					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P15					Dokumenttitel: **Politik for backup 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/forordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1.3, 8	Risikobehandling, planlægning og operationelle backupkontroller
ISO/IEC 27002:2022	Kontroller 8.13, 5.28, 5.29	Backupstyring, sikker bortskaffelse og robusthed
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Krav til systembackup, gendannelse og sanitering af medier
EU GDPR	Artikel 32, betragtning 49	Gendannelse og tilgængelighed af personoplysninger samt forretningskontinuitet
EU NIS2	Artikel 21(2)(c-e)	Backup- og kontinuitetskontroller for robusthed
EU DORA	Artikel 10, 11	Krav til backup, gendannelse og test i den finansielle sektor
COBIT 2019	DSS01, DSS04, MEA03	Backupdrift, kontinuitet og overvågning af efterlevelse

1. Formål

1.1 Formålet med denne politik er at fastlægge de obligatoriske krav til backup og gendannelse af data, systemer og applikationer for at understøtte operationel robusthed, dataintegritet og forretningskontinuitet.

1.2 Politikken etablerer en standardiseret ramme til at:

1.2.1 Beskytte organisationens data mod tab som følge af sletning, korruption, fejl eller cyberangreb

1.2.2 Fastlægge forventninger til gendannelse gennem klare parametre for RTO (Recovery Time Objective) og RPO (Recovery Point Objective)

1.2.3 Integrere backupdrift med det overordnede ledelsessystem for informationssikkerhed (ISMS) og planer for forretningskontinuitet og katastrofeberedskab (BCP/DRP)

1.2.4 Sikre overholdelse af gældende lovgivning og sektorspecifik regulering vedrørende tilgængelighed og mulighed for gendannelse

1.3 Politikken håndhæver kontroller i ISO/IEC 27001:2022 vedrørende sikker bortskaffelse af data (5.28), robusthed (5.29) og informationsbackup (8.13) og er tilpasset best practice fra ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA og NIS2.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle forretningskritiske og operationelle systemer inden for ISMS-omfanget

2.1.2 Alle strukturerede og ustrukturerede forretningsdata, herunder databaser, filer, e-mails og konfigurationer

2.1.3 Alle miljøer - on-premises, cloud, hybride og eksterne lagringsmiljøer

2.1.4 Alt personale med ansvar for at styre, udføre, verificere eller gendanne backupprocesser

2.2 Den gælder også for:

2.2.1 Backupmedier og backupinfrastruktur, herunder fysiske bånd, virtuelle appliances, disksnapshots og cloudbaserede backupløsninger

2.2.2 Tredjepartsleverandører med kontrakt om at hoste, administrere eller behandle organisationens backups

2.2.3 Backup af logfiler, konfigurationer, revisionsspor og driftsdokumentation, der er kritisk for forretningskontinuiteten

2.3 Systemer, der udtrykkeligt er undtaget fra backup, skal dokumenteres, risikovurderes og formelt godkendes af den ISMS-ansvarlige og systemejeren.

3. Mål

3.1 Sikre, at alle kritiske systemer og data sikkerhedskopieres pålideligt med tilstrækkelig frekvens, redundans og sikkerhedskontroller.

3.2 Etablere gendannelsesmekanismer, der opfylder fastlagte forventninger til RTO og RPO i overensstemmelse med business impact analysis.

3.3 Opretholde fuldstændig dokumentation for backupprocedurer, opbevaringsplaner, roller og teknologier.

3.4 Validere effektiviteten af backupdriften gennem systematisk test af gendannelse, logning af fejl og sporing af afhjælpning.

3.5 Beskytte backupdata mod uautoriseret adgang, ændring eller ødelæggelse gennem hele deres livscyklus.

3.6 Muliggøre overholdelse af:

3.6.1 ISO/IEC 27001-krav til operationelle kontroller og kontinuitetskontroller

3.6.2 NIST SP 800-53 CP- og MP-familierne for backup og sanitering

3.6.3 GDPR artikel 32 og betragtning 49 om gendannelse af adgang til personoplysninger

3.6.4 DORA artikel 10 og NIS2 artikel 21 om IKT-forretningskontinuitet og robusthed

3.7 Sikre, at tredjeparts backuptjenester opfylder kontraktlige og regulatoriske sikkerhedsforpligtelser, herunder kryptering, bortskaffelse og underretningsprotokoller.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender denne politik og sikrer, at forretningskritiske systemer er tilstrækkeligt beskyttet gennem godkendte praksisser for backup og gendannelse.

4.1.2 Er ansvarlig for, at backupdriften er tilstrækkeligt ressourceunderstøttet og gennemgås periodisk med henblik på regulatorisk efterlevelse.

4.2 Chief Information Security Officer (CISO)

4.2.1 Ejer denne politik og sikrer tilpasning til de overordnede rammer for informationssikkerhed, risikostyring og kontinuitet.

4.2.2 Fører tilsyn med integrationen af backupprocedurer i BCP/DRP, håndtering af sikkerhedshændelser og planlægning af robusthed.

4.2.3 Gennemgår backupundtagelser og vurderer forslag om risikoaccept for udelukkelse af kritiske systemer.

[... 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 tidligere, hvis det udløses af:

9.1.1 Ændringer i strategien for forretningskontinuitet eller katastrofeberedskab

9.1.2 Nye regulatoriske eller retlige forpligtelser, der påvirker backupfrekvens eller dataopbevaring

9.1.3 Ændringer i systemarkitektur, backupværktøjer eller tjenesteudbydere

9.1.4 Væsentlige hændelser eller revisionskonstateringer relateret til datatab eller gendannelsesfejl

9.2 Gennemgangen skal koordineres af CISO i samarbejde med:

9.2.1 IT-infrastruktur og drift

9.2.2 Intern revision

9.2.3 Data Protection Officer (DPO)

9.2.4 Teams for forretningskontinuitet og katastrofeberedskab

9.3 Backupplaner, lister over omfattede systemer, gendannelsesdokumentation og undtagelseslogfiler skal gennemgås parallelt for at sikre:

9.3.1 Korrekt backupdækning for alle kritiske aktiver

9.3.2 Overholdelse af RTO/RPO og krav til opbevaring

9.3.3 Fuldstændighed i testlogfiler og hændelsesrapporter

9.3.4 Korrektion af tidligere identificerede kontrolmangler

9.4 Alle opdateringer skal:

9.4.1 Være underlagt versionsstyring og opbevares i ISMS-dokumentrepository

9.4.2 Indeholde en opsummering af ændringer og begrundelse

9.4.3 Godkendes af direktionen

9.4.4 Kommunikeres til alt berørt teknisk personale og forretningspersonale

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter direkte og hænger sammen med følgende relaterede dokumenter:

10.1.1 P6 - Politik for risikostyring: Identificerer risikobaseret prioritering af backupbeskyttelse for systemer og tjenester.

10.1.2 P12 - Politik for aktivstyring: Sikrer, at systemer, der er omfattet af backup, er registreret i aktivfortegnelsen og knyttet til livscyklus- og klassifikationssporing.

10.1.3 P13 - Politik for dataklassificering og mærkning: Angiver hvilke datakategorier der kræver backup, herunder mærkningsmetadata til prioritering.

10.1.4 P14 - Politik for dataopbevaring og bortskaffelse: Koordinerer backupopbevaring med regulatoriske opbevaringsgrænser og korrekt bortskaffelse af udløbne medier.

10.1.5 P16 - Politik for datamaskering og pseudonymisering: Understøtter dataminimering ved backup af følsomme datasæt.

10.1.6 P30 - Politik for hændelseshåndtering: Aktiveres ved backupfejl, gendannelsesproblemer eller kompromittering af backupdatarepositories.

10.2 Disse sammenhængende politikker udgør en samlet ramme, der sikrer, at backupstyring er indlejret i organisationens overordnede ISMS og strategi for operationel robusthed.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:

11.1.1 Klausul 6.1.3 - risikobehandlingsplan: Understøtter risikobaseret prioritering af backup og planlægning af gendannelse.

11.1.2 Klausul 8.1 - operationel planlægning og styring: Integrerer gendannelses- og kontinuitetskontroller som en del af de operationelle sikkerhedsforanstaltninger.

11.1.3 Bilag A kontrol 5.28 - sikker bortskaffelse eller genbrug af udstyr: Omhandler sikker sanitering af backupmedier.

11.1.4 Bilag A kontrol 5.29 - informationssikkerhed under forstyrrelser: Sikrer gendannelseskapaciteter under hændelser eller katastrofer.

11.1.5 Bilag A kontrol 8.13 - informationsbackup: Er direkte adresseret gennem planlagt, testet og sikker backupdrift.

11.2 ISO/IEC 27002:2022 - kontroller 8.13, 5.28, 5.29: Disse kontroller understøtter kravet om regelmæssige backups, integritetsvalidering og planlægning af gendannelse på tværs af alle IT-miljøer.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - systembackup: Etablerer omfattende backupprocedurer, herunder ekstern lagring og test af gendannelse.

11.3.2 CP-10 - systemgenopretning og gendannelse: Kræver validerede procedurer for fuld eller delvis gendannelse i overensstemmelse med gendannelsesmål.

11.3.3 MP-6 - sanitering af medier: Sikrer sikker håndtering af forældede backupmedier.

11.3.4 SI-12 - procedurer for informationshåndtering: Understøtter ansvar for backup og gendannelse af følsomme data.

11.4 EU GDPR (2016/679):

11.4.1 Artikel 32 - behandlingssikkerhed: Pålægger krav om gendannelseskapaciteter og sikkerhedsforanstaltninger for datatilgængelighed, særligt for personoplysninger.

11.4.2 Betragtning 49: Understøtter forretningskontinuitet og katastrofeberedskabsforanstaltninger, herunder sikker backup som en del af organisationens robusthed.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Artikel 21(2)(c-e): Kræver tekniske og organisatoriske foranstaltninger, herunder backup- og kontinuitetskontroller, for at sikre tjenesternes robusthed.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 10 - IKT-forretningskontinuitet: Kræver, at finansielle enheder har fuld backup af data, gendannelse og kontinuitetsplanlægning.

11.6.2 Artikel 11 - test af planer for IKT-forretningskontinuitet: Fremhæver validering af gendannelseskapacitet gennem regelmæssig test.

11.7 COBIT 2019:

11.7.1 DSS01 - Managed Operations: Understøtter pålidelig levering af tjenester gennem beskyttet datatilgængelighed.

11.7.2 DSS04 - Managed Continuity: Definerer strategiske og operationelle kontinuitetskontroller, herunder verificerede backups.

11.7.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Kræver periodisk gennemgang af kontinuitetsforanstaltninger, herunder effektiviteten af backupkontroller.