					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P12					Dokumenttitel: **Politik for styring af aktiver**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

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

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

1. Formål

1.1 Denne politik fastsætter de obligatoriske organisatoriske krav til identifikation, klassificering, styring og beskyttelse af informationsaktiver gennem hele deres livscyklus. Den understøtter organisationsdækkende styring af hardware-, software-, data-, cloud- og immaterielle informationsaktiver, herunder mobile, fjernadministrerede og tredjepartsadministrerede miljøer.

1.2 Formålet med denne politik er at sikre fuld synlighed i organisationens samlede informationsaktivlandskab, så effektive sikkerhedskontroller, tydeligt ejerskab, overholdelse af efterlevelseskrav samt ansvarlig udfasning eller bortskaffelse kan gennemføres.

1.3 Politikken er afstemt med ISO/IEC 27001:2022 Annex A, kontrol 5.9, ved at kræve vedligeholdelse af en centraliseret fortegnelse over information og tilknyttede aktiver. Den sikrer ansvarlighed ved at knytte hvert aktiv til en ejer og anvende klassificeringsbaseret beskyttelse ud fra forretningsmæssig følsomhed og regulatoriske krav.

2. Omfang

2.1 Denne politik gælder for alle medarbejdere, konsulenter, tredjepartsleverandører og tjenesteudbydere, som administrerer, anvender, tilgår, opbevarer eller behandler informationsaktiver, der ejes eller kontrolleres af organisationen.

2.2 Omfanget omfatter alle kategorier af aktiver, herunder:

2.2.1 Fysiske aktiver: bærbare computere, stationære computere, mobile enheder, flytbare medier, printere, netværksudstyr

2.2.2 Digitale aktiver: software, applikationer, systemimages, databaser, sikkerhedskopidata, krypteringsnøgler

2.2.3 Informationsaktiver: strukturerede og ustrukturerede data, rapporter, e-mails, immaterielle rettigheder

2.2.4 Cloud- og virtuelle aktiver: IaaS-, SaaS- og PaaS-miljøer, virtuelle maskiner, containere

2.2.5 Logiske aktiver: domænenavne, licenser, brugerkonti, baselinekonfigurationer

2.3 Politikken omfatter også aktiver, der anvendes i fjernarbejde, hybride arbejdsformer eller outsourcede miljøer, og sikrer beskyttelse og synlighed, også når aktiver ikke er fysisk placeret på organisationens lokationer.

3. Mål

3.1 At opretholde en fuldstændig, nøjagtig og ajourført fortegnelse over alle organisationens informationsaktiver med definerede attributter for ejerskab, klassificering og placering.

3.2 At udpege aktivansvarlige med ansvar for klassificering, håndtering og beskyttelse af de aktiver, der er under deres kontrol, i overensstemmelse med politikker for datastyring og informationssikkerhed.

3.3 At anvende passende klassificering og mærkning på alle aktiver ud fra følsomhed, kritikalitet og regulatoriske hensyn.

3.4 At beskytte aktiver i overensstemmelse med deres klassificering og tilknyttede risikoeksponering, herunder opbevaring, adgang, overførsel og bortskaffelse.

3.5 At håndhæve procedurer for tilbagelevering af aktiver og sikker bortskaffelse ved medarbejderes fratræden, kontraktophør eller afslutning af aktivets livscyklus.

3.6 At understøtte regulatorisk efterlevelse af rammeværk som ISO/IEC 27001, GDPR, NIS2, DORA og COBIT 2019 gennem struktureret aktivstyring og revisionsspor.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender politikken for styring af aktiver og sikrer, at der afsættes ressourcer til fuld implementering.

4.1.2 Har det overordnede ansvar for at sikre, at organisationens aktiver beskyttes og forvaltes i overensstemmelse med regulatoriske og kontraktlige forpligtelser.

4.2 Chief Information Security Officer (CISO)

4.2.1 Er ejer af politikken for styring af aktiver og sikrer integration med organisationens ledelsessystem for informationssikkerhed (ISMS).

4.2.2 Gennemgår undtagelser og afvigelser fra denne politik og håndhæver risikobaserede afbødende foranstaltninger.

4.2.3 Fører tilsyn med periodiske gennemgange af aktivklassificering, aktivfortegnelsens integritet og efterlevelse af krav til aktivets livscyklus.

[... 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 eller som reaktion på:

9.1.1 Ændringer i retlige eller regulatoriske forpligtelser, der påvirker krav til aktivklassificering eller fortegnelser

9.1.2 Indførelse af nye aktivkategorier eller administrationsplatforme (f.eks. cloud-native CMDB'er)

9.1.3 Revisionskonstateringer fra intern revision eller sikkerhedshændelser, der involverer mangelfuld styring af aktiver

9.1.4 Organisatoriske omstruktureringer, der påvirker ejerskab eller livscykluskontroller

9.2 Gennemgangsprocessen skal initieres af IT Asset Manager og koordineres med CISO, Indkøb, Juridisk og relevante afdelingsledere.

9.3 Ekstraordinære gennemgange kan også udløses af:

9.3.1 Overtagelse eller frasalg af forretningsenheder

9.3.2 Leverandørændringer, der påvirker tredjepartsadministrerede aktiver

9.3.3 Teknologifornyelser, der omfatter masseudfasning eller provisionering

9.4 Alle revisioner af denne politik skal:

9.4.1 Være underlagt versionsstyring og opbevares i ISMS-repositoriet

9.4.2 Godkendes af direktionen

9.4.3 Indeholde en sammenfatning af ændringerne og begrundelsen herfor

9.4.4 Kommunikeres til alle berørte interessenter, herunder opdaterede procedurer eller systemtræning, hvor relevant

10. Relaterede politikker og sammenhænge

10.1 Denne politik fungerer sammen med og understøtter håndhævelsen af følgende relaterede politikker:

10.1.1 P4 - Politik for adgangskontrol: Sikrer, at synlighed i aktiver er afstemt med adgangsrettigheder og kontrolmekanismer på tværs af systemer og datamiljøer.

10.1.2 P7 - Politik for onboarding og fratrædelse: Regulerer rettidig tildeling af adgang og tilbagelevering af fysiske og logiske aktiver ved personaleskift.

10.1.3 P13 - Politik for dataklassificering og mærkning: Fastlægger obligatoriske klassificeringsregler for aktiver, som styrer mærkning, håndtering og bortskaffelsesprocedurer.

10.1.4 P14 - Politik for dataopbevaring og databortskaffelse: Definerer tidsfrister og metoder for sikker bortskaffelse af digitale og fysiske aktiver, der indeholder information.

10.1.5 P22 - Politik for logning og overvågning: Muliggør sporbarhed for adgang til og anvendelse af aktiver gennem systemlogning, endepunktssynlighed og adfærdsanalyse.

10.1.6 P30 - Politik for hændelsesrespons: Understøtter hurtig inddæmning og undersøgelse af aktivrelaterede brud, såsom tabte bærbare computere eller ikke-sporede lagringsmedier.

10.2 Disse politikker udgør en sammenhængende styringsstruktur, der sikrer, at aktiver forvaltes sikkert, registreres nøjagtigt og håndteres korrekt gennem hele deres livscyklus.

11. Referencestandarder og rammeværk

11.1 Denne politik er afstemt med internationalt anerkendte standarder for informationssikkerhed og regulatoriske rammeværk, som kræver robust styring af aktiver gennem hele livscyklussen.

11.2 ISO/IEC 27001:

11.2.1 Klausul 8.1 - Kræver, at organisationer planlægger, implementerer og kontrollerer de processer, der er nødvendige for at opfylde krav til informationssikkerhed, herunder krav til styring af aktivets livscyklus.

11.3 ISO/IEC 27002:2022 - Kontroller 5.9 til 5.11

11.3.1 Kontrol 5.9 - Fortegnelse over information og andre tilknyttede aktiver: Kræver en ajourført og fuldstændig fortegnelse over alle aktiver, der er relevante for informationsbehandling.

11.3.2 Kontrol 5.10 - Acceptabel brug af information og aktiver: Understøttes af regler for brug, ejerskab og processer for tilbagelevering.

11.3.3 Kontrol 5.11 - Tilbagelevering af aktiver: Implementeres gennem formelle overdragelses- og udfasningsprocedurer.

11.3.4 Disse kontroller fastlægger strukturerede krav til identifikation, mærkning, vedligeholdelse og sporing af organisationens aktiver samt tilhørende ansvar for ejere og forvaltere gennem hele livscyklussen.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Fortegnelse over systemkomponenter: Afspejles gennem centraliseret styring af aktiver, synlighed i realtid og kobling til driftskonfigurationer.

11.4.2 RA-3 - Risikovurdering: Aktivfortegnelser udgør grundlæggende elementer for trusselsmodellering og risikovurdering.

11.4.3 MP-6 - Medierensning: Håndhæves gennem sikre bortskaffelsesmetoder fastlagt i kontroller for aktivets livscyklus og politikken for databortskaffelse.

11.5 EU GDPR (2016/679):

11.5.1 Artikel 30 - Fortegnelser over behandlingsaktiviteter: Kræver, at organisationer dokumenterer systemer, enheder og repositories, der opbevarer eller behandler personoplysninger.

11.5.2 Artikel 32 - Behandlingssikkerhed: Er afstemt med aktivbaseret risikovurdering og sikkerhedsforanstaltninger tilpasset klassificerede aktiver og kritisk infrastruktur.

11.6 EU NIS2-direktivet (2022/2555):

11.6.1 Artikel 21(2)(a, b): Kræver synlighed i aktiver og fortegnelser som grundlag for risikoanalyse, beskyttelse og respons på cybersikkerhedshændelser.

11.6.2 Artikel 21(3): Understreger nødvendigheden af struktureret styring af aktiver som en del af organisationens sikkerhedskultur.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 5 - IKT-styring og intern kontrol: Kræver, at finansielle enheder kontrollerer IKT-aktiver med klare krav til fortegnelse, ejerskab og beskyttelse.

11.7.2 Artikel 9 - Ramme for styring af IKT-risiko: Fastlægger, at processer for styring af aktiver skal understøtte trusselsreduktion, planlægning af forretningskontinuitet og robusthed i tjenester.

11.8 COBIT 2019:

11.8.1 BAI09 - Manage Assets: Direkte afstemt med struktureret identifikation, klassificering, anvendelse og bortskaffelse af organisationens aktiver.

11.8.2 DSS01 - Managed Operations: Understøtter implementering af kontroller, der sikrer beskyttelse af aktiver og løbende driftsmæssig styring.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Sikrer regelmæssig revision af kontroller for styring af aktiver og deres effektivitet i forhold til regulatorisk overensstemmelse.