					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P15S					Dokumenttitel: **Politik for sikkerhedskopiering og gendannelse**							
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 8	Kontroller for sikkerhedskopiering i overensstemmelse med ISMS-krav
ISO/IEC 27002:2022	Kontrol 5.29, 8.13	Bedste praksis for sikkerhedskopiering og integration med forretningskontinuitet
NIST SP 800-53 Rev. 5	CP-9, MP-6	Sikkerhedskopiering og beskyttelse af medier
EU NIS2	Artikel 21(2)(c)	Robusthed og kontinuitet gennem sikkerhedskopiering
EU DORA	Artikel 10(1)	IKT-kontinuitet – sikkerhedskopiering for finansielle virksomheder
COBIT 2019	BAI04.05, DSS04	Dokumentation og test af sikkerhedskopier samt processtyring
GDPR	Artikel 5(1)(f), 32(1)(c)	Integritet, tilgængelighed og rettidig gendannelse af data

1. Formål

1.1 Denne politik fastlægger, hvordan organisationen gennemfører og styrer sikkerhedskopiering for at sikre forretningskontinuitet, beskytte mod datatab og muliggøre rettidig gendannelse efter hændelser.

1.2 Den fastsætter bindende krav til, hvordan systemer og data skal sikkerhedskopieres, opbevares og gendannes, særligt i SMV'er uden kompleks it-infrastruktur.

1.3 Denne politik understøtter revisionsberedskab og ISO/IEC 27001-certificering ved at sikre, at væsentlige kontroller for sikkerhedskopiering er etableret, anvendes konsekvent og gennemgås regelmæssigt.

1.4 Organisationens evne til at gendanne efter tekniske fejl, utilsigtet sletning eller cyberhændelser afhænger af streng efterlevelse af denne politik.

2. Omfang

2.1 Denne politik gælder for alle forretningssystemer og data, herunder:

2.1.1 Finansielle optegnelser, kundeoplysninger og HR-data

2.1.2 Stationære og bærbare computere, servere og cloudapplikationer, der anvendes i driften

2.1.3 Sikkerhedskopieringsmedier såsom USB-drev, eksterne lagringsmedier eller cloudbaserede sikkerhedskopier

2.2 Den gælder også for alle personer med ansvar for håndtering eller styring af sikkerhedskopieringsprocesser, herunder:

2.2.1 Direktøren eller anden udpeget ansvarlig

2.2.2 Eksterne it-supportleverandører eller konsulenter

2.2.3 Alle medarbejdere med ansvar for at gemme data på godkendte placeringer

3. Mål

3.1 Sikre, at alle kritiske forretningsdata og systemer sikkerhedskopieres sikkert med passende intervaller baseret på risiko og driftsmæssigt behov.

3.2 Sikre, at data kan gendannes rettidigt og fuldstændigt efter driftsforstyrrelser.

3.3 Forebygge uautoriseret adgang, manipulation eller tab af sikkerhedskopidata gennem effektive opbevaringskontroller.

3.4 Tydeligt tildele og håndhæve roller og ansvar for implementering og test af sikkerhedskopieringsprocedurer.

3.5 Understøtte overholdelse af ISO/IEC 27001, GDPR og andre regulatoriske forpligtelser gennem strukturerede og dokumenterede sikkerhedskopieringspraksisser.

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender denne politik og sikrer, at den håndhæves

4.1.2 Allokerer ressourcer og udpeger ansvarlige for aktiviteter vedrørende sikkerhedskopiering og gendannelse

4.1.3 Gennemgår fejl i sikkerhedskopiering, hændelser eller afvigelser fra politikken

4.1.4 Leder den årlige gennemgang af politikken og sikrer revisionsberedskab

4.2 Ekstern it-tjenesteudbyder (hvis relevant)

4.2.1 Implementerer og administrerer backup-løsninger (lokale eller cloudbaserede)

4.2.2 Overvåger gennemførte sikkerhedskopieringer og planlægger gendannelsestest

4.2.3 Rapporterer fejl og hændelser direkte til direktøren

4.2.4 Sikrer kryptering, adgangsbegrænsning og korrekt håndtering af backupmedier

[... 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 årligt af direktøren. Udløsende forhold for mellemliggende gennemgange omfatter:

9.1.1 Væsentlige ændringer i systemer eller lagringsmetoder

9.1.2 Indførelse af nye cloud- eller it-platforme

9.1.3 Juridiske eller regulatoriske ændringer, der påvirker datagendannelse

9.1.4 Konstateringer fra revisioner eller hændelser

9.2 Direktøren er ansvarlig for at igangsætte gennemgangen, godkende ændringer og kommunikere opdateringer.

9.3 Versioner af politikken skal versionsstyres og arkiveres. Erstattede versioner skal have begrænset adgang for at undgå forveksling under revision eller i forbindelse med forretningsgendannelse.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er tilpasset følgende SME-politikker og afhænger af dem:

10.1.1 P14S – Dataopbevaringspolitik og politik for bortskaffelse: Fastlægger, hvor længe sikkerhedskopidata skal opbevares og slettes sikkert.

10.1.2 P13S – Politik for dataklassificering og mærkning: Hjælper med at prioritere, hvilke data der skal sikkerhedskopieres, baseret på klassifikationsniveauer.

10.1.3 P30S – Politik for hændelseshåndtering: Omfatter procedurer, hvis sikkerhedskopiering mislykkes, eller hvis datagendannelse er nødvendig efter et brud eller en driftsafbrydelse.

10.1.4 P2S – Politik for styringsroller og ansvarsområder: Tildeler tydelige beføjelser til tilsyn med sikkerhedskopiering og håndhævelse af politikken.

10.1.5 P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at håndtering af sikkerhedskopier med personoplysninger sker i overensstemmelse med databeskyttelseslovgivning og regulatoriske krav.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1: operationel planlægning og styring af backupsystemer som en del af ISMS

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.13: Fastlægger bedste praksis for planlægning, overvågning og gendannelse af sikkerhedskopier

11.2.2 Bilag A, kontrol 5.29: Integration af sikkerhedskopiering med forretningskontinuitet og gendannelsesberedskab

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (beredskabsplanlægning): Fastlægger strukturerede backupstrategier til understøttelse af forretningsmæssig robusthed

11.3.2 MP-6 (mediebeskyttelse): Kræver sikker håndtering og destruktion af backupmedier

11.4 GDPR

11.4.1 Artikel 5(1)(f): Kræver integritet og tilgængelighed af personoplysninger

11.4.2 Artikel 32(1)(c): Kræver evnen til rettidigt at gendanne adgang til personoplysninger

11.5 NIS2-direktivet

11.5.1 Artikel 21(2)(c): Kræver sikkerhedskopiering og gendannelse som en del af planlægning for robusthed og kontinuitet

11.6 DORA

11.6.1 Artikel 10(1): Organisationer i den finansielle sektor skal sikre sikkerhedskopiering som en del af foranstaltninger for IKT-kontinuitet

11.7 COBIT 2019

11.7.1 BAI04.05: Kræver dokumenterede backupstrategier

11.7.2 DSS04.07: Fremhæver rutinemæssig test og styring af processer for sikkerhedskopiering og datagendannelse