					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P12S					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**

Juridiskt meddelande (upphovsrätt och användningsbegränsningar)

(C) 2025 Clarysec LLC. All rights reserved.

Detta dokument är Clarysec LLC:s immateriella egendom. Ingen del av detta dokument får kopieras, återanvändas, distribueras eller ändras för kommersiella eller implementeringsändamål utan uttryckligt skriftligt förhandstillstånd.
Obehörig användning är strängt förbjuden och kan leda till rättsliga åtgärder.
För licensiering, kontakta: info@clarysec.com

Anpassning till tillämpliga standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Krav avseende tillgångshantering
ISO/IEC 27002:2022	Kontroll 5	Kontroller för tillgångshantering
NIST SP 800-53 Rev.5	CM-8	Inventering av systemkomponenter
EU:s NIS2-direktiv	Artikel 21(2)(a)	Spårbarhet för tillgångar till skydd för nätverks- och informationssystem
EU:s DORA-förordning	Artikel 5(8)	Krav på inventering av IKT-tillgångar
COBIT 2019	BAI	Livscykelhantering av IT-tillgångar
EU:s GDPR	Artikel 30	Register över behandling av personuppgifter

1. Syfte

1.1 Denna policy fastställer hur organisationen identifierar, spårar, skyddar och avvecklar sina informationstillgångar, inklusive både fysiska och digitala komponenter.

1.2 Syftet är att minska operativa risker och säkerhetsrisker genom att upprätthålla spårbarhet, ansvar och säker hantering av samtliga verksamhetstillgångar under hela deras livscykel.

1.3 En tillförlitlig tillgångsförteckning stödjer regelefterlevnad, incidenthantering, kontinuitetsplanering och riskhantering.

1.4 Denna policy stödjer även certifiering enligt ISO/IEC 27001 och visar anpassning till rättsliga, finansiella och cybersäkerhetsrelaterade skyldigheter enligt ramverk som GDPR, NIS2 och DORA.

1.5 För små och medelstora företag (SME) är ett enkelt men systematiskt arbetssätt för tillgångshantering avgörande för att undvika tillgångar utan styrning, dataförlust eller brister vid revision, särskilt när den tekniska bemanningen är begränsad.

2. Omfattning

2.1 Denna policy gäller för samtliga tillgångar som ägs, leasas eller på annat sätt hanteras av organisationen, inklusive tillgångar som används i:

2.1.1 Kontorsarbete

2.1.2 Distansarbete eller hybridarbete

2.1.3 Fältverksamhet eller mobil verksamhet

2.1.4 Molnmiljöer och outsourcade miljöer

2.2 Tillgångstyper som omfattas inkluderar, men är inte begränsade till:

2.2.1 Hårdvara: bärbara datorer, stationära datorer, bildskärmar, telefoner, surfplattor, USB-enheter, routrar, skrivare, säkerhetskopieringsmedier

2.2.2 Programvara: installerade applikationer, SaaS-tjänster, operativsystem, antivirusverktyg, licenser

2.2.3 Datatillgångar: verksamhetsdatabaser, kalkylblad, kundregister, källkod

2.2.4 Digitala behörigheter och tjänster: domännamn, digitala certifikat, API-nycklar, e-postkonton, inloggningar till molntjänster

2.2.5 Åtkomstmedier: nycklar, smartkort, passertaggar, biometriska token

2.3 Samtliga anställda, konsulter och tredjepartsleverantörer som hanterar organisationens tillgångar omfattas av denna policy.

2.4 Policyn omfattar både kortfristiga tillgångar (t.ex. projektspecifika bärbara datorer) och långfristiga tillgångar samt delade tillgångar som används av flera personer.

3. Mål

3.1 Upprätta och upprätthålla en fullständig och korrekt förteckning över alla relevanta tillgångar, som uppdateras löpande.

3.2 Säkerställa att varje tillgång har en utsedd ägare som ansvarar för dess användning, förvaring och återlämning.

3.3 Klassificera tillgångar utifrån känslighet, verksamhetspåverkan eller regulatorisk relevans för att möjliggöra differentierade skyddsnivåer.

3.4 Fastställa tydliga rutiner för utlämning, omfördelning, underhåll, rapportering av förlust och avveckling av tillgångar.

3.5 Säkerställa att tillgångar hanteras säkert under hela sin livscykel och att den information de lagrar antingen skyddas eller raderas på ett säkert sätt vid avyttring.

3.6 Minska sannolikheten för säkerhetsincidenter som orsakas av ospårade, ej återlämnade eller felaktigt använda resurser som tillhör organisationen.

3.7 Stödja efterlevnad av tillämpliga lagkrav (t.ex. GDPR:s ansvarsskyldighet) och standarder för cybersäkerhetscertifiering.

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 Är policyägare för denna policy och ansvarar för att arbetssätt för tillgångshantering införs och efterlevs i hela organisationen.

4.1.2 Granskar och godkänner uppdateringar av tillgångsförteckningen samt godkänner avveckling eller överföring av tillgångar vid behov.

4.1.3 Ska informeras om varje betydande förlust, stöld eller otillåten användning av tillgångar.

4.2 IT-ansvarig eller utsedd tillgångsansvarig

4.2.1 Ansvarar för att underhålla tillgångsförteckningen (t.ex. i ett kalkylblad, ett ärendehanteringssystem eller ett enkelt verktyg för tillgångshantering).

4.2.2 Tilldelar ägarskap för tillgångar och följer förändringar i status (t.ex. ny, i bruk, under reparation, avvecklad).

4.2.3 Verifierar att samtliga utlämnade tillgångar är dokumenterade och kopplade till en person eller verksamhetsenhet.

4.2.4 Säkerställer att klassificeringsetiketter tillämpas och efterlevs (t.ex. Intern, Konfidentiell).

4.2.5 Samordnar återtagande, säker radering och avaktivering av tillgångar vid avslut av anställning eller uppdrag samt vid avveckling.

4.2.6 Rapporterar varje olöst avvikelse i tillgångshanteringen till VD.

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

9. Krav på granskning och uppdatering

9.1 Denna policy ska granskas minst en gång per år samt när:

9.1.1 Nya typer av teknik eller tillgångar införs

9.1.2 Rutiner för spårning av tillgångar förändras (t.ex. införande av nya verktyg eller plattformar)

9.1.3 Nya regulatoriska skyldigheter påverkar spårbarhet eller avveckling av tillgångar

9.1.4 En incident eller revision identifierar en brist i nuvarande arbetssätt för tillgångshantering

9.2 Granskningar ska omfatta VD och IT-ansvarig samt inkludera uppdateringar av rutiner för tillgångshantering, mallar för tillgångsförteckning och vägledning för klassificering.

9.3 Samtliga uppdateringar ska dokumenteras och kommuniceras till berörd personal. En versionshanterad ändringslogg ska bevaras.

10. Relaterade policyer och kopplingar

10.1 P2S – Policy för styrningsroller och ansvar: Fastställer ansvar för policyägarskap och IT-drift.

10.2 P4S – Policy för åtkomstkontroll: Kopplar användning av tillgångar (t.ex. bärbara datorer och mobila enheter) till användares åtkomsträttigheter och identitetshantering.

10.3 P7S – Policy för onboarding och avslut: Säkerställer att utlämning och återtagande av tillgångar ingår i processer för medarbetarlivscykeln.

10.4 P13S – Policy för dataklassificering och märkning: Anger regler för att avgöra om en tillgång ska klassificeras som Intern eller Konfidentiell.

10.5 P30S – Policy för incidenthantering: Vägleder hanteringen om en händelse kopplad till en tillgång leder till en säkerhetsincident eller personuppgiftsincident.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1: Kräver operativa kontroller för att hantera tillgångar och skydda dem under hela användningstiden.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.9: Beskriver hur tillgångar ska identifieras, tilldelas ägare, klassificeras och hanteras säkert.

11.3 NIST SP 800-53 Rev

11.3.1 CM-8: Kräver att organisationer upprättar och underhåller en förteckning över systemkomponenter, inklusive hårdvara, programvara och virtuella tillgångar.

11.4 EU:s GDPR

11.4.1 Artikel 30: Kräver dokumentation av personuppgiftsbehandlingar, vilket förutsätter kännedom om var uppgifter lagras och på vilka tillgångar.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(a): Kräver tekniska och organisatoriska åtgärder, inklusive spårning av tillgångar, för att skydda nätverks- och informationssystem.

11.6 EU:s DORA-förordning

11.6.1 Artikel 5(8): Finansiella entiteter ska upprätthålla detaljerade förteckningar över IKT-tillgångar som en del av hanteringen av IKT-risker.

11.7 COBIT 2019

11.7.1 BAI09: Anger att IT-tillgångar ska hanteras under hela sin livscykel – från anskaffning till avveckling – med tydligt ägarskap och lämpliga kontroller.