					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P32S					Dokumenttitel: **Policy för verksamhetskontinuitet och katastrofåterställning**							
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	Klausul 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontroller 5.29, 5	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
EU:s dataskyddsförordning (GDPR)	Artiklarna 32, 33	
EU:s NIS2-direktiv	Artikel 21.2 f	
EU:s DORA-förordning	Artikel 10	
COBIT 2019	DSS	

1. Syfte

1.1 Denna policy säkerställer att organisationen kan upprätthålla verksamheten och återställa väsentliga IT-tjänster under och efter störningar såsom strömavbrott, cyberattacker, ransomwareangrepp eller systemfel.

1.2 Den tillhandahåller ett tydligt ramverk för planering av verksamhetskontinuitet och katastrofåterställning (BC/DR), anpassat för små och medelstora företag utan särskilda IT-team.

1.3 Denna policy hjälper organisationen att uppfylla tillämpliga krav enligt ISO/IEC 27001:2022, GDPR, NIS2, DORA och COBIT 2019, samtidigt som den stärker verksamhetens resiliens och kundernas förtroende.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla verksamhetskritiska system och tjänster (t.ex. e-post, molnlagring, faktureringsplattformar, kundregister)

2.1.2 Alla anställda och externa IT-tjänsteleverantörer med ansvar för beredskap och genomförande inom BC/DR

2.1.3 Alla typer av störningar, inklusive cyberincidenter, hårdvarufel, strömavbrott, översvämning och otillgängliga kontorslokaler

2.2 Den omfattar:

2.2.1 hantering av säkerhetskopiering

2.2.2 planering för verksamhetskontinuitet (BCP)

2.2.3 åtgärder för katastrofåterställning

2.2.4 utbildning och testning av personal

2.2.5 rättsliga och regulatoriska rutiner för hantering av incidenter

3. Mål

3.1 Skydda organisationens förmåga att leverera viktiga tjänster trots oplanerade störningar.

3.2 Säkerställa snabb återställning av system och data utifrån fördefinierade återställningstidsmål (RTO).

3.3 Säkerställa att all personal kan följa kontinuitetsrutiner under kriser med minimal osäkerhet.

3.4 Upprätthålla efterlevnad av lagkrav avseende dataskydd och operativ resiliens, inklusive artikel 32 i GDPR och artikel 21 i NIS2.

3.5 Etablera en praktisk och testbar strategi för kontinuitet och återställning som är lämplig för små och medelstora företag.

4. Roller och ansvar

4.1 Verkställande chef (GM)

4.1.1 Äger BC/DR-processen och denna policy

4.1.2 Godkänner planen för verksamhetskontinuitet (BCP)

4.1.3 Samordnar incidenthantering och intern kommunikation under störningar

4.1.4 Gör regulatoriska anmälningar vid behov (t.ex. anmälan av personuppgiftsincidenter enligt GDPR)

4.2 IT-leverantör/systemadministratör

4.2.1 Underhåller och testar säkerhetskopior

4.2.2 Verkställer rutiner för katastrofåterställning när de aktiveras

4.2.3 Dokumenterar alla återställningsåtgärder och händelser kopplade till systemåterställning

4.2.4 Rapporterar omedelbart kritiska IT-incidenter till GM

[... 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 Årlig granskning av policy och plan

9.1.1 Verkställande chef (GM) ska säkerställa att denna policy och tillhörande plan för verksamhetskontinuitet (BCP) formellt granskas minst en gång per år.

9.1.2 Granskningen ska omfatta:

9.1.2.1 utvärdering av nya eller framväxande risker

9.1.2.2 förnyad validering av RTO/RPO

9.1.2.3 verifiering av leverantörs- och kontaktinformation

9.1.2.4 anpassning till förändringar i IKT-system, rättsliga skyldigheter eller verksamheten

9.2 Utlösarbaserade uppdateringar

9.2.1 Denna policy ska även uppdateras vid:

9.2.1.1 större incidenter eller störningar, särskilt om målen inte uppnåddes

9.2.1.2 nya rättsliga eller regulatoriska skyldigheter (t.ex. ändringar i DORA)

9.2.1.3 förändringar i kritiska system, molnplattformar eller personal

9.2.1.4 iakttagelser från årliga BCP/DR-tester

9.3 Process för ändringsstyrning

9.3.1 Alla ändringar ska godkännas av GM

9.3.2 En versionshistorik ska föras, inklusive datum, beskrivning av ändringen och godkännare

9.3.3 Den uppdaterade policyn ska distribueras på nytt till all relevant personal, inklusive IT-leverantören och avdelningscheferna

9.4 Dokumentation av lärdomar

9.4.1 Efter tester eller faktiska störningar ska dokumenterade lärdomar införas i kommande revideringar

9.4.2 Dessa granskningar ska även omfatta utvärdering av leverantörers prestation och kontroll av om hanteringen var tillräcklig

10. Relaterade policyer och kopplingar

10.1 Denna policy är nära integrerad med följande SME-policyer:

10.1.1 P1S – Informationssäkerhetspolicy: Definierar de övergripande säkerhetsmålen som kontinuitets- och återställningsrutiner ska stödja.

10.1.2 P4S – Policy för åtkomstkontroll: Möjliggör akut återkallelse eller återställning av användaråtkomst vid scenarier med verksamhetsstörning.

10.1.3 P6S – Riskhanteringspolicy: Utgör grunden för att identifiera, utvärdera och prioritera kontinuitetsrelaterade risker.

10.1.4 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att anställda är förberedda att agera vid störningar och förstår BCP.

10.1.5 P15S – Policy för säkerhetskopiering och återställning: Anger specifika tekniska rutiner för att skydda datatillgänglighet och återhämtning.

10.1.6 P17S – Policy för dataskydd och integritet: Säkerställer att kontinuitetsplanering respekterar skyddet av personuppgifter och följer GDPR under och efter incidenter.

10.1.7 P22S – Policy för loggning och övervakning: Stödjer detektering av händelser som kan utlösa BC/DR-processer och tillhandahåller forensiska revisionsspår efter störningar.

10.1.8 P30S – Policy för incidenthantering: Föregår direkt aktivering av återställningsprocessen vid cyberincidenter eller operativa incidenter.

10.1.9 P31S – Policy för bevisinsamling och forensik: Säkerställer att digital bevisning samlas in vid kontinuitetsscenarier för regelefterlevnad, försäkring eller utredningsbehov.

10.2 Dessa policyer utgör tillsammans ett sammanhållet, revisionsklart ramverk för resiliens, ansvarsskyldighet och kontinuitet i kontroller inom hela SME-verksamheten.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:

11.1.1 Klausul 6.1 – Kräver riskbaserad planering och behandling, inklusive verksamhetskontinuitet och återställning.

11.1.2 Klausul 6.3 – Betonar kontinuerlig förbättring efter störningar.

11.1.3 Klausul 8.1 – Kräver operativa kontroller, inklusive dokumenterade kontinuitetsåtgärder.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 5.29 – Kräver att arrangemang för verksamhetskontinuitet etableras och upprätthålls.

11.2.2 Kontroll 5.30 – Kräver testning och granskning av dessa arrangemang.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Definierar krav för beredskapsplanering.

11.3.2 CP-4 – Kräver beredskapsutbildning för organisationens personal.

11.3.3 CP-6 – Omfattar krav på alternativ lagringsplats.

11.3.4 CP-7 – Styr krav på alternativ plats för bearbetning.

11.4 EU:s dataskyddsförordning (GDPR):

11.4.1 Artikel 32 – Kräver åtgärder för att säkerställa fortlöpande tillgänglighet och resiliens i behandlingssystem och tjänster.

11.4.2 Artikel 33 – Utlöser skyldigheter att anmäla personuppgiftsincidenter när bristande kontinuitet leder till att personuppgifter kompromitteras.

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

11.5.1 Artikel 21.2 f – Kräver kontinuitetsplanering och förmåga till krishantering som en del av beredskapen för cyberrisker.

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

11.6.1 Artikel 10 – Kräver genomförande av testning för digital operativ resiliens och återställningsförmåga, särskilt för SME-företag inom finanssektorn.

11.7 COBIT 2019:

11.7.1 DSS04 – Hantera kontinuitet: Ger vägledning för styrning och ledning för att upprätthålla och validera operativ resiliens, inklusive ägarskap, testning, leverantörsintegration och granskningar efter händelser.