					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P14S					Dokumenttitel: **policy för dokumentbevarande och bortskaffande**							
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**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1.3, 8	Omfattar riskbehandling, operativa kontroller och krav på bevarande
ISO/IEC 27002:2022	Kontroll 5	Ger vägledning om bevarandeperioder och säkra metoder för förstöring
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Bevarande av revisionsunderlag, sanering av lagringsmedier, gränser för databevarande och tillämpning
EU:s NIS2-direktiv	Artikel 21(2)(a)	Kräver en policy för riskanpassad livscykelhantering
EU:s DORA-förordning	Artikel 5(1)	IKT-riskhantering: datatillgänglighet och borttagning
COBIT 2019	BAI03.04, DSS01	Kontroller för informationslivscykeln och säkert bortskaffande
EU:s GDPR	Artikel 5(1)(e), 17	Uppgifter får inte bevaras längre än nödvändigt; rätt till radering

1. Syfte

1.1 Syftet med denna policy är att fastställa bindande regler för bevarande och säkert bortskaffande av information i en SME-miljö. Policyn säkerställer att uppgifter endast bevaras så länge som krävs enligt lag, avtalskrav eller verksamhetsmässiga behov och därefter förstörs på ett säkert sätt.

1.2 Denna policy syftar till att minska informationsrisker, hantera rättslig exponering och begränsa lagring av redundanta eller inaktuella data. Den bidrar till efterlevnad av ISO/IEC 27001 och dataskyddsramverk såsom EU:s GDPR genom att minimera otillåtet bevarande av personuppgifter eller känslig information.

1.3 Ett välstrukturerat ramverk för bevarande och bortskaffande minskar driftskostnader, förbättrar systemprestanda och stärker revisionsberedskapen. För SME-verksamheter med begränsad IT-kapacitet ger det ett praktiskt sätt att hantera digitala och fysiska informationstillgångar på ett ansvarsfullt sätt.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla uppgifter, filer, loggar, kommunikationer och datamängder som skapas, samlas in, behandlas eller lagras av organisationen

2.1.2 Alla anställda, entreprenörer och tredjepartsleverantörer som hanterar organisationens data

2.1.3 Alla dataformat (t.ex. papper, elektroniskt, bild, ljud eller logg) och alla lagringsmedier (t.ex. lokala enheter, molntjänster, e-postservrar, säkerhetskopior)

2.2 Omfattningen inkluderar:

2.2.1 Verksamhetsdokumentation (t.ex. fakturor, avtal, projektrapporter)

2.2.2 Operativa underlag (t.ex. loggar, åtkomsthistorik, ögonblicksbilder av säkerhetskopior)

2.2.3 Personuppgifter (t.ex. HR-filer, klientkommunikation, supportuppgifter)

2.2.4 Data som driftas internt, externt eller i hybrida system

2.2.5 Arkiverade data och säkerhetskopior, oavsett om de är aktiva eller inaktiva

2.3 Alla steg i datans livscykel omfattas, från skapande till godkänt bortskaffande.

3. Mål

3.1 Fastställa enhetliga regler för bevarande baserat på rättsliga, operativa och regulatoriska kriterier.

3.2 Förhindra förtida radering av kritiska uppgifter och eliminera onödig ackumulering av data.

3.3 Säkerställa säkert och oåterkalleligt bortskaffande av data när bevarande inte längre krävs.

3.4 Tilldela ansvar för tillämpning av beslut om bevarande och radering inom ramen för SME-verksamhetens personella begränsningar.

3.5 Tillhandahålla dokumentation som säkerställer revisionsberedskap och visar vederbörlig omsorg enligt ISO 27001, EU:s GDPR, EU:s NIS2-direktiv och andra ramverk.

3.6 Främja säker hantering av data genom hela livscykeln utan att lägga en onödig teknisk börda på personal utan specialistkompetens.

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 Godkänner denna policy och är dess ägare.

4.1.2 Säkerställer att rutiner för bevarande och bortskaffande genomförs på ett sätt som är förenligt med rättsliga krav och verksamhetsrisker.

4.1.3 Godkänner undantag och juridiskt bevarande vid behov.

4.1.4 Initierar policygranskningar och godkänner uppdateringar utifrån förändringar i verksamheten eller regelverken.

4.2 Utsedd dataägare

4.2.1 Utses per datakategori (t.ex. finansiella uppgifter, HR, klientregister).

4.2.2 Klassificerar uppgifter och fastställer lämplig bevarandeperiod utifrån denna policy och juridisk vägledning.

4.2.3 Godkänner radering när kraven på bevarande har uppfyllts.

4.2.4 Stöder internrevisioner genom att tillhandahålla kontext kring bevarandelogik och bortskaffandehändelser.

[... 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 eller vid:

9.1.1 Förändringar i tillämpliga lagkrav (t.ex. dataskydd, finansiell rapportering)

9.1.2 Införande av nya system eller processer som påverkar datans livscykel

9.1.3 Revisionsiakttagelser eller incidenter som visar på brister i rutiner för bevarande

9.2 Granskningar ska säkerställa att bevaranderegistret förblir fullständigt och omfattar alla större uppgiftskategorier.

9.3 Uppdateringar av policyn ska godkännas av VD och kommuniceras till berörd personal. Den senaste versionen ska vara tillgänglig och versionshanterad.

10. Relaterade policyer och kopplingar

10.1 P2S – Policy för styrningsroller och ansvar: Definierar policyägarskap och befogenhet att godkänna undantag.

10.2 P13S – Policy för dataklassificering och märkning: Fastställer hur regler för bevarande anpassas till dataklassificering.

10.3 P12S – Policy för tillgångshantering: Styr lagringsmedier som innehåller data som omfattas av bevarande och bortskaffande.

10.4 P17S – Policy för dataskydd och integritet: Säkerställer uppgiftsminimering och stödjer laglig behandling enligt EU:s GDPR.

10.5 P30S – Policy för incidenthantering: Aktiveras när brister i bortskaffande eller bevarande leder till potentiell dataexponering.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1.3: Kräver behandling av informationsrelaterade risker, inklusive risker kopplade till bevarande.

11.1.2 Klausul 8.1: Definierar operativa kontroller för livscykelhantering.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.33: Ger vägledning om fastställande av bevarandeperioder och säkra metoder för förstöring.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Kräver bevarande av revisionsunderlag.

11.3.2 MP-6: Definierar rutiner för sanering av lagringsmedier.

11.3.3 SI-12: Behandlar gränser för databevarande och tillämpning.

11.4 EU:s GDPR

11.4.1 Artikel 5(1)(e): Uppgifter får inte bevaras längre än nödvändigt.

11.4.2 Artikel 17: Rätt till radering gäller när uppgifter inte längre bevaras på laglig grund.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(a): Kräver riskanpassade organisatoriska policyer, inklusive livscykelhantering.

11.6 EU:s DORA-förordning

11.6.1 Artikel 5(1): IKT-riskhantering omfattar datatillgänglighet och borttagning.

11.7 COBIT 2019

11.7.1 BAI03.04: Kräver kontroller för informationslivscykeln.

11.7.2 DSS01.06: Rutiner för säkert bortskaffande som en del av skyddet av informationstillgångar.