Beleid rond het beheer van assets

 Sjabloon

Contents

[Dit document gebruiken 3](#_Toc169010532)

[Autoriteit en herziening 3](#_Toc169010533)

[Documentcontrole en beoordeling 3](#_Toc169010534)

[Versiebeheer 3](#_Toc169010535)

[Doel 4](#_Toc169010536)

[Definities 4](#_Toc169010537)

[Verantwoordelijkheden 4](#_Toc169010538)

[Asset Owners 4](#_Toc169010539)

[Medewerkers 4](#_Toc169010540)

[Levenscyclus van assets 5](#_Toc169010541)

[Inventarisatie van Assets 6](#_Toc169010543)

[Primaire assets 6](#_Toc169010544)

[Secundaire assets 7](#_Toc169010545)

[(Virtuele) hardware 7](#_Toc169010546)

[software 7](#_Toc169010547)

[Gebruik en Onderhoud 8](#_Toc169010548)

[Gebruik 8](#_Toc169010549)

[Preventief Onderhoud 8](#_Toc169010550)

[Correctief Onderhoud 8](#_Toc169010551)

[Beveiliging van Assets 8](#_Toc169010552)

[Fysieke Beveiliging 8](#_Toc169010553)

[Netwerkbeveiliging 8](#_Toc169010554)

[Toegangsbeheer 8](#_Toc169010555)

[Gegevensbescherming 9](#_Toc169010556)

[Veilige verwijdering en vernietiging van assets 9](#_Toc169010557)

[Gecontroleerde verwijdering 9](#_Toc169010558)

[Ongecontroleerde verwijdering 9](#_Toc169010559)

[Incidentbeheer 10](#_Toc169010560)

[Training en bewustwording 10](#_Toc169010561)

[Compliance en audit 10](#_Toc169010562)

[Wijzigingen en afwijkingen 10](#_Toc169010563)

# Dit document gebruiken

Dit document bevat richtlijnen en voorbeelden die organisaties kunnen volgen om de ontwikkeling van hun eigen beleid rond asset management te ondersteunen. Het sjabloon is niet uitputtend. Het beleid rond asset management van elke organisatie moet worden aangepast aan de unieke werkomgeving, prioriteiten, middelen en verplichtingen. Deze tekst is alleen bedoeld als voorbeeld en mag niet worden gebruikt als basis voor uw eigen beleid rond asset management.

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole**  |  |
| Auteur  |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door  |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie**  | **Datum van goedkeuring** | **Goedgekeurd door**  | **Beschrijving van verandering** |
|  |  |  |  |

# Doel

Het doel van dit beleid is om richtlijnen en procedures vast te stellen voor het beheer van assets bij **[organisatie],** in overeenstemming met de normen van ISO 27002, CIS Controls versie 8, en IEC 62443. Dit beleid is bedoeld om de beschikbaarheid, integriteit en vertrouwelijkheid van alle fysieke en digitale Assets van **[organisatie]** te waarborgen. Een goed asset management beleid is een fundament voor de beveiliging, efficiëntie, en effectiviteit van een organisatie. Het biedt een gestructureerde aanpak voor het beheer van alle assets, wat leidt tot kostenbesparingen, verbeterde beveiliging, naleving van regelgeving, en beter risicobeheer. Dit alles draagt bij aan de algehele gezondheid en succes van de organisatie.

Dit beleid is van toepassing op alle medewerkers, contractanten en derden die betrokken zijn bij het gebruik, beheer, onderhoud of beveiliging van (informatie) assets en industriële automatiserings- en controlesystemen (IACS) van **[organisatie].**

Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die **[Organisatie]** ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.

# Definities

|  |  |
| --- | --- |
| **Assets** | Alle gegevens, informatie, en informatiesystemen die eigendom zijn van of worden beheerd door **[organisatie],** inclusief hardware, software, databases, netwerken, domeinnamen, (fysieke) documentatie,… |
| **Kritieke assets** | Kritieke assets zijn middelen of onderdelen van een organisatie die essentieel zijn voor de werking en het succes ervan. |
| **IACS-Assets** | Alle hardware, software, netwerkcomponenten, en informatie die deel uitmaken van de industriële automatiserings- en controlesystemen van **[organisatie].** |
| **Asset eigenaar** | Een aangewezen persoon of team verantwoordelijk voor het beheer van specifieke informatie- en IACS-Assets binnen de organisatie. |
| **Media** | Alle fysieke apparaten die gegevens opslaan, zoals harde schijven, SSD's, USB-sticks, CD's/DVD's, tapes en mobiele apparaten,… |
| **Gevoelige Gegevens** | Informatie die vertrouwelijk, persoonlijk identificeerbaar, of bedrijfskritisch is en beschermd moet worden tegen ongeautoriseerde toegang. |

# Verantwoordelijkheden

Asset Owners
Verantwoordelijk voor het onderhouden van de nauwkeurigheid van de asset registers, vaststellen van beveiligingsvereisten, en coördineren van onderhoud en herstel.

Medewerkers
Verantwoordelijk voor het juiste gebruik en onderhoud van toegewezen informatie- en IACS-Assets en het rapporteren van eventuele problemen of incidenten in lijn met het beleid rond cybersecurity.

# Levenscyclus van assets

Het identificeren en traceren van assets is een belangrijk proces. Om een netwerk te beschermen, moet een onderneming eerst weten wat zich op het netwerk bevindt. Daarnaast zijn veel andere beveiligingscontroles afhankelijk van de assetsinventarisatie, zoals gegevensbeheer, veilige configuratie van assets, toegangscontrole en meer. De figuur hieronder toont de belangrijkste "stappen" van de Asset Lifecycle.

#

**Aankoop/ontwikkeling**

* Aankoop en/of ontwikkeling van nieuwe assets of verkrijging van nieuwe assets door overdracht van een andere bedrijfseenheid.

**Discovery / monitoring /inventarisatie**

* Het identificeren van nieuwe assets door actief te zoeken naar systemen die zijn aangesloten op het bedrijfsnetwerk. Dit proces vindt voortdurend plaats gedurende de levenscyclus van een asset.

**Gebruik**

* Het geautoriseerde gebruik van assets door gebruikers. In dit document kunnen gebruikers werknemers zijn (zowel op locatie als op afstand), externe leveranciers, aannemers, dienstverleners, consultants of andere gebruikers die assets gebruiken.

**Gecontroleerde verwijdering**

* Assets op een veilige manier buiten gebruik stellen.

**Ongecontroleerde verwijdering**

* Verloren, gestolen of anderszins onopgehelderde assets. Naarmate een bedrijf groeit, wordt dit een regelmatig terugkerend probleem en het is de moeite waard om de procedures hieromtrent te bespreken voordat het een probleem wordt

# Inventarisatie van Assets

Er moet een inventarisatie zijn van alle relevante primaire en ondersteunende (secundaire) assets. Ook de afhankelijkheden of relaties tussen ondersteunende en primaire assets wordt in kaart gebracht en up to date gehouden. Een inventarisatie kan geautomatiseerd of handmatig worden uitgevoerd.

## Primaire assets

Primaire assets zijn de gegevens, informatie en kennis die **[Organisatie]** nodig heeft om haar activiteiten uit te voeren en beslissingen te nemen. Ze zijn altijd ergens opgeslagen, verwerkt of beschikbaar via software, op papier of in de hoofden van mensen. Als de primaire assets verstoord zijn, kan de **[Organisatie]** niet draaien en kunnen er geen beslissingen worden genomen en managementproblemen ontstaan.

 *\*Elke Organisatie heeft een andere lijst van primaire bedrijfsmiddelen, afhankelijk van de branche. De volgende lijst kan een bron van inspiratie zijn:*

* uw bedrijfsgegevens, orders, contracten, projectgegevens enz.
* uw klantgegevens
* persoonlijke gegevens van uw werknemers
* uw specifieke expertise
* gegevens over uw producten of technologieën (bijv., broncode)
* inloggegevens (voor bankieren, andere systemen)
* alle informatie die als vertrouwelijk is gemarkeerd
* bedrijfsprocessen

De lijst moet ten minste volgende informatie per asset bevatten:

* Naam
* Beschrijving
* Eigenaar
* Classificatie van vertrouwelijkheid, integriteit en beschikbaarheid
* Registratie van het bestaan van persoonlijke gegevens
* Beheerd door
* Leverancier (indien van toepassing)

Relevante primaire assets die extern gehost of onderhouden worden, moeten ook deel uitmaken van de inventaris en moeten ook een interne eigenaar hebben. Dit is meestal de afdeling die verantwoordelijk is voor het (outsourcing)-contract. Deze leverancier moet worden gedocumenteerd met contactgegevens zodat deze kan gecontacteerd worden indien nodig.

## Secundaire assets

Ondersteunende (secundaire) informatiemiddelen zijn software, hardware, fysieke infrastructuur zoals serverruimtes of andere faciliteiten, mensen en ingekochte diensten. Dit zijn alle informatie- en communicatietechnologieën, sites of diensten waarvan de primaire assets afhankelijk zijn.

Met andere woorden, als een ondersteunend asset uitvalt, is de primaire asset ook niet beschikbaar.

Ondersteunende assets worden verondersteld de primaire assets te ondersteunen.

### (Virtuele) hardware

Er moet een inventaris zijn van alle (virtuele) hardware die nodig is voor de relevante informatiesystemen. Deze inventaris omvat vaste en draagbare computers, servers, tablets, mobiele telefoons, programmeerbare logische Controllers (PLC's), sensoren, actuatoren, robots, machinegereedschappen, netwerk switches, routers, en andere netwerkcomponenten of -apparaten. De inventaris moet ten minste de volgende aspecten vermelden:

* Identificatiecode asset
* Datum van aankoop / afschrijving
* Beschrijving
* Fabrikant
* Modelnummer
* Serienummer
* Firmware versie indien aanwezig
* Naam van de eigenaar van het asset (bijv. beheerder, gebruiker), rol of bedrijfseenheid, indien van toepassing.
* Fysieke locatie van bedrijfsactiva, indien van toepassing
* Fysiek (Media Access Control (MAC)) adres
* Vervaldatum garantie

Er dient genoeg aandacht geschonken te worden aan virtuele assets. Deze zijn onderdeel van externe (publieke) Cloudplatformen. Het is aan te raden om ook technische specificaties, ondersteuningsinformatie, klantinformatie en leveranciersinformatie te registreren, indien van toepassing. De hardware die externe beheerd wordt (vb. Cloud hardware) dient aan dezelfde vereisten te voldoen en het beheer van de gegevens dient contractueel verzekerd te worden Uiteraard kunnen hulpmiddelen voor ICT-assets beheer overwogen worden.

**Zorg ervoor dat administratieve zaken -zoals domeinnamen, private Keys voor certificaten en andere crypto- niet vergeten worden om op te nemen in deze inventaris**

### software

Er moet een inventaris zijn van alle software die nodig is voor de relevante informatiesystemen. De inventaris moet ten minste de volgende aspecten vermelden:

* Naam
* Beschrijving
* Eigenaar
* Versie
* Licentie-informatie (inclusief looptijd van het contract, aantal licenties,…)
* Contactgegevens leverancier.
* Contractnummer.
* Optioneel kan er ook aangegeven worden welke data de SW behandelt
* Er zou een onderscheid moeten worden gemaakt tussen niet-ondersteunde software en niet-geautoriseerde software.

Het is aan te raden om ook technische specificaties en ondersteuningsinformatie te registreren, indien van toepassing. De externe beheerders (SaaS) dienen aan dezelfde vereisten te voldoen en dit dient een onderdeel te vormen van de contractuele overeenkomst met de externe beheerder.

**[De verantwoordelijke dienst] moet de inventaris van assets elke zes maanden of vaker controleren.**

# Gebruik en Onderhoud

## Gebruik

* Gebruikers moeten zorgvuldig omgaan met alle assets.
* **[Halfjaarlijkse]** of frequentere controles van elk asset moeten persoonlijk of op afstand worden uitgevoerd, tenzij het toezichthoudend management toestemming heeft gegeven voor een uitzondering.
* Het is de verantwoordelijkheid van de eigenaar van assets om:
* Behoud de controle over het asset.
* Neem contact op met [De verantwoordelijke dienst] bij problemen zoals storingen, noodzakelijke reparaties en onderbenutte apparatuur of bij verlies van apparatuur.

## Preventief Onderhoud

* Regelmatig onderhoud en updates op endpoints (laptops, desktops, werkstations, servers,….) moeten worden uitgevoerd om de beveiliging en prestaties van Assets te waarborgen zoals beschreven in het [Beleid rond vulnerability- en patchmanagement](https://atwork.safeonweb.be/sites/default/files/2024-03/Beleid%20rond%20het%20beheer%20van%20kwetsbaarheden%20en%20patches.docx)
* Alle onderhoudswerkzaamheden moeten worden gedocumenteerd. Dit kan bijgehouden worden in een afzonderlijk logboek of in de reeds bestaande inventaris.

## Correctief Onderhoud

* Eventuele defecten of beveiligingsincidenten met betrekking tot Assets moeten onmiddellijk worden aangepakt en gedocumenteerd.
* Incidenten moeten worden geanalyseerd en passende corrigerende maatregelen moeten worden genomen om herhaling te voorkomen.

# Beveiliging van Assets

Fysieke Beveiliging

Assets moeten fysiek worden beveiligd tegen ongeautoriseerde toegang, diefstal, en beschadiging door middel van maatregelen zoals toegangscontrole, sloten, en beveiligde opslagruimten.

Netwerkbeveiliging
Netwerksegmentatie moet worden toegepast om kritieke IACS-componenten te scheiden van andere netwerksegmenten. Firewalls, intrusiemeldingssystemen (IDS) en andere netwerkbeveiligingsmaatregelen moeten worden geïmplementeerd zoals beschreven in [het Netwerkbeveiligigngsbeleid](https://atwork.safeonweb.be/sites/default/files/2024-04/Netwerkbeveiligingsbeleid.docx) om de integriteit en beschikbaarheid van netwerken te beschermen

## Toegangsbeheer

Toegang tot Assets moet worden behandeld conform [het Toegangsbeleid](https://atwork.safeonweb.be/sites/default/files/2024-03/Toegangsbeleid_0.docx) van de organisatie verantwoordelijkheden van de gebruiker. Authenticatie- en autorisatiemechanismen moeten worden toegepast conform [het wachtwoordenbeleid](https://atwork.safeonweb.be/sites/default/files/2024-03/Wachtwoordenbeleid.docx) van de organisatie.

## Gegevensbescherming

Gevoelige gegevens moeten worden versleuteld tijdens overdracht en opslag om de vertrouwelijkheid te waarborgen. Back-ups van cruciale gegevens moeten regelmatig worden gemaakt zoals beschreven in het [backup- en herstelbeleid.](https://atwork.safeonweb.be/sites/default/files/2024-04/Backup-%20en%20herstelbeleid.docx)

# Veilige verwijdering en vernietiging van assets

Assets die verouderd, niet-repareerbaar of economisch onrendabel zijn, moeten worden afgevoerd volgens de vastgestelde procedures. Alle gegevens op digitale apparaten moeten veilig worden gewist of vernietigd voordat ze worden afgevoerd.

## Gecontroleerde verwijdering

* Assets (hardware, software) die buiten gebruik worden gesteld of buiten gebruik worden gesteld, moeten worden teruggegeven aan **[De verantwoordelijke dienst]**.
* **[De verantwoordelijke dienst]**  moet indien nodig een kopie maken van de gebruikersgegevens.
* **[De verantwoordelijke dienst]**  is verantwoordelijk voor het veilig wissen van het primaire geheugenopslag binnen het asset, indien van toepassing. (encryptie, versnipperen volgens DIN-66399 norm, degausser,…)
* Verwijder oude documenten, beleidsnota’s, standard operationele procedures, handleidingen,… en hou hiervan een logboek bij.
* **[De verantwoordelijke dienst]**  is verantwoordelijk voor het bijwerken van de status van het asset binnen alle bedrijfsbeheersystemen.
* Documenteer de verwijdering van het asset uit de onderneming binnen de inventaris van assets.
* Oude domeinnamen verwijderen

Hoewel de domeinnamen mogelijks niet meer in gebruik zijn, kan het toch een probleem vormen.

 Er bestaat de mogelijkheid tot domeinkaping, waarbij verlopen domeinen worden opgekocht door derden, vaak oplichters of cybercriminelen. Deze kunnen het domein gebruiken voor kwaadwillige doeleinden zoals phishing-campagnes of het plaatsen van ongepaste inhoud. Vele van deze e-maildomeinen ontvangen nog steeds mails met gevoelige (burger)informatie en zijn vaak gekoppeld aan cloud accounts (zoals Dropbox, OneDrive, iCloud, Google Drive,…) die opnieuw ingesteld kunnen worden door de nieuwe eigenaar van het domein, door middel van het onderscheppen van wachtwoordherstellinks.
Wanneer domeinnamen niet meer in actief gebruik zijn, wordt er sterk aangeraden om deze gedurende een overgangsperiode toch nog in eigen beheer te houden.

***Denk eraan: de registratiekost voor een domeinnaam bedraagt meestal slechts enkele tientallen euro per jaar – de kost voor die extra verlenging weegt niet op tegen de schade die je kan lopen.***

**Meer info rond het beheer van oude domeinnamen is terug te vinden bij DNS Belgium**

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

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

## Ongecontroleerde verwijdering

* Alle verloren of gestolen assets moeten onmiddellijk worden gemeld aan de **[De verantwoordelijke dienst].**
* De bedrijfsactiva moeten ook uit de inventaris worden verwijderd.

# Incidentbeheer

Alle (beveiligings)incidenten met betrekking tot Assets moeten onmiddellijk worden gerapporteerd en gedocumenteerd volgens het [Plan voor respons bij cyberincidenten](https://atwork.safeonweb.be/sites/default/files/2024-03/Cyber%20Incident%20Response%20Plan_0.docx) van de **[organisatie].**

Incidenten moeten worden geanalyseerd en passende corrigerende maatregelen moeten worden genomen om herhaling te voorkomen.

# Training en bewustwording

Alle medewerkers moeten training krijgen over hun verantwoordelijkheden met betrekking tot het beheer en de beveiliging van Assets. Regelmatige bewustwordingscampagnes moeten worden gehouden om het belang van informatiebeveiliging te benadrukken. Er worden **4** trainingsmomenten per jaar ingelast.

Bij het opstellen van trainingsmomenten zal er steeds rekening gehouden worden met de inhoud van de [10 Gouden regels voor cyberveiligheid](https://atwork.safeonweb.be/sites/default/files/2024-03/10%20gouden%20regels%20voor%20cyberveiligheid_0.docx) en met de resultaten van de geleerde lessen bij een cyberincident.

Indien nodig zullen er extra bewustwordingscampagnes opgesteld worden.

# Compliance en audit

Regelmatige interne controles moeten worden uitgevoerd om de naleving van dit beleid en de relevante normen te waarborgen. Alle betrokkenen moeten voldoen aan de geldende wet- en regelgeving met betrekking tot informatie- en IACS-beveiliging.

# Wijzigingen en afwijkingen

Wijzigingen in dit beleid moeten worden goedgekeurd door de directie van **[organisatie].**

Afwijkingen van dit beleid kunnen alleen worden toegestaan met schriftelijke toestemming van de **[Functie]**