					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P15S					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/förordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Kontroller för säkerhetskopiering enligt kraven i ISMS
ISO/IEC 27002:2022	Kontroller 5.29, 8	Bästa praxis för säkerhetskopiering och integration med verksamhetskontinuitet
NIST SP 800-53 Rev.5	CP-9, MP-6	Säkerhetskopiering och skydd av lagringsmedier
EU:s NIS2-direktiv	Artikel 21.2 c	Resiliens och kontinuitet genom säkerhetskopiering
DORA-förordningen	Artikel 10.1	IKT-kontinuitet – säkerhetskopiering för finansiella entiteter
COBIT 2019	BAI04.05, DSS04	Dokumentation och testning av säkerhetskopior samt kontrollprocesser
EU:s GDPR	Artiklarna 5.1 f, 32.1 c	Integritet, tillgänglighet och återställning av data i rätt tid

1. Syfte

1.1 Denna policy anger hur organisationen ska utföra och hantera säkerhetskopiering för att säkerställa verksamhetskontinuitet, skydda mot dataförlust och möjliggöra återställning i rätt tid efter incidenter.

1.2 Den fastställer bindande krav för hur system och data ska säkerhetskopieras, lagras och återställas, särskilt i små och medelstora företag utan komplex IT-infrastruktur.

1.3 Denna policy stödjer revisions- och certifieringsberedskap enligt ISO/IEC 27001 genom att säkerställa att väsentliga kontroller för säkerhetskopiering finns på plats, tillämpas konsekvent och granskas regelbundet.

1.4 Organisationens förmåga att återställa verksamheten efter tekniska fel, oavsiktlig radering eller cyberincidenter är beroende av att denna policy efterlevs strikt.

2. Omfattning

2.1 Denna policy gäller för alla verksamhetssystem och all data, inklusive:

2.1.1 finansiella register, kundinformation och HR-data

2.1.2 stationära datorer, bärbara datorer, servrar och molntjänster som används i verksamheten

2.1.3 säkerhetskopieringsmedier såsom USB-enheter, extern lagring eller säkerhetskopior i molnmiljö

2.2 Den gäller även för alla personer med ansvar för att hantera eller administrera säkerhetskopieringsprocesser, inklusive:

2.2.1 verkställande direktör eller annan utsedd ansvarig

2.2.2 externa IT-tjänsteleverantörer eller konsulter

2.2.3 samtliga anställda som ansvarar för att spara data på godkända platser

3. Mål

3.1 Säkerställa att all kritisk verksamhetsinformation och alla kritiska system säkerhetskopieras på ett säkert sätt med lämpliga intervall utifrån risk och verksamhetens behov.

3.2 Säkerställa att data kan återställas fullständigt och inom rimlig tid efter störningar.

3.3 Förhindra obehörig åtkomst, manipulation eller förlust av säkerhetskopierad data genom effektiva lagringskontroller.

3.4 Tydligt fastställa och upprätthålla roller och ansvar för genomförande och testning av säkerhetskopieringsrutiner.

3.5 Stödja efterlevnad av ISO/IEC 27001, EU:s GDPR och andra regulatoriska krav genom strukturerad och dokumenterad säkerhetskopieringspraxis.

4. Roller och ansvar

4.1 Verkställande direktör

4.1.1 godkänner denna policy och säkerställer att den tillämpas

4.1.2 tilldelar resurser och utser ansvariga för aktiviteter avseende säkerhetskopiering och återställning

4.1.3 granskar fel i säkerhetskopiering, incidenter och policyavvikelser

4.1.4 leder den årliga policygranskningen och säkerställer revisionsberedskap

4.2 Extern IT-tjänsteleverantör (om tillämpligt)

4.2.1 inför och förvaltar lösningar för säkerhetskopiering lokalt eller i molnmiljö

4.2.2 övervakar utfallet av säkerhetskopieringar och schemalägger återställningstester

4.2.3 rapporterar fel och incidenter direkt till verkställande direktör

4.2.4 säkerställer kryptering, åtkomstbegränsningar och korrekt hantering av säkerhetskopieringsmedier

[... 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 av verkställande direktör. Utlösande faktorer för mellanliggande granskning omfattar:

9.1.1 väsentliga ändringar i system eller lagringsmetoder

9.1.2 införande av nya molnplattformar eller IT-plattformar

9.1.3 rättsliga eller regulatoriska förändringar som påverkar dataåterställning

9.1.4 iakttagelser från revisioner eller incidenter

9.2 Verkställande direktör ansvarar för att initiera granskningen, godkänna ändringar och kommunicera uppdateringar.

9.3 Policyversioner ska följas upp och arkiveras. Ersatta versioner ska vara åtkomstbegränsade för att undvika oklarheter vid revision eller återställning av verksamheten.

10. Relaterade policyer och kopplingar

10.1 Denna policy är anpassad till och beroende av följande SME-policyer:

10.1.1 P14S – Policy för databevarande och bortskaffande: Anger hur länge säkerhetskopierad data ska bevaras och hur den ska raderas på ett säkert sätt.

10.1.2 P13S – Policy för dataklassificering och märkning: Hjälper till att prioritera vilka data som ska säkerhetskopieras utifrån klassificeringsnivåer.

10.1.3 P30S – Policy för incidenthantering: Omfattar rutiner om säkerhetskopiering misslyckas eller om dataåterställning krävs efter intrång eller avbrott.

10.1.4 P2S – Policy för styrningsroller och ansvar: Tilldelar tydliga befogenheter för styrning av säkerhetskopiering och tillämpning av policyn.

10.1.5 P17S – Policy för dataskydd och integritet: Säkerställer att hantering av personuppgifter i säkerhetskopiering är förenlig med rättsliga krav och integritetsregler.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1: Operativ planering och styrning av säkerhetskopiering som en del av ISMS

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.13: Anger bästa praxis för schemaläggning, övervakning och återställning av säkerhetskopiering

11.2.2 Bilaga A, kontroll 5.29: Integrering av säkerhetskopiering med verksamhetskontinuitet och återställningsberedskap

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Contingency Planning): Definierar strukturerade strategier för säkerhetskopiering för verksamhetens motståndskraft

11.3.2 MP-6 (Media Protection): Kräver säker hantering och destruktion av säkerhetskopieringsmedier

11.4 EU:s GDPR

11.4.1 Artikel 5.1 f: Kräver integritet och tillgänglighet för personuppgifter

11.4.2 Artikel 32.1 c: Kräver förmåga att återställa tillgång till personuppgifter inom rimlig tid

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21.2 c: Kräver säkerhetskopiering och återställning som en del av planering för resiliens och kontinuitet

11.6 DORA-förordningen

11.6.1 Artikel 10.1: Organisationer i den finansiella sektorn ska säkerställa säkerhetskopiering som en del av åtgärder för IKT-kontinuitet

11.7 COBIT 2019

11.7.1 BAI04.05: Kräver dokumenterade strategier för säkerhetskopiering

11.7.2 DSS04.07: Betonar regelbunden testning och kontroll av processer för säkerhetskopiering och återställning