					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P14					Dokumenttitel: **Policy för datalagring och säker bortskaffning**							
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**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontroller 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
EU:s GDPR	Artiklar 5(1)(e), 17, 32	
EU:s NIS2-direktiv	Artikel 21(2)(a-e)	
EU:s DORA-förordning	Artiklar 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Syfte

1.1 Syftet med denna policy är att fastställa organisationens krav för datalagring och säker bortskaffning genom informationslivscykelns samtliga faser. Den säkerställer efterlevnad av tillämpliga rättsliga, regulatoriska och avtalsmässiga skyldigheter samt förhindrar onödig eller riskfylld ansamling av data.

1.2 Denna policy stödjer införandet av ISO/IEC 27001:2022 genom att upprätthålla kontroll över lagringstider för data och irreversibla rutiner för bortskaffning. Den möjliggör spårbar dokumentation av poster, säkerställer att lagring sker i enlighet med informationens klassificeringsnivå och upprätthåller beredskap för revision, regulatorisk tillsyn och rättslig bevisinhämtning.

1.3 Policyn syftar vidare till att upprätthålla konfidentialitet, riktighet och tillgänglighet för data, samtidigt som verksamhetsrisker, operativa ineffektiviteter och exponering för integritetsincidenter till följd av felaktig datalagring eller förstöring minimeras.

2. Omfattning

2.1 Denna policy gäller för alla fysiska och digitala informationstillgångar som ägs, behandlas eller lagras av organisationen, inklusive sådana som står under kontroll av tredje part, dotterbolag eller outsourcingpartner.

2.2 Omfattningen inkluderar, men är inte begränsad till:

2.2.1 Dokument, filer och poster (digitala och pappersbaserade)

2.2.2 Databaser och arkiv

2.2.3 E-post och loggar från snabbmeddelanden

2.2.4 Säkerhetskopior, systemloggar och revisionsspår

2.2.5 Källkod, applikationsdata och tillgångar i molnmiljö

2.2.6 Flyttbara lagringsmedier och utrangerad hårdvara som innehåller data

2.3 Policyn reglerar både operativ information och reglerade datamängder (t.ex. finansiellt, juridiskt, HR-, kundrelaterat och revisionsrelevant innehåll), oavsett lagringsplats eller system.

2.4 Den gäller för samtliga avdelningar inom organisationen samt för anställda, entreprenörer och leverantörer som deltar i skapande, lagring, hantering eller bortskaffning av data.

3. Mål

3.1 Säkerställa att data endast lagras så länge som det är rättsligt, avtalsmässigt eller operativt nödvändigt, och att data bortskaffas säkert när den inte längre behövs.

3.2 Förhindra förtida, otillåten eller oavsiktlig radering av poster som behövs för pågående verksamhet, regelefterlevnad, rättsprocesser eller revisionsändamål.

3.3 Etablera och tillämpa konsekventa lagringsscheman baserade på informationsklassificering, tillgångstyp, tillämpliga lagkrav och riskexponering.

3.4 Skydda dataskydd och sekretess under lagringsperioden och vid tidpunkten för bortskaffning, inklusive uppfyllande av registrerades rättigheter (t.ex. radering enligt artikel 17 i EU:s GDPR).

3.5 Säkerställa att alla metoder för bortskaffning av data är irreversibla, ändamålsenligt dokumenterade och förenliga med erkända standarder såsom NIST SP 800-88.

3.6 Minimera operativa ineffektiviteter, kostnadspåslag och rättslig exponering som orsakas av överdriven lagring eller ospårade äldre data.

3.7 Stödja mål för verksamhetskontinuitet och katastrofåterställning genom integrerad styrning av lagring för säkerhetskopior och försvarbara metoder för dataarkivering.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner denna policy och säkerställer lämplig finansiering, resurstilldelning och integration i organisationens riskhanterings- och regelefterlevnadsprogram.

4.1.2 Har det övergripande ansvaret för efterlevnad av rättsliga och regulatoriska krav avseende datalagring och säker bortskaffning.

4.2 Informationssäkerhetschef (CISO)

4.2.1 Är policyägare för denna policy och ansvarar för att definiera och följa upp styrningen av lagring och bortskaffning i linje med ISMS.

4.2.2 Säkerställer att klassificeringsstyrda krav på lagring och bortskaffning införs inom verksamhetsenheter och tekniska system.

4.2.3 Följer upp efterlevnaden av policyn och initierar korrigerande åtgärder vid behov.

[... 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 årligen eller när något av följande villkor är uppfyllt:

9.1.1 Förändringar i tillämpliga lagar eller regelverk som påverkar datalagring (t.ex. uppdateringar av GDPR, skattelagstiftning eller DORA-förordningen)

9.1.2 Revideringar av klassificeringsramverket eller verksamhetsprocesser som påverkar steg i informationslivscykeln

9.1.3 Införande av nya IT-system, arkivplattformar eller tekniker för bortskaffning av medier

9.1.4 Revisionsiakttagelser från internrevision eller regulatoriska rekommendationer som påvisar brister i rutiner för lagring eller bortskaffning

9.2 Granskningen ska ledas av CISO och dataskyddsombudet (DPO), med bidrag från juridisk funktion, regelefterlevnad, IT och verksamhetsenheter.

9.3 Det övergripande lagringsschemat för data (MDRS) och registret för bortskaffning ska granskas parallellt för att säkerställa att:

9.3.1 Scheman förblir korrekta och återspeglar operativa, rättsliga och regulatoriska behov

9.3.2 Dokumentation för bortskaffning är fullständig och granskningsbar

9.3.3 Poster om rättsligt bevarande valideras och avslutas när det är lämpligt

9.4 Eventuella uppdateringar av policyn ska:

9.4.1 Versionshanteras formellt och bevaras i ISMS dokumentregister

9.4.2 Innehålla revisionshistorik och motivering till ändringen

9.4.3 Godkännas av verkställande ledning

9.4.4 Kommuniceras till berörd personal tillsammans med uppdaterat utbildnings- eller vägledningsmaterial

9.5 Vid betydande policyändringar ska berörda anställda genomföra riktad repetitionsutbildning inom 30 dagar från publicering för att säkerställa fortsatt efterlevnad.

9.6 Relaterade policyer och kopplingar

10. Relaterade policyer och kopplingar

10.1.1 P4 - Policy för åtkomstkontroll: Säkerställer att endast behöriga personer får åtkomst till data under lagringsperioden och att data vars lagringstid har löpt ut begränsas i avvaktan på bortskaffning.

10.1.2 P12 - Policy för tillgångshantering: Identifierar vilka tillgångar som innehåller data som kräver schemalagd bortskaffning och följer deras livscykel från anskaffning till förstöring.

10.1.3 P13 - Policy för dataklassificering och märkning: Vägleder klassificeringsbeslut som direkt påverkar hur länge data lagras och vilken metod för bortskaffning som krävs.

10.1.4 P15 - Policy för säkerhetskopiering och återställning: Definierar lagringsperioder och rutiner för bortskaffning av säkerhetskopieringsmedier och replikerade datatillgångar.

10.1.5 P18 - Policy för kryptografiska kontroller: Stödjer kryptografisk radering vid bortskaffning och säkerställer kryptering under datalagring fram till förstöring.

10.1.6 P30 - Policy för incidenthantering (P30): Aktiveras när felaktig bortskaffning leder till potentiell dataförlust, överträdelse eller regulatorisk avvikelse.

10.2 Varje länkad policy bidrar till att upprätthålla en sammanhållen styrningsmodell för data avseende klassificering, livscykelstyrning, åtkomst och revisionsberedskap.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till globalt erkända standarder och regulatoriska ramverk som definierar säkra, regelefterlevnadsanpassade och effektiva arbetssätt för informationslivscykeln.

11.2 ISO/IEC 27001:

11.2.1 Klausul 6.1.3 - riskbehandlingsplan: Stödjer begränsning av risker kopplade till överdriven lagring, dataintrång eller fel i bortskaffningsprocessen.

11.2.2 Klausul 8.1 - operativ planering och styrning: Etablerar livscykelkontroller som reglerar lagring, arkivering och förstöring.

11.3 ISO/IEC 27002:2022 - Kontroller 5.10, 5.12, 5.30, 5: Ger praktisk vägledning om godtagbar användning av data, motivering för lagring, kontrollerad radering och försvarbar dokumenthantering i linje med organisationens riskaptit och risktolerans.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Bevarande av revisionsunderlag: Säkerställer tillräcklig lagring av revisionsloggar och underlag för regelefterlevnad.

11.4.2 MP-6 - Mediesanering: Kräver säkra och dokumenterade metoder för förstöring av fysiska och elektroniska medier.

11.4.3 SI-12 - Informationshantering: Säkerställer att data hanteras på ett lämpligt sätt i linje med kontroller för lagring och bortskaffning.

11.4.4 PL-2 - Systemsäkerhets- och integritetsplan: Kräver systemspecifik dokumentation av hantering genom informationslivscykeln och bestämmelser om säker bortskaffning.

11.5 EU:s GDPR (2016/679):

11.5.1 Artikel 5(1)(e) - uppgiftsminimering och lagringsbegränsning: Kräver att data inte lagras längre än nödvändigt.

11.5.2 Artikel 17 - rätt till radering ("rätten att bli bortglömd"): Kräver skyndsam och permanent radering av personuppgifter efter giltig begäran.

11.5.3 Artikel 32 - säkerhet i behandlingen: Förstärker dataskydd under lagringsperioden och kräver säker förstöring av poster vars lagringstid har löpt ut.

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

11.6.1 Artikel 21(2)(a-e): Kräver att entiteter inför policyer och tekniska åtgärder för säker datahantering, inklusive begränsning av lagringstid och metoder för bortskaffning.

11.7 EU:s DORA-förordning (2022/2554):

11.7.1 Artikel 5 - styrning och kontroll: Kräver strukturerad IKT-riskhantering, inklusive säker hantering av informationslivscykeln.

11.7.2 Artikel 9 - ramverk för IKT-riskhantering: Kräver policyer för datalagring, förstöring och efterlevnad av rättsliga och regulatoriska krav för digital verksamhet.

11.8 COBIT 2019:

11.8.1 DSS01 - Hanterad drift: Stödjer spårning av lagring och konsekvens mellan datasystem.

11.8.2 DSS05 - Hanterade säkerhetstjänster: Säkerställer skydd av lagrade och arkiverade data fram till säker bortskaffning.

11.8.3 MEA03 - Övervaka, utvärdera och bedöma regelefterlevnad: Möjliggör revision av tillämpning av lagringskrav, raderingsrutiner och uppfyllande av regulatoriska krav.