					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P14S					Dokumenttitel: **Politik for opbevaring og sikker bortskaffelse af data**							
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**

Afstemt med standarder og regler, hvor relevant

Standard/regulering	Punkt/artikel	Kommentar
ISO/IEC 27001:2022	Punkt 6.1.3, 8	Omfatter risikobehandling, operationelle kontroller og krav til opbevaring
ISO/IEC 27002:2022	Kontrol 5	Vejledning om opbevaringsperioder og metoder til sikker destruktion
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12	Opbevaring af revisionsspor, sanering af medier, grænser for dataopbevaring og håndhævelse
EU NIS2	Artikel 21(2)(a)	Kræver en politik for livscyklusstyring tilpasset risiko
EU DORA	Artikel 5(1)	IKT-risikostyring: datatilgængelighed og fjernelse
COBIT 2019	BAI03.04, DSS01	Kontroller for informationslivscyklus og sikker bortskaffelse
GDPR	Artikel 5(1)(e), 17	Data må ikke opbevares længere end nødvendigt; ret til sletning

1. Formål

1.1 Formålet med denne politik er at fastsætte bindende regler for opbevaring og sikker bortskaffelse af information i et SMV-miljø. Den sikrer, at registreringer kun opbevares i den periode, der kræves efter lovgivning, kontraktlige forpligtelser eller forretningsmæssig nødvendighed, og derefter destrueres sikkert.

1.2 Denne politik skal reducere informationsrisici, håndtere juridisk eksponering og begrænse opbevaring af overflødige eller forældede data. Den understøtter efterlevelse af ISO/IEC 27001 og databeskyttelsesrammer som GDPR ved at minimere uautoriseret opbevaring af personoplysninger eller følsomme oplysninger.

1.3 En velstruktureret ramme for opbevaring og bortskaffelse reducerer driftsomkostninger, forbedrer systemydelsen og styrker revisionsberedskabet. For SMV'er med begrænset IT-kapacitet giver den en praktisk metode til ansvarlig håndtering af digitale og fysiske informationsaktiver.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle registreringer, filer, logfiler, kommunikation og datasæt, som organisationen opretter, indsamler, behandler eller opbevarer

2.1.2 Alle medarbejdere, konsulenter og eksterne leverandører, der håndterer organisationens data

2.1.3 Alle dataformater (f.eks. papir, elektronisk, billede, lyd eller log) og alle lagringsmedier (f.eks. lokale drev, cloudtjenester, mailservere og sikkerhedskopier)

2.2 Omfanget omfatter:

2.2.1 Forretningsdokumenter (f.eks. fakturaer, kontrakter og projektrapporter)

2.2.2 Driftsdata (f.eks. logfiler, adgangshistorik og snapshots af sikkerhedskopier)

2.2.3 Personoplysninger (f.eks. HR-filer, kundekommunikation og supportregistreringer)

2.2.4 Data, der hostes internt, eksternt eller i hybride miljøer

2.2.5 Arkiverede data og sikkerhedskopier, uanset om de er aktive eller inaktive

2.3 Alle faser i dataenes livscyklus er omfattet – fra oprettelse til godkendt bortskaffelse.

3. Mål

3.1 Fastlægge ensartede regler for opbevaring baseret på juridiske, operationelle og regulatoriske kriterier.

3.2 Forebygge for tidlig sletning af kritiske registreringer og eliminere unødvendig ophobning af data.

3.3 Sikre sikker og irreversibel bortskaffelse af data, når opbevaring ikke længere er påkrævet.

3.4 Fastlægge ejerskab for håndhævelse af beslutninger om opbevaring og sletning inden for SMV'ens bemandingsmæssige rammer.

3.5 Tilvejebringe revisionsklar dokumentation, der dokumenterer rettidig omhu efter ISO 27001, GDPR, NIS2 og andre relevante rammer.

3.6 Fremme sikker håndtering af data gennem hele livscyklussen uden at pålægge medarbejdere uden specialistkompetencer unødig teknisk byrde.

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender og ejer denne politik.

4.1.2 Sikrer, at procedurer for opbevaring og bortskaffelse implementeres i overensstemmelse med juridisk risiko og forretningsrisiko.

4.1.3 Godkender undtagelser og retlige tilbageholdelser, når det er nødvendigt.

4.1.4 Iværksætter gennemgang af politikken og godkender opdateringer på baggrund af forretningsmæssige eller regulatoriske ændringer.

4.2 Udpeget dataejer

4.2.1 Udpeges for hver datakategori (f.eks. finans, HR og kunderegistreringer).

4.2.2 Klassificerer registreringer og fastsætter passende opbevaringsperioder på baggrund af politikken og juridisk vejledning.

4.2.3 Godkender sletning, når opbevaringskravene er opfyldt.

4.2.4 Understøtter interne revisioner ved at give kontekst om opbevaringslogik og bortskaffelseshændelser.

[... 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 om året eller ved:

9.1.1 Ændringer i gældende lovgivning (f.eks. databeskyttelse og finansiel rapportering)

9.1.2 Indførelse af nye systemer eller processer, der påvirker dataenes livscyklus

9.1.3 Revisionsresultater eller hændelser, der afdækker mangler i praksis for opbevaring

9.2 Gennemgange skal sikre, at opbevaringsregisteret fortsat er fuldstændigt og afspejler alle væsentlige registreringskategorier.

9.3 Opdateringer af politikken skal godkendes af direktøren og kommunikeres til berørte medarbejdere. Den seneste version skal være tilgængelig og versionsstyret.

10. Relaterede politikker og sammenhænge

10.1 P2S – Politik for styringsroller og ansvar: Definerer ejerskab til politikken og bemyndigelse til undtagelser.

10.2 P13S – Politik for dataklassifikation og mærkning: Fastlægger, hvordan regler for opbevaring afstemmes med dataklassifikation.

10.3 P12S – Politik for aktivstyring: Regulerer lagringsmedier, som indeholder data omfattet af opbevaring og bortskaffelse.

10.4 P17S – Politik for databeskyttelse og privatliv: Sikrer dataminimering og understøtter lovlig behandling efter GDPR.

10.5 P30S – Politik for hændelseshåndtering: Aktiveres, når fejl i bortskaffelse eller opbevaring medfører potentiel eksponering af data.

11. Referencestandarder og rammer

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1.3: Kræver behandling af informationsrelaterede risici, herunder risici ved opbevaring.

11.1.2 Punkt 8.1: Definerer operationelle kontroller for livscyklussen.

11.2 ISO/IEC 27002

11.2.1 Kontrol 5.33: Vejledning om fastsættelse af opbevaringsperioder og metoder til sikker destruktion.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Krav om opbevaring af revisionsspor.

11.3.2 MP-6: Definerer procedurer for sanering af medier.

11.3.3 SI-12: Omhandler grænser for dataopbevaring og håndhævelse.

11.4 GDPR

11.4.1 Artikel 5(1)(e): Data må ikke opbevares længere end nødvendigt.

11.4.2 Artikel 17: Ret til sletning gælder, når data ikke længere opbevares lovligt.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): Kræver risikotilpassede organisatoriske politikker, herunder livscyklusstyring.

11.6 EU DORA

11.6.1 Artikel 5(1): IKT-risikostyring omfatter datatilgængelighed og fjernelse.

11.7 COBIT 2019

11.7.1 BAI03.04: Krav om kontroller for informationslivscyklus.

11.7.2 DSS01.06: Procedurer for sikker bortskaffelse som led i beskyttelsen af informationsaktiver.