					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P14					Dokumenttitel: **Politik for dataopbevaring og bortskaffelse**							
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**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 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 GDPR	Artikel 5(1)(e), 17, 32	
EU NIS2	Artikel 21(2)(a-e)	
EU DORA	Artikel 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Formål

1.1 Formålet med denne politik er at fastlægge organisationens krav til dataopbevaring og sikker bortskaffelse på tværs af alle faser i informationens livscyklus. Politikken skal sikre overholdelse af gældende juridiske, regulatoriske og kontraktlige forpligtelser samt forebygge unødvendig eller risikofyldt ophobning af data.

1.2 Denne politik understøtter implementeringen af ISO/IEC 27001:2022 ved at håndhæve styring af dataopbevaringsperioder og irreversible bortskaffelsesmetoder. Den muliggør sporbar dokumentation af registreringer, håndhæver opbevaring i overensstemmelse med klassificeringens følsomhed og sikrer revisionsberedskab i forbindelse med revision, regulatorisk inspektion og juridisk bevisførelse.

1.3 Politikken har desuden til formål at opretholde dataenes fortrolighed, integritet og tilgængelighed, samtidig med at forretningsrisiko, driftsmæssige ineffektiviteter og eksponering for brud på databeskyttelsen som følge af ukorrekt dataopbevaring eller destruktion minimeres.

2. Omfang

2.1 Denne politik gælder for alle fysiske og digitale informationsaktiver, som ejes, behandles eller opbevares af organisationen, herunder aktiver under kontrol af tredjeparter, datterselskaber eller outsourcingpartnere.

2.2 Omfanget omfatter blandt andet:

2.2.1 Dokumenter, filer og registreringer (digitale og papirbaserede)

2.2.2 Databaser og arkiver

2.2.3 E-mails og logfiler fra instant messaging

2.2.4 Sikkerhedskopier, systemlogfiler og revisionsspor

2.2.5 Kildekode, applikationsdata og cloud-hostede aktiver

2.2.6 Flytbare medier og udfaset hardware, der indeholder data

2.3 Politikken omfatter både driftsregistreringer og regulerede datasæt (f.eks. finansielt, juridisk, HR-, kunderelateret og revisionsrelevant indhold), uanset lagringsplacering eller system.

2.4 Den gælder for alle organisatoriske enheder samt alle medarbejdere, kontrahenter og leverandører, der er involveret i oprettelse, lagring, styring eller bortskaffelse af data.

3. Mål

3.1 At sikre, at data kun opbevares så længe, det er juridisk, kontraktligt eller driftsmæssigt nødvendigt, og bortskaffes sikkert, når de ikke længere er påkrævet.

3.2 At forhindre for tidlig, uautoriseret eller utilsigtet sletning af registreringer, der er nødvendige for løbende drift, efterlevelse, retssager eller revisionsformål.

3.3 At etablere og håndhæve ensartede opbevaringsplaner baseret på informationsklassificering, aktivtype, gældende lovgivning og risikoeksponering.

3.4 At beskytte databeskyttelse og fortrolighed i opbevaringsperioden og ved bortskaffelse, herunder opfyldelse af registreredes rettigheder (f.eks. sletning efter GDPR artikel 17).

3.5 At sikre, at alle metoder til databortskaffelse er irreversible, tilstrækkeligt dokumenterede og i overensstemmelse med anerkendte standarder såsom NIST SP 800-88.

3.6 At minimere driftsmæssige ineffektiviteter, omkostningsoverhead og juridisk eksponering forårsaget af overdreven opbevaring eller ikke-sporede legacy-data.

3.7 At understøtte målsætninger for forretningskontinuitet og katastrofeberedskab gennem integreret styring af opbevaring af sikkerhedskopier og juridisk forsvarlig dataarkivering.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender denne politik og sikrer tilstrækkelig finansiering, ressourceallokering og integration i programmer for enterprise risk management og compliance.

4.1.2 Har det overordnede ansvar for overholdelse af juridiske og regulatoriske krav vedrørende dataopbevaring og sikker bortskaffelse.

4.2 Chief Information Security Officer (CISO)

4.2.1 Ejer denne politik og er ansvarlig for at definere og gennemgå styringen af opbevaring og bortskaffelse i overensstemmelse med ISMS.

4.2.2 Sikrer, at klassifikationsdrevne krav til opbevaring og bortskaffelse implementeres i forretningsenheder og tekniske systemer.

4.2.3 Overvåger efterlevelse af politikken og iværksætter korrigerende handlinger, hvor det er nødvendigt.

[... 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 årligt, eller når en af følgende betingelser er opfyldt:

9.1.1 Ændringer i gældende lovgivning eller regulering, der påvirker dataopbevaring (f.eks. opdateringer til GDPR, skattelovgivning, DORA)

9.1.2 Revisioner af klassificeringsrammen eller forretningsprocesser, der påvirker dataenes livscyklusfaser

9.1.3 Indførelse af nye IT-systemer, arkiveringsplatforme eller teknologier til mediedestruktion

9.1.4 Revisionskonstateringer fra intern revision eller regulatoriske anbefalinger, der peger på mangler i praksis for opbevaring eller bortskaffelse

9.2 Gennemgangen skal ledes af CISO og Data Protection Officer (DPO) med input fra Jura, compliance, IT og forretningsenheder.

9.3 Hovedplanen for dataopbevaring (MDRS) og registeret for bortskaffelse skal gennemgås parallelt for at sikre:

9.3.1 At planerne forbliver korrekte og afspejler driftsmæssige, juridiske og regulatoriske behov

9.3.2 At dokumentation for bortskaffelse er fuldstændig og revisionsklar

9.3.3 At registreringer af juridisk opbevaringspligt valideres og ophæves, når det er relevant

9.4 Enhver opdatering af politikken skal:

9.4.1 Versionsstyres formelt og opbevares i ISMS-dokumentrepositoryet

9.4.2 Omfatte versionshistorik og begrundelse for ændringer

9.4.3 Godkendes af direktionen

9.4.4 Kommunikeres til relevant personale sammen med opdateret træning eller vejledningsmateriale

9.5 Ved væsentlige ændringer i politikken skal berørte medarbejdere gennemføre målrettet genoptræning inden for 30 dage efter offentliggørelse for at sikre fortsat efterlevelse.

9.6 Relaterede politikker og sammenhænge

10. Relaterede politikker og sammenhænge

10.1.1 P4 - Politik for adgangskontrol: Sikrer, at kun autoriserede personer har adgang til data i opbevaringsperioden, og at udløbne data begrænses i afventning af bortskaffelse.

10.1.2 P12 - Politik for aktivstyring: Identificerer hvilke aktiver der indeholder data, som kræver planlagt bortskaffelse, og sporer deres livscyklus fra anskaffelse til destruktion.

10.1.3 P13 - Politik for dataklassificering og mærkning: Styrer klassificeringsbeslutninger, som direkte påvirker, hvor længe data opbevares, og hvilken bortskaffelsesmetode der kræves.

10.1.4 P15 - Politik for sikkerhedskopiering og gendannelse: Definerer opbevaringsperioder og procedurer for bortskaffelse af backupmedier og replikerede dataaktiver.

10.1.5 P18 - Politik for kryptografiske kontroller: Understøtter kryptografisk sletning ved bortskaffelse og håndhæver kryptering under dataopbevaring frem til destruktion.

10.1.6 P30 - Politik for hændelseshåndtering: Aktiveres i tilfælde, hvor ukorrekt bortskaffelse medfører potentielt datatab, brud eller regulatorisk overtrædelse.

10.2 Hver tilknyttet politik spiller en rolle i håndhævelsen af en sammenhængende model for datastyring på tværs af klassificering, livscyklusstyring, adgang og revisionsberedskab.

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset globalt anerkendte standarder og regulatoriske rammeværker, der fastlægger sikker, compliant og effektiv praksis for dataenes livscyklus.

11.2 ISO/IEC 27001:

11.2.1 Klausul 6.1.3 - Risikobehandlingsplan: Understøtter begrænsning af risici forbundet med overdreven opbevaring, brud på persondatasikkerheden eller fejl i bortskaffelse.

11.2.2 Klausul 8.1 - Operationel planlægning og styring: Etablerer livscykluskontroller, der regulerer lagring, arkivering og destruktion.

11.3 ISO/IEC 27002:2022 - Kontroller 5.10, 5.12, 5.30, 5: Giver praktisk vejledning om acceptabel brug af data, begrundelse for opbevaring, kontrolleret sletning og juridisk forsvarlig registreringspraksis i overensstemmelse med organisationens risikotolerance.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Opbevaring af revisionsregistreringer: Sikrer tilstrækkelig opbevaring af revisionslogfiler og bevis for overholdelse.

11.4.2 MP-6 - Sanering af medier: Kræver sikre og dokumenterede destruktionsmetoder for fysiske og elektroniske medier.

11.4.3 SI-12 - Informationshåndtering: Håndhæver passende databehandling i overensstemmelse med kontroller for opbevaring og bortskaffelse.

11.4.4 PL-2 - Systemplan for sikkerhed og databeskyttelse: Kræver systemspecifik dokumentation af håndtering af dataenes livscyklus og bestemmelser om sikker bortskaffelse.

11.5 EU GDPR (2016/679):

11.5.1 Artikel 5(1)(e) - Dataminimering og opbevaringsbegrænsning: Kræver, at data ikke opbevares længere end nødvendigt.

11.5.2 Artikel 17 - Ret til sletning ("retten til at blive glemt"): Kræver hurtig og permanent sletning af personoplysninger efter gyldig anmodning.

11.5.3 Artikel 32 - Behandlingssikkerhed: Styrker databeskyttelsen under opbevaring og kræver sikker destruktion af udløbne registreringer.

11.6 EU NIS2-direktivet (2022/2555):

11.6.1 Artikel 21(2)(a-e): Kræver, at enheder vedtager politikker og tekniske foranstaltninger for sikker datahåndtering, herunder begrænsninger for lagring og metoder til bortskaffelse.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 5 - Styring og kontrol: Pålægger struktureret styring af IKT-risiko, herunder sikker håndtering af informationens livscyklus.

11.7.2 Artikel 9 - Styringsramme for IKT-risiko: Kræver politikker for dataopbevaring, destruktion og juridisk/regulatorisk overholdelse i digitale driftsaktiviteter.

11.8 COBIT 2019:

11.8.1 DSS01 - Managed Operations: Understøtter sporing af opbevaring og ensartethed på tværs af datasystemer.

11.8.2 DSS05 - Managed Security Services: Sikrer beskyttelse af lagrede og arkiverede data indtil sikker bortskaffelse.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Muliggør revision af håndhævelse af opbevaring, sletteprocedurer og regulatorisk efterlevelse.