollen von der Bestandsaufnahme der Assets ab, z. B. die Datenverwaltung, die sichere Konfiguration von Assets, die Zugriffskontrolle und vieles mehr. Die folgende Abbildung zeigt die wichtigsten "Schritte" des Lebenszyklus von Vermögenswerten.

# 

**Akquisition/Entwicklung**

* Erwerb und/oder Entwicklung neuer Vermögenswerte oder Erwerb neuer Vermögenswerte durch Übertragung von einer anderen Geschäftseinheit.

**Entdeckung / Überwachung / Bestandsaufnahme**

* Identifizierung neuer Anlagen durch aktive Suche nach Systemen, die mit dem Unternehmensnetz verbunden sind. Dieser Prozess findet kontinuierlich während des gesamten Lebenszyklus eines Assets statt.

**Verwendung**

* Die autorisierte Nutzung von Anlagen durch Benutzer. In diesem Dokument kann es sich bei den Nutzern um Mitarbeiter (vor Ort oder aus Distanz), externe Lieferanten, Auftragnehmer, Dienstleister, Berater oder andere Nutzer handeln, die Anlagen nutzen.

**Kontrollierte Entfernung**

* Sichere Außerbetriebsetzung von Anlagen.

**Unkontrollierte Entfernung**

* Verlorene, gestohlene oder anderweitig ungeklärte Vermögenswerte. Wenn ein Unternehmen wächst, wird dies zu einem regelmäßigen Problem, und es lohnt sich, die entsprechenden Verfahren zu besprechen, bevor es zu einem Problem wird

# Inventar der Vermögenswerte

Es sollte ein Inventar aller relevanten primären und unterstützenden (sekundären) Vermögenswerte vorhanden sein. Abhängigkeiten oder Beziehungen zwischen unterstützenden und primären Vermögenswerten werden ebenfalls ermittelt und auf dem neuesten Stand gehalten. Eine Inventarisierung kann automatisiert oder manuell erfolgen.

## Primäre Vermögenswerte

Primäre Vermögenswerte sind die Daten, Informationen und das Wissen, die **[Organisation] benötigt**, um ihre Tätigkeiten auszuführen und Entscheidungen zu treffen. Sie sind immer irgendwo gespeichert, verarbeitet oder verfügbar, sei es durch Software, auf Papier oder in den Köpfen der Menschen. Wenn die primären Vermögenswerte gestört sind, kann die **[Organisation]** nicht arbeiten, und es können keine Entscheidungen getroffen werden, was zu Managementproblemen führt.

*\*Jede Organisation hat je nach Branche eine andere Liste von Primärwerten. Die folgende Liste kann als Quelle der Inspiration dienen:*

* Ihre Unternehmensdaten, Aufträge, Verträge, Projektdaten usw.
* Ihre Kundendaten
* persönliche Daten Ihrer Mitarbeiter
* Ihr spezifisches Fachwissen
* Daten über Ihre Produkte oder Technologien (z. B. Quellcode)
* Anmeldedaten (für Bankgeschäfte, andere Systeme)
* alle als vertraulich gekennzeichneten Informationen
* Geschäftsabläufe

Die Liste sollte für jeden Vermögenswert mindestens die folgenden Informationen enthalten:

* Name
* Beschreibung
* Eigentümer
* Klassifizierung von Vertraulichkeit, Integrität und Verfügbarkeit
* Aufzeichnungen über das Vorhandensein von personenbezogenen Daten
* Verwaltet von
* Lieferant (falls zutreffend)

Relevante primäre Vermögenswerte, die extern gehostet oder gepflegt werden, sollten ebenfalls Teil des Inventars sein und einen internen Eigentümer haben. Dies ist in der Regel die für den (Outsourcing-)Vertrag zuständige Abteilung. Dieser Anbieter sollte mit Kontaktangaben dokumentiert werden, damit er bei Bedarf kontaktiert werden kann.

## Sekundäres Vermögen

Zu den unterstützenden (sekundären) Informationsgütern gehören Software, Hardware, physische Infrastrukturen wie Serverräume oder andere Einrichtungen, Mitarbeiter und zugekaufte Dienstleistungen. Dies sind alle Informations- und Kommunikationstechnologien, Standorte oder Dienste, von denen die primären Ressourcen abhängen.

Mit anderen Worten: Wenn eine unterstützende Anlage ausfällt, ist auch die primäre Anlage nicht verfügbar.

Die Hilfsmittel sollen die Hauptmittel unterstützen.

### (Virtuelle) Hardware

Es sollte ein Inventar der gesamten (virtuellen) Hardware vorhanden sein, die für die relevanten Informationssysteme benötigt wird. Dieses Inventar umfasst stationäre und tragbare Computer, Server, Tablets, Mobiltelefone, speicherprogrammierbare Steuerungen (SPS), Sensoren, Aktoren, Roboter, Werkzeugmaschinen, Netzwerk-Switches, Router und andere Netzwerkkomponenten oder -geräte. Das Inventar sollte mindestens die folgenden Aspekte umfassen:

* Anlagenkennzeichen
* Datum der Anschaffung/Abschreibung
* Beschreibung
* Hersteller
* Modellnummer
* Seriennummer
* Firmware-Version, falls vorhanden
* Name des Asset-Eigentümers (z. B. Administrator, Benutzer), Rolle oder Geschäftseinheit, falls zutreffend.
* Physischer Standort der Vermögenswerte des Unternehmens, falls zutreffend
* Physikalische Adresse (Media Access Control (MAC))
* Ablaufdatum der Garantie

Virtuellen Vermögenswerten sollte ausreichend Aufmerksamkeit gewidmet werden. Diese sind Teil von externen (öffentlichen) Cloud-Plattformen. Es ist ratsam, auch technische Spezifikationen, Support-Informationen, Kunden- und ggf. Lieferanteninformationen zu erfassen. Extern verwaltete Hardware (z.B. Cloud-Hardware) sollte die gleichen Anforderungen erfüllen und die Datenverwaltung sollte vertraglich zugesichert werden. Natürlich können IKT-Asset-Management-Tools in Betracht gezogen werden.

**Stellen Sie sicher, dass administrative Elemente - wie Domänennamen, private Schlüssel für Zertifikate und andere Kryptowährungen - nicht vergessen werden, in dieses Inventar aufgenommen zu werden.**

### Software

Es sollte ein Inventar der gesamten für die jeweiligen Informationssysteme erforderlichen Software erstellt werden. Das Inventar sollte mindestens die folgenden Aspekte umfassen:

* Name
* Beschreibung
* Eigentümer
* Version
* Lizenzinformationen (einschließlich Vertragslaufzeit, Anzahl der Lizenzen,...)
* Kontaktdaten des Lieferanten.
* Vertragsnummer.
* Optional können Sie auch angeben, welche Daten die SW verarbeitet
* Es ist zu unterscheiden zwischen nicht unterstützter Software und nicht zugelassener Software.

Es ist ratsam, auch die technischen Spezifikationen und ggf. die Supportinformationen zu erfassen. Externe Administratoren (SaaS) sollten die gleichen Anforderungen erfüllen und dies sollte Teil der vertraglichen Vereinbarung mit dem externen Administrator sein.

**[Die zuständige Abteilung] sollte das Inventar der Vermögenswerte alle sechs Monate oder öfter überprüfen.**

# Nutzung und Wartung

## Verwenden Sie

* Die Benutzer sollten mit allen Vermögenswerten vorsichtig umgehen.
* **Die [halbjährlichen]** oder häufigeren Inspektionen jedes Vermögenswerts müssen persönlich oder aus der Ferne durchgeführt werden, es sei denn, die Aufsichtsbehörde hat eine Ausnahme genehmigt.
* Es liegt in der Verantwortung des Eigentümers der Anlage:
* Die Kontrolle über den Vermögenswert zu behalten.
* Sich bei Problemen wie Funktionsstörungen, notwendigen Reparaturen und nicht ausgelasteten Geräten oder bei Verlust von Geräten an **[den zuständigen Dienst]** zu wenden.

## Vorbeugende Wartung

* Die Endgeräte (Laptops, Desktops, Workstations, Server, ....) sollten regelmäßig gewartet und aktualisiert werden, um die Sicherheit und die Leistung der Anlagen zu gewährleisten, wie in der [Richtlinie über die Verwaltung von Schwachstellen und Patches](https://atwork.safeonweb.be/sites/default/files/2024-03/Beleid%20rond%20het%20beheer%20van%20kwetsbaarheden%20en%20patches.docx) beschrieben.
* Alle Wartungsarbeiten sollten dokumentiert werden. Dies kann in einem separaten Logbuch oder in dem bereits vorhandenen Inventar erfolgen.

## Korrigierende Wartung

* Alle Mängel oder Sicherheitsvorfälle im Zusammenhang mit Assets sollten sofort behoben und dokumentiert werden.
* Die Vorfälle sollten analysiert und geeignete Abhilfemaßnahmen getroffen werden, um eine Wiederholung zu verhindern.

# Sicherheit der Vermögenswerte

Physische Sicherheit

Vermögenswerte sollten durch Maßnahmen wie Zugangskontrollen, Schlösser und sichere Lagerbereiche physisch gegen unbefugten Zugang, Diebstahl und Beschädigung gesichert werden.

Netzsicherheit Durch Netzsegmentierung sollten kritische ICS-Komponenten von anderen Netzsegmenten getrennt werden. Firewalls, Intrusion Detection Systems (IDS) und andere Netzwerksicherheitsmaßnahmen sollten wie in [der Netzwerksicherheitspolitik](https://atwork.safeonweb.be/sites/default/files/2024-04/Netwerkbeveiligingsbeleid.docx) beschrieben implementiert werden, um die Integrität und Verfügbarkeit der Netzwerke zu schützen

## Verwaltung des Zugangs

Der Zugang zu den Assets sollte in Übereinstimmung mit den Benutzerzuständigkeiten [der Access Policy](https://atwork.safeonweb.be/sites/default/files/2024-03/Toegangsbeleid_0.docx) der Organisation gehandhabt werden. Die Authentifizierungs- und Autorisierungsmechanismen sollten in Übereinstimmung mit den [Passwortrichtlinien der](https://atwork.safeonweb.be/sites/default/files/2024-03/Wachtwoordenbeleid.docx) Organisation angewandt werden.

## Datenschutz

Sensible Daten sollten während der Übertragung und Speicherung verschlüsselt werden, um die Vertraulichkeit zu gewährleisten. Von kritischen Daten sollten regelmäßig Sicherungskopien erstellt werden, wie in der [Sicherungs- und Wiederherstellungsrichtlinie](https://atwork.safeonweb.be/sites/default/files/2024-04/Backup-%20en%20herstelbeleid.docx) beschrieben[.](https://atwork.safeonweb.be/sites/default/files/2024-04/Backup-%20en%20herstelbeleid.docx)

# Sichere Entfernung und Vernichtung von Vermögenswerten

Veraltete, nicht mehr zu reparierende oder wirtschaftlich unrentableVermögenswerte sollten gemäß den festgelegten Verfahren entsorgt werden. Alle Daten auf digitalen Geräten sollten vor der Entsorgung sicher gelöscht oder vernichtet werden.

## Kontrollierte Entfernung

* Vermögenswerte (Hardware, Software), die stillgelegt oder außer Betrieb genommen werden, müssen an **[die zuständige Dienststelle]** zurückgegeben werden.
* **[Die zuständige Abteilung]** sollte bei Bedarf eine Kopie der Benutzerdaten anfertigen.
* **Die [zuständige Abteilung]** ist für die sichere Löschung des Primärspeichers innerhalb der Anlage verantwortlich, falls zutreffend. (Verschlüsselung, Schreddern nach DIN-66399, Degausser, ...)
* Löschen Sie alte Dokumente, Richtlinienvermerke, Standardarbeitsanweisungen, Handbücher usw. und führen Sie darüber ein Protokoll.
* **Die [zuständige Abteilung]** ist für die Aktualisierung des Status des Vermögenswerts in allen Geschäftsverwaltungssystemen verantwortlich.
* Dokumentieren Sie die Entfernung des Vermögenswerts aus dem Unternehmen im Rahmen des Inventars.
* Alte Domänennamen löschen

Auch wenn die Domänennamen nicht mehr in Gebrauch sind, könnte dies ein Problem darstellen.

Es besteht die Möglichkeit des Domain-Hijackings, bei dem abgelaufene Domains von Dritten, oft Betrügern oder Cyberkriminellen, aufgekauft werden. Diese können die Domäne für bösartige Zwecke wie Phishing-Kampagnen oder die Veröffentlichung unangemessener Inhalte nutzen. Viele dieser E-Mail-Domänen erhalten immer noch E-Mails mit sensiblen (Bürger-)Informationen und sind oft mit Cloud-Konten (wie Dropbox, OneDrive, iCloud, Google Drive,...) verknüpft, die vom neuen Eigentümer der Domäne durch Abfangen von Passwort-Wiederherstellungslinks zurückgesetzt werden können.   
Wenn Domänennamen nicht mehr aktiv genutzt werden, wird dringend empfohlen, sie für eine Übergangszeit in der eigenen Kontrolle zu behalten.

***Denken Sie daran: Die Kosten für die Registrierung eines Domänennamens belaufen sich in der Regel nur auf einige Dutzend Euro pro Jahr - die Kosten für diese zusätzliche Verlängerung wiegen den Schaden, der Ihnen entstehen kann, nicht auf.***

**Weitere Informationen zur Verwaltung alter Domänennamen finden Sie bei DNS Belgium**

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

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

## Unkontrollierte Entfernung

* Alle verlorenen oder gestohlenen Gegenstände sind unverzüglich **[der zuständigen Dienststelle] zu** melden**.**
* Auch das Betriebsvermögen sollte aus dem Inventar entfernt werden.

# Management von Zwischenfällen

Alle (Sicherheits-)Vorfälle im Zusammenhang mit Vermögenswerten müssen unverzüglich gemäß dem [Reaktionsplan für Cyber-Vorfälle](https://atwork.safeonweb.be/sites/default/files/2024-03/Cyber%20Incident%20Response%20Plan_0.docx) der **[Organisation**] gemeldet und dokumentiert werden**.**

Die Vorfälle sollten analysiert und geeignete Abhilfemaßnahmen getroffen werden, um eine Wiederholung zu verhindern.

# Schulung und Sensibilisierung

Alle Mitarbeiter sollten in ihrer Verantwortung für die Verwaltung und Sicherheit von Vermögenswerten geschult werden. Es sollten regelmäßige Sensibilisierungskampagnen durchgeführt werden, um die Bedeutung der Informationssicherheit zu unterstreichen. Es sind **4** Schulungen pro Jahr vorgesehen.

Der Inhalt der [10 goldenen Regeln der Cybersicherheit](https://atwork.safeonweb.be/sites/default/files/2024-03/10%20gouden%20regels%20voor%20cyberveiligheid_0.docx) und die Ergebnisse der bei einem Cybervorfall gemachten Erfahrungen werden bei der Gestaltung von Schulungsangeboten stets berücksichtigt.

Falls erforderlich, werden zusätzliche Sensibilisierungskampagnen vorbereitet.

# Einhaltung der Vorschriften und Prüfung

Es sollten regelmäßige interne Kontrollen durchgeführt werden, um die Einhaltung dieser Politik und der einschlägigen Normen zu gewährleisten. Alle Beteiligten müssen die geltenden Gesetze und Vorschriften zur Informations- und ICS-Sicherheit einhalten.

# Änderungen und Abweichungen

Änderungen an dieser Politik müssen von der Leitung der **[Organisation]** genehmigt werden**.**

Abweichungen von dieser Politik dürfen nur mit schriftlicher Zustimmung der **[Funktion]** gewährt werden.