					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P15					Dokumenttitel: **Policy för säkerhetskopiering och återställning**							
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**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 6.1.3, 8	Riskbehandling, planering och operativa kontroller för säkerhetskopiering
ISO/IEC 27002:2022	Kontroller 8.13, 5.28, 5.29	Hantering av säkerhetskopiering, säker bortskaffning och motståndskraft
NIST SP 800-53 Rev. 5	CP-9, CP-10, SI-12, MP-6	Krav på systemsäkerhetskopiering, återställning och sanering av lagringsmedier
EU:s GDPR	Artikel 32, skäl 49	Återställning och tillgänglighet för personuppgifter samt verksamhetskontinuitet
EU:s NIS2-direktiv	Artikel 21(2)(c-e)	Kontroller för säkerhetskopiering och kontinuitet för resiliens
EU:s DORA-förordning	Artiklarna 10, 11	Krav inom finanssektorn avseende säkerhetskopiering, återställning och testning
COBIT 2019	DSS01, DSS04, MEA03	Drift av säkerhetskopiering, kontinuitet och övervakning av efterlevnad

1. Syfte

1.1 Syftet med denna policy är att fastställa bindande krav för säkerhetskopiering och återställning av data, system och applikationer för att stödja operativ resiliens, dataintegritet och verksamhetskontinuitet.

1.2 Policyn fastställer ett standardiserat ramverk för att:

1.2.1 Skydda organisationens data mot förlust till följd av radering, korruption, fel eller cyberattacker

1.2.2 Fastställa krav på återställning genom tydliga parametrar för RTO (Recovery Time Objective) och RPO (Recovery Point Objective)

1.2.3 Integrera säkerhetskopieringsverksamheten med det övergripande ISMS samt planer för verksamhetskontinuitet (BCP/DRP)

1.2.4 Säkerställa efterlevnad av tillämpliga lagar och sektorsspecifika regelverk avseende tillgänglighet och återställbarhet

1.3 Policyn implementerar kontroller enligt ISO/IEC 27001:2022 avseende säker bortskaffning av data (5.28), motståndskraft (5.29) och säkerhetskopiering av information (8.13), och är anpassad till etablerad branschpraxis enligt ISO/IEC 27002:2022, NIST SP 800-53 Rev. 5, EU:s GDPR, EU:s DORA-förordning och EU:s NIS2-direktiv.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla verksamhetskritiska och operativa system inom ISMS omfattning

2.1.2 Alla strukturerade och ostrukturerade verksamhetsdata, inklusive databaser, filer, e-postmeddelanden och konfigurationer

2.1.3 Alla miljöer – lokala miljöer, molnmiljöer, hybrida miljöer samt fjärrlagring och extern lagring

2.1.4 All personal som ansvarar för att hantera, utföra, verifiera eller återställa säkerhetskopieringsprocesser

2.2 Den gäller även för:

2.2.1 Säkerhetskopieringsmedier och infrastruktur, inklusive fysiska band, virtuella appliance-lösningar, diskögonblicksbilder och molnbaserade säkerhetskopieringslösningar

2.2.2 Tredjepartsleverantörer som har avtalats för att lagra, hantera eller behandla organisationens säkerhetskopior

2.2.3 Säkerhetskopiering av loggar, konfigurationer, revisionsspår och operativ dokumentation som är kritisk för kontinuiteten

2.3 System som uttryckligen undantas från säkerhetskopiering ska dokumenteras, riskbedömas och formellt godkännas av ISMS-ansvarig och systemägare.

3. Mål

3.1 Säkerställa att alla kritiska system och data säkerhetskopieras tillförlitligt med tillräcklig frekvens, redundans och lämpliga säkerhetskontroller.

3.2 Tillhandahålla återställningsmekanismer som uppfyller fastställda RTO- och RPO-krav i linje med verksamhetskonsekvensanalyser.

3.3 Upprätthålla fullständig dokumentation av säkerhetskopieringsrutiner, bevarandescheman, roller och tekniska lösningar.

3.4 Validera effektiviteten i säkerhetskopieringsverksamheten genom systematisk testning av återställning, loggning av fel och uppföljning av korrigerande åtgärder.

3.5 Skydda säkerhetskopierade data mot obehörig åtkomst, ändring eller förstöring under hela informationslivscykeln.

3.6 Möjliggöra efterlevnad av:

3.6.1 Operativa krav och kontinuitetskrav enligt ISO/IEC 27001

3.6.2 NIST SP 800-53:s CP- och MP-familjer för säkerhetskopiering och sanering

3.6.3 Artikel 32 och skäl 49 i EU:s GDPR avseende återställning av åtkomst till personuppgifter

3.6.4 Artikel 10 i DORA och artikel 21 i NIS2 avseende IKT-kontinuitet och motståndskraft

3.7 Säkerställa att tredjepartsbaserade säkerhetskopieringstjänster uppfyller avtalskrav och regulatoriska säkerhetskrav, inklusive kryptering, bortskaffning och underrättelseförfaranden.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Fastställer denna policy och säkerställer att verksamhetskritiska system skyddas på ett ändamålsenligt sätt genom godkända rutiner för säkerhetskopiering och återställning.

4.1.2 Är ytterst ansvarig för att säkerställa att säkerhetskopieringsverksamheten har tillräckliga resurser och granskas periodiskt avseende regulatorisk efterlevnad.

4.2 Informationssäkerhetschef (CISO)

4.2.1 Är policyägare för denna policy och säkerställer anpassning till övergripande ramverk för informationssäkerhet, riskhantering och kontinuitet.

4.2.2 Utövar tillsyn över integrationen av säkerhetskopieringsrutiner i BCP/DRP, incidenthantering och planering för motståndskraft.

4.2.3 Granskar undantag från säkerhetskopiering och utvärderar förslag till riskacceptans för undantag av kritiska system.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas minst en gång per år, eller tidigare om det utlöses av:

9.1.1 Förändringar i strategi för verksamhetskontinuitet eller katastrofåterställning

9.1.2 Nya regulatoriska eller rättsliga krav som påverkar säkerhetskopieringsfrekvens eller databevarande

9.1.3 Förändringar i systemarkitektur, säkerhetskopieringsverktyg eller tjänsteleverantörer

9.1.4 Betydande incidenter eller revisionsiakttagelser kopplade till dataförlust eller misslyckad återställning

9.2 Granskningen ska samordnas av CISO i samarbete med:

9.2.1 IT-infrastruktur och drift

9.2.2 Internrevision

9.2.3 Dataskyddsombud (DPO)

9.2.4 Team för verksamhetskontinuitet och katastrofåterställning

9.3 Säkerhetskopieringsscheman, listor över inkluderade system, återställningsdokumentation och undantagsloggar ska granskas parallellt för att säkerställa:

9.3.1 Korrekt täckning av säkerhetskopiering för alla kritiska tillgångar

9.3.2 Efterlevnad av krav på RTO/RPO och bevarande

9.3.3 Fullständighet i testloggar och incidentrapporter

9.3.4 Åtgärdande av tidigare identifierade kontrollbrister

9.4 Alla uppdateringar ska:

9.4.1 Versionshanteras och bevaras i ISMS dokumentregister

9.4.2 Innehålla en ändringssammanfattning och motivering

9.4.3 Godkännas av verkställande ledning

9.4.4 Kommuniceras till all berörd teknisk personal och verksamhetspersonal

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer direkt och samverkar med följande relaterade dokument:

10.1.1 P6 - Riskhanteringspolicy: Identifierar riskbaserad prioritering av säkerhetskopieringsskydd för system och tjänster.

10.1.2 P12 - Policy för tillgångshantering: Säkerställer att system som ska omfattas av säkerhetskopiering finns i tillgångsförteckningen och är kopplade till livscykelspårning och klassificering.

10.1.3 P13 - Policy för dataklassificering och märkning: Styr vilka datakategorier som kräver säkerhetskopiering, inklusive märkningsmetadata för prioritering.

10.1.4 P14 - Policy för databevarande och bortskaffning: Samordnar bevarande av säkerhetskopior med regulatoriska bevarandegränser och korrekt bortskaffning av utgångna medier.

10.1.5 P16 - Policy för datamaskering och pseudonymisering: Stödjer uppgiftsminimering vid säkerhetskopiering av känsliga dataset.

10.1.6 P30 - Policy för incidenthantering: Aktiveras vid fel i säkerhetskopiering, återställningsproblem eller kompromettering av lagringsplatser för säkerhetskopior.

10.2 Dessa sammankopplade policyer utgör ett sammanhållet ramverk som säkerställer att styrningen av säkerhetskopiering är integrerad i organisationens övergripande ISMS och strategi för operativ resiliens.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:

11.1.1 Klausul 6.1.3 - riskbehandlingsplan: Stödjer riskbaserad prioritering av säkerhetskopiering och planering av återställning.

11.1.2 Klausul 8.1 - operativ planering och styrning: Integrerar återställnings- och kontinuitetskontroller som en del av de operativa skyddsåtgärderna.

11.1.3 Bilaga A kontroll 5.28 - säker bortskaffning eller återanvändning av utrustning: Omfattar säker sanering av säkerhetskopieringsmedier.

11.1.4 Bilaga A kontroll 5.29 - informationssäkerhet vid störningar: Säkerställer återställningsförmåga vid incidenter eller katastrofer.

11.1.5 Bilaga A kontroll 8.13 - säkerhetskopiering av information: Hanteras direkt genom schemalagd, testad och säker säkerhetskopieringsverksamhet.

11.2 ISO/IEC 27002:2022 - kontroller 8.13, 5.28, 5.29: Dessa kontroller förstärker kravet på regelbunden säkerhetskopiering, integritetsvalidering och planering för återställning i alla IT-miljöer.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 CP-9 - systemsäkerhetskopiering: Fastställer heltäckande säkerhetskopieringsrutiner, inklusive lagring utanför arbetsplatsen och återställningstester.

11.3.2 CP-10 - återhämtning och återställning av system: Kräver validerade rutiner för fullständig eller partiell återställning i linje med återställningsmålen.

11.3.3 MP-6 - sanering av medier: Säkerställer säker hantering av uttjänta säkerhetskopieringsmedier.

11.3.4 SI-12 - rutiner för informationshantering: Förstärker ansvar för säkerhetskopiering och återställning av känsliga data.

11.4 EU:s GDPR (2016/679):

11.4.1 Artikel 32 - behandlingens säkerhet: Kräver återställningsförmåga och skyddsåtgärder för datatillgänglighet, särskilt för personuppgifter.

11.4.2 Skäl 49: Stödjer åtgärder för verksamhetskontinuitet och katastrofåterställning, inklusive säker säkerhetskopiering som del av organisatorisk motståndskraft.

11.5 EU:s NIS2-direktiv (2022/2555):

11.5.1 Artikel 21(2)(c-e): Kräver tekniska och organisatoriska åtgärder, inklusive säkerhetskopiering och kontinuitetskontroller, för att säkerställa tjänsters motståndskraft.

11.6 EU:s DORA-förordning (2022/2554):

11.6.1 Artikel 10 - IKT-verksamhetskontinuitet: Kräver att finansiella entiteter har fullständig säkerhetskopiering av data, återställning och kontinuitetsplanering.

11.6.2 Artikel 11 - testning av planer för IKT-verksamhetskontinuitet: Betonar validering av återställningsförmåga genom regelbunden testning.

11.7 COBIT 2019:

11.7.1 DSS01 - hanterad drift: Stödjer tillförlitlig leverans av tjänster genom skyddad datatillgänglighet.

11.7.2 DSS04 - hanterad kontinuitet: Fastställer strategiska och operativa kontinuitetskontroller, inklusive verifierade säkerhetskopior.

11.7.3 MEA03 - övervaka, utvärdera och bedöma efterlevnad: Kräver periodisk granskning av kontinuitetsåtgärder, inklusive effektiviteten i säkerhetskopieringskontroller.