| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Indsæt navnet på den registrerede juridiske enhed her | | | | | | | |
| Dokumentnummer:<br>P12S | | | | | Dokumenttitel:<br>**Politik for aktiver** | | | | | | | |
| Version:<br>1.0 | | Ikrafttrædelsesdato:<br>01.01.2025 | | | Dokumentejer: | | | | | | | |
| X | Politik | | Standard | | Procedure | | Formular | | Register | | Andet | |

| **Revisionshistorik** | | | | |
|---|---|---|---|---|
| **Revisionsnummer** | **Revisionsdato** | **Ændringer** | **Gennemgået af** | **Procesejer** |
| | | | | |
| | | | | |

| **Godkendelser** | | | |
|---|---|---|---|
| **Navn** | **Stilling** | **Dato** | **Underskrift** |
| | | | |
| | | | |

Tilpasset relevante standarder og krav

| Standard/regulering | Klausul/artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Clause 8 | Krav til styring af aktiver |
| ISO/IEC 27002:2022 | Control 5 | Kontroller for styring af aktiver |
| NIST SP 800-53 Rev. 5 | CM-8 | Aktivfortegnelse over systemkomponenter |
| EU NIS2 | Article 21(2)(a) | Sporing af aktiver til beskyttelse af net- og informationssystemer |
| EU DORA | Article 5(8) | Krav til aktivfortegnelse for IKT-aktiver |
| COBIT 2019 | BAI | Livscyklusstyring af IT-aktiver |
| EU GDPR | Article 30 | Fortegnelse over behandlingsaktiviteter |

## 1. Formål

1.1 Denne politik fastlægger, hvordan organisationen identificerer, registrerer, beskytter og udfaser sine informationsaktiver, herunder både fysiske og digitale komponenter.

1.2 Formålet er at reducere drifts- og sikkerhedsrisici ved at opretholde overblik, ansvar og sikker håndtering af alle forretningsaktiver gennem hele deres livscyklus.

1.3 En pålidelig aktivfortegnelse understøtter efterlevelse af lovkrav, hændelseshåndtering, planlægning af forretningskontinuitet og risikostyring.

1.4 Denne politik understøtter også certificering efter ISO/IEC 27001 og dokumenterer overensstemmelse med juridiske, finansielle og cybersikkerhedsmæssige forpligtelser i henhold til rammeværk som GDPR, NIS2 og DORA.

1.5 For små og mellemstore virksomheder (SMV'er) er en enkel, men systematisk tilgang til styring af aktiver afgørende for at undgå enheder uden forvaltning, datatab eller manglende revisionsberedskab, navnlig når de tekniske personaleressourcer er begrænsede.

## 2. Omfang

**2.1 Denne politik gælder for alle aktiver, der ejes, leases eller på anden måde administreres af organisationen, herunder aktiver, der anvendes i:**

2.1.1 Kontorarbejde

2.1.2 Fjernarbejde eller hybride arbejdsformer

2.1.3 Feltbaserede eller mobile aktiviteter

2.1.4 Cloud- og outsourcede miljøer

**2.2 Omfattede aktivtyper omfatter blandt andet:**

2.2.1 Hardware: bærbare computere, stationære computere, skærme, telefoner, tablets, USB-drev, routere, printere, sikkerhedskopimedier

2.2.2 Software: installerede applikationer, SaaS-værktøjer, operativsystemer, antivirusværktøjer, licenser

2.2.3 Dataaktiver: lagre for forretningsdata, regneark, kunderegistre, kildekode

2.2.4 Digitale legitimationsoplysninger og tjenester: domænenavne, digitale certifikater, API-nøgler, e-mailkonti, cloudloginoplysninger

2.2.5 Adgangsenheder: nøgler, smartcards, adgangsbrikker, biometriske tokens

2.3 Alle medarbejdere, kontrahenter og tredjepartsleverandører, der håndterer organisationens aktiver, er omfattet af denne politik.

2.4 Politikken omfatter både kortvarige aktiver (f.eks. projektspecifikke bærbare computere) og langsigtede aktiver samt delte aktiver, der anvendes af flere medarbejdere.

**3. Mål**

3.1 Etablere og vedligeholde en fuldstændig og korrekt aktivfortegnelse over alle relevante aktiver, som opdateres løbende.

3.2 Sikre, at hvert aktiv har en udpeget ejer med ansvar for brug, opbevaring og tilbagelevering.

3.3 Klassificere aktiver ud fra følsomhed, forretningsmæssig konsekvens eller regulatorisk relevans, så differentierede beskyttelsesniveauer kan anvendes.

3.4 Fastlægge klare procedurer for udlevering, omfordeling, vedligeholdelse, rapportering af tab og udfasning af aktiver.

3.5 Sikre, at aktiver håndteres sikkert gennem hele deres livscyklus, og at oplysninger, de opbevarer, enten beskyttes eller slettes sikkert ved bortskaffelse.

3.6 Reducere sandsynligheden for sikkerhedshændelser forårsaget af aktiver, der ikke er registreret, ikke er tilbageleveret eller misbruges.

3.7 Understøtte efterlevelse af relevante lovkrav (f.eks. GDPR's ansvarlighedsprincip) og certificeringsstandarder inden for cybersikkerhed.

**4. Roller og ansvar**

**4.1 Direktør**

4.1.1 Er ejer af denne politik og ansvarlig for at sikre, at praksis for styring af aktiver implementeres og efterleves i hele organisationen.

4.1.2 Gennemgår og godkender opdateringer til aktivfortegnelsen og godkender udfasning eller overdragelse af aktiver, hvor det er nødvendigt.

4.1.3 Skal orienteres om ethvert væsentligt tab, tyveri eller misbrug af aktiver.

**4.2 IT-ansvarlig eller udpeget aktivforvalter**

4.2.1 Vedligeholder aktivfortegnelsen (f.eks. i et regneark, et sagsstyringssystem eller et enkelt værktøj til aktivsporing).

4.2.2 Tildeler ejerskab til aktiver og registrerer ændringer i status (f.eks. ny, i brug, under reparation, udfaset).

4.2.3 Verificerer, at alle udleverede aktiver er dokumenteret og knyttet til en person eller forretningsenhed.

4.2.4 Sikrer, at klassificeringsmærkninger anvendes og efterleves (f.eks. Intern, Fortrolig).

4.2.5 Koordinerer tilbagelevering, sikker sletning og deaktivering af aktiver i forbindelse med fratrædelse eller udfasning.

4.2.6 Rapporterer alle uafklarede afvigelser i aktivfortegnelsen til direktøren.

[ ... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ... ]

**9. Krav til gennemgang og opdatering**

**9.1 Denne politik skal gennemgås mindst én gang årligt samt når:**

9.1.1 Nye typer teknologi eller aktiver introduceres

9.1.2 Procedurer for aktivsporing ændres (f.eks. ved indførelse af nye værktøjer eller platforme)

9.1.3 Nye regulatoriske forpligtelser påvirker sporbarhed eller bortskaffelse af aktiver

9.1.4 En hændelse eller revision identificerer en mangel i den nuværende praksis for styring af aktiver

9.2 Gennemgange skal involvere direktøren og den IT-ansvarlige og omfatte opdateringer af procedurer for håndtering af aktiver, skabeloner til aktivfortegnelsen og vejledning om klassificering.

9.3 Alle opdateringer skal dokumenteres og kommunikeres til berørte medarbejdere. En ændringslog under versionsstyring skal opbevares.

## 10. Relaterede politikker og sammenhænge

10.1 P2S – Politik for styringsroller og ansvarsområder: Tildeler ansvar for politik-ejerskab og IT-drift.

10.2 P4S – Politik for adgangskontrol: Knytter brug af aktiver (f.eks. bærbare computere og mobile enheder) til adgangsrettigheder og identitetsstyring.

10.3 P7S – Politik for onboarding og fratrædelse: Sikrer, at udlevering og tilbagelevering af aktiver indgår i processerne for medarbejderlivscyklussen.

10.4 P13S – Politik for dataklassificering og mærkning: Fastlægger regler for, om et aktiv skal klassificeres som Internt eller Fortroligt.

10.5 P30S – Politik for hændelsesrespons: Angiver procedurer for respons, hvis en aktivrelateret hændelse medfører et sikkerheds- eller databeskyttelsesbrud.

## 11. Referencestandarder og rammeværk

### 11.1 ISO/IEC 27001

11.1.1 Clause 8.1: Kræver driftsmæssige kontroller til at styre aktiver og beskytte dem gennem hele deres anvendelse.

### 11.2 ISO/IEC 27002

11.2.1 Control 5.9: Beskriver, hvordan aktiver identificeres, tildeles ejerskab, klassificeres og styres sikkert.

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

11.3.1 CM-8: Kræver, at organisationer udvikler og vedligeholder en aktivfortegnelse over systemkomponenter, herunder hardware, software og virtuelle aktiver.

### 11.4 EU GDPR

11.4.1 Article 30: Kræver dokumentation af behandlingsaktiviteter, hvilket afhænger af viden om, hvor data opbevares, og på hvilke aktiver.

### 11.5 EU NIS2

11.5.1 Article 21(2)(a): Kræver tekniske og organisatoriske foranstaltninger, herunder sporing af aktiver, til beskyttelse af net- og informationssystemer.

### 11.6 EU DORA

11.6.1 Article 5(8): Finansielle enheder skal vedligeholde detaljerede fortegnelser over IKT-aktiver som led i styring af IKT-risiko.

### 11.7 COBIT 2019

11.7.1 BAI09: Fastsætter, at IT-aktiver skal styres gennem hele deres livscyklus – fra anskaffelse til udfasning – med klart ejerskab og relevante kontroller.