					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P12					Dokumenttitel: **Policy för tillgångshantering**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

1. Syfte

1.1 Denna policy fastställer obligatoriska organisatoriska krav för att identifiera, klassificera, hantera och skydda informationstillgångar under hela deras livscykel. Den stödjer organisationsövergripande styrning av hårdvara, programvara, data, molntillgångar samt immateriella informationstillgångar, inklusive mobila miljöer, distansmiljöer och miljöer som hanteras av tredje part.

1.2 Syftet med denna policy är att säkerställa fullständig synlighet i organisationens tillgångslandskap, så att effektiva säkerhetskontroller, tilldelning av ägarskap, uppfyllande av regelefterlevnadskrav samt ansvarsfull avveckling eller bortskaffning möjliggörs.

1.3 Policyn är anpassad till ISO/IEC 27001:2022 bilaga A, kontroll 5.9, genom att kräva att en centraliserad förteckning över information och tillhörande tillgångar upprätthålls. Den säkerställer ansvarstagande genom att koppla varje tillgång till en ägare och tillämpa klassificeringsstyrt skydd baserat på verksamhetsmässig känslighet och regulatoriska krav.

2. Omfattning

2.1 Denna policy gäller för alla anställda, entreprenörer, tredjepartsleverantörer och tjänsteleverantörer som hanterar, använder, har åtkomst till, lagrar eller behandlar informationstillgångar som ägs eller kontrolleras av organisationen.

2.2 Omfattningen inkluderar alla kategorier av tillgångar, såsom:

2.2.1 Fysiska tillgångar: bärbara datorer, stationära datorer, mobila enheter, flyttbara medier, skrivare, nätverksutrustning

2.2.2 Digitala tillgångar: programvara, applikationer, systemavbildningar, databaser, säkerhetskopierade data, krypteringsnycklar

2.2.3 Informationstillgångar: strukturerade och ostrukturerade data, rapporter, e-postmeddelanden, immateriella rättigheter

2.2.4 Moln- och virtuella tillgångar: IaaS-, SaaS- och PaaS-miljöer, virtuella maskiner, containrar

2.2.5 Logiska tillgångar: domännamn, licenser, användarkonton, baskonfigurationer

2.3 Policyn omfattar även tillgångar som används vid distansarbete, i hybridmiljöer eller i outsourcade miljöer och säkerställer skydd och synlighet även när tillgångarna inte är fysiskt placerade i organisationens lokaler.

3. Mål

3.1 Att upprätthålla en fullständig, korrekt och aktuell förteckning över organisationens samtliga informationstillgångar, med definierat ägarskap, klassificering och platsinformation.

3.2 Att utse tillgångsägare som ansvarar för klassificering, hantering och skydd av de tillgångar som står under deras kontroll, i linje med organisationens styrning av data och säkerhetspolicyer.

3.3 Att tillämpa lämplig klassificering och märkning på alla tillgångar utifrån känslighet, kritikalitet och regulatoriska krav.

3.4 Att skydda tillgångar enligt deras klassificering och tillhörande riskexponering, inklusive lagring, åtkomst, överföring och bortskaffning.

3.5 Att säkerställa rutiner för återlämning av tillgångar och säker avveckling vid avslut, upphörande av avtal eller när tillgångens livscykel avslutas.

3.6 Att stödja regelefterlevnad enligt ramverk såsom ISO/IEC 27001, GDPR, NIS2, DORA och COBIT 2019 genom strukturerad tillgångshantering och spårbarhet.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner policyn för tillgångshantering och säkerställer att resurser avsätts för dess fullständiga införande.

4.1.2 Har det yttersta ansvaret för att säkerställa att organisationens tillgångar skyddas och hanteras i enlighet med regulatoriska skyldigheter och avtalskrav.

4.2 Informationssäkerhetschef (CISO)

4.2.1 Äger policyn för tillgångshantering och säkerställer integration med organisationens övergripande ledningssystem för informationssäkerhet (ISMS).

4.2.2 Granskar undantag och avvikelser från denna policy och säkerställer riskbaserade riskreducerande åtgärder.

4.2.3 Utövar tillsyn över periodiska granskningar av tillgångsklassificering, tillgångsförteckningens integritet och efterlevnad av krav genom tillgångarnas livscykel.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas minst årligen, eller som svar på:

9.1.1 Förändringar i rättsliga eller regulatoriska skyldigheter som påverkar klassificering av tillgångar eller krav på tillgångsregister

9.1.2 Införande av nya tillgångskategorier eller plattformar för hantering (t.ex. molnbaserade CMDB-lösningar)

9.1.3 Interna revisionsiakttagelser eller säkerhetsincidenter som rör felaktig hantering av tillgångar

9.1.4 Omstrukturering av organisationen som påverkar ägarskap eller livscykelkontroller

9.2 Granskningsprocessen ska initieras av IT Asset Manager/konfigurationsansvarig och samordnas med informationssäkerhetschef (CISO), upphandling, juridik och berörda avdelningschefer.

9.3 Interimistiska granskningar kan också utlösas av:

9.3.1 Förvärv eller avyttring av verksamhetsenheter

9.3.2 Leverantörsförändringar som påverkar tillgångar som hanteras av tredje part

9.3.3 Teknikförnyelser som innefattar avveckling eller tilldelning i större omfattning

9.4 Alla revideringar av denna policy ska:

9.4.1 Versionshanteras och lagras i ISMS-dokumentregistret

9.4.2 Godkännas av verkställande ledning

9.4.3 Innehålla en ändringssammanfattning och motivering

9.4.4 Kommuniceras till alla berörda intressenter, inklusive uppdaterade rutiner eller systemutbildning där så är tillämpligt

10. Relaterade policyer och kopplingar

10.1 Denna policy gäller tillsammans med och stödjer tillämpningen av följande relaterade policyer:

10.1.1 P4 - Åtkomstkontrollpolicy: Säkerställer att synlighet för tillgångar är i linje med behörigheter och kontrollmekanismer i system och datamiljöer.

10.1.2 P7 - Policy för introduktion och avslut: Reglerar snabb tilldelning och återlämning av fysiska och logiska tillgångar vid personalförändringar.

10.1.3 P13 - Policy för dataklassificering och märkning: Fastställer obligatoriska regler för klassificering av tillgångar, vilka styr märkning, hantering och bortskaffning.

10.1.4 P14 - Policy för databevarande och databortskaffning: Definierar tidsramar och metoder för säker bortskaffning av digitala och fysiska tillgångar som innehåller information.

10.1.5 P22 - Loggnings- och övervakningspolicy: Möjliggör spårbarhet av åtkomst till och användning av tillgångar genom systemloggning, synlighet i klienter och beteendeanalys.

10.1.6 P30 - Policy för incidenthantering: Stödjer snabb begränsning och utredning av tillgångsrelaterade överträdelser, såsom förlorade bärbara datorer eller lagringsmedier som inte kan spåras.

10.2 Dessa policyer utgör en sammanhållen styrningsstruktur som säkerställer att tillgångar hanteras säkert, inventeras korrekt och hanteras på lämpligt sätt under hela sin livscykel.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända standarder för informationssäkerhet och regulatoriska ramverk som kräver robust tillgångshantering under hela livscykeln.

11.2 ISO/IEC 27001:

11.2.1 Klausul 8.1 - Kräver att organisationer planerar, inför och styr de processer som behövs för att uppfylla informationssäkerhetskrav, inklusive krav för livscykelhantering av tillgångar.

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

11.3.1 Kontroll 5.9 - Förteckning över information och andra tillhörande tillgångar: Kräver en aktuell och fullständig förteckning över alla tillgångar som är relevanta för informationsbehandling.

11.3.2 Kontroll 5.10 - Godtagbar användning av information och tillgångar: Stöds av användningsregler, ägarskap och processer för återlämning.

11.3.3 Kontroll 5.11 - Återlämning av tillgångar: Genomförs genom formella överlämnings- och avvecklingsrutiner.

11.3.4 Dessa kontroller fastställer strukturerade krav för att identifiera, märka, upprätthålla och spåra organisationens tillgångar, med motsvarande ansvar för ägare och förvaltare under hela livscykeln.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Förteckning över systemkomponenter: Återspeglas genom centraliserad tillgångshantering, synlighet i realtid och koppling till operativa konfigurationer.

11.4.2 RA-3 - Riskbedömning: Tillgångsregister utgör grundläggande underlag för hotmodellering och riskbedömning.

11.4.3 MP-6 - Sanering av medier: Säkerställs genom metoder för säker bortskaffning som definieras i livscykelkontroller för tillgångar och policyn för databortskaffning.

11.5 EU:s GDPR (2016/679):

11.5.1 Artikel 30 - Register över behandlingsaktiviteter: Kräver att organisationer dokumenterar system, enheter och arkiv som lagrar eller behandlar personuppgifter.

11.5.2 Artikel 32 - Säkerhet i behandlingen: Är i linje med riskbedömning baserad på tillgångar och skyddsåtgärder anpassade till klassificerade tillgångar och kritisk infrastruktur.

11.6 EU:s NIS2-direktiv (2022/2555):

11.6.1 Artikel 21(2)(a, b): Kräver synlighet för tillgångar och tillgångsregister som grund för riskanalys, skydd och incidenthantering inom cybersäkerhet.

11.6.2 Artikel 21(3): Understryker behovet av strukturerad styrning av tillgångar som en del av organisationens informationssäkerhetskultur.

11.7 DORA-förordningen (2022/2554):

11.7.1 Artikel 5 - IKT-styrning och intern kontroll: Kräver att finansiella entiteter kontrollerar IKT-tillgångar med tydliga krav på registrering, ägarskap och skydd.

11.7.2 Artikel 9 - Ramverk för IKT-riskhantering: Fastställer att processer för tillgångshantering ska stödja riskreducering, kontinuitetsplanering och operativ motståndskraft.

11.8 COBIT 2019:

11.8.1 BAI09 - Hantera tillgångar: Är direkt anpassad till strukturerad identifiering, klassificering, användning och bortskaffning av organisationens tillgångar.

11.8.2 DSS01 - Hanterad drift: Stödjer införandet av kontroller som säkerställer skydd av tillgångar och kontinuerlig operativ styrning.

11.8.3 MEA03 - Övervaka, utvärdera och bedöma regelefterlevnad: Säkerställer regelbunden revision av kontroller för tillgångshantering och deras effektivitet i förhållande till regulatoriska krav.