					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P32					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**

Anslutning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	
ISO/IEC 27002:2022	Kontroller 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 till CP-11	
NIST SP 800-34 Rev.1	Beredskapsplanering	Ramverk
ISO 22301:2019		Krav för ledningssystem för verksamhetskontinuitet
EU:s dataskyddsförordning (GDPR)	Artikel 32	
EU:s NIS2-direktiv	Artikel 21.2 f	
EU:s DORA-förordning	Artikel 10	
COBIT 2019	DSS04	

1. Syfte

1.1. Denna policy fastställer obligatoriska kontroller och ansvar för att säkerställa organisationens förmåga att upprätthålla eller återställa kritisk verksamhet och stödjande IKT-tjänster under och efter en störande incident.

1.2. Policyn syftar till att skydda liv, operativ stabilitet, rättsliga skyldigheter, kundåtaganden och organisationens anseende genom att bygga in resiliens genom proaktiv planering och validerad återställningsförmåga.

1.3. Denna policy utgör grunden för organisationens ramverk för verksamhetskontinuitet och katastrofåterställning och säkerställer efterlevnad av tillämpliga regulatoriska krav, avtalskrav och krav enligt vedertagen branschpraxis.

2. Omfattning

2.1. Denna policy gäller för alla organisatoriska enheter, organisationens informationssystem, verksamhetsprocesser, all personal och tredjepartstjänster som klassificeras som kritiska eller väsentliga utifrån resultatet av konsekvensanalys för verksamheten (Business Impact Analysis, BIA).

2.2. Policyn omfattar:

2.2.1. Naturliga och människoskapade störningar, inklusive cyberattacker, infrastrukturfel, datacenteravbrott, pandemier och avbrott i leverantörers tjänster

2.2.2. Planering, testning och kontinuerlig förbättring av verksamhetskontinuitetsplaner (BCP) och katastrofåterställningsplaner (DRP)

2.2.3. Roller och ansvar för insatser vid nödläge, återställningssamordning och incidenteskalering

2.3. All personal med ansvar för kontinuitet eller återställning, inklusive IT, verksamhetsägare, krisledare och leverantörer, omfattas av bestämmelserna i denna policy.

3. Mål

3.1. Att säkerställa kontinuitet i verksamhet och tjänster genom fördefinierade och testade rutiner, med minimerad operativ påverkan, anseendeskada och rättslig påverkan.

3.2. Att återställa IKT-tjänster inom fastställda återställningstidsmål (Recovery Time Objective, RTO) och återställningspunktsmål (Recovery Point Objective, RPO), i linje med verksamhetens risktolerans.

3.3. Att tydligt tilldela ägarskap för planering, genomförande och styrning av verksamhetskontinuitet och katastrofåterställning i hela organisationen.

3.4. Att säkerställa att kontinuitetsförmågor testas regelbundet, underhålls och förbättras utifrån realistiska scenarier och revisionsiakttagelser.

3.5. Att uppfylla krav på regelefterlevnad enligt ISO, NIST, GDPR, DORA och NIS2 samt stödja tillbörlig aktsamhet avseende operativ resiliens och tillgänglighet.

4. Roller och ansvar

4.1. Verkställande ledning

4.1.1. Godkänner policyn för verksamhetskontinuitet och katastrofåterställning och säkerställer strategisk anpassning.

4.1.2. Tilldelar budget och resurser för att stödja verksamhetskontinuitet, insatser vid nödläge och återställningsövningar.

4.2. Ansvarig för verksamhetskontinuitet

4.2.1. Ansvarar för utveckling och underhåll av organisationsövergripande kontinuitetsplaner samt samordning av kontinuitetstester.

4.2.2. Upprätthåller BIA-processen, samordnar utbildning och säkerställer att dokumentationen uppfyller krav på regelefterlevnad.

[... 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 årligen av ansvarig för verksamhetskontinuitet och informationssäkerhetschef (CISO) för att säkerställa anpassning till:

9.1.1. Förändringar i verksamheten, kritiska system eller infrastruktur

9.1.2. Erfarenheter från incidenter, revisioner, skrivbordsövningar eller DR-tester

9.1.3. Uppdaterade regulatoriska skyldigheter eller avtalskrav (t.ex. DORA, GDPR, kundkrav på RTO/RPO)

9.1.4. Förändringar i organisationens riskaptit eller kontinuitetsstrategi

9.2. Granskningar ska omfatta:

9.2.1. Validering av planernas relevans och kontaktuppgifter

9.2.2. Förnyad bedömning av RTO, RPO och återställningsnivåer

9.2.3. Utvärdering av kapacitet för säkerhetskopiering och DR-tjänster

9.2.4. Återkoppling från intressenter som nyligen har använt återställningsplaner eller deltagit i tester

9.3. Alla policyändringar ska:

9.3.1. Versionshanteras med dokumenterad motivering och godkännande från berörda intressenter

9.3.2. Kommuniceras till nyckelpersoner och team med uppdaterade ansvarsområden

9.3.3. Återspeglas i uppdaterad utbildning, informationsmaterial och operativa rutiner

9.4. Tillfälliga akuta uppdateringar ska utfärdas om en större organisatorisk förändring, ett rättsligt krav eller en kritisk iakttagelse medför att nuvarande planer eller policy inte längre är tillämpliga.

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med följande nyckeldokument:

10.1.1. P1 – Informationssäkerhetspolicy: Fastställer krav på riskbaserad och resilient verksamhet under alla förhållanden.

10.1.2. P5 – Policy för ändringshantering: Säkerställer att alla återställningsrelaterade konfigurations- eller infrastrukturändringar följer dokumenterade och godkända arbetsflöden.

10.1.3. P14 – Policy för datalagring och gallring: Reglerar livscykeln för säkerhetskopieringsmedier och återställda data som används i kontinuitetsarbetet.

10.1.4. P15 – Policy för säkerhetskopiering och återställning: Fastställer kontroller för frekvens, säkerhet och verifiering av återställning.

10.1.5. P18 – Policy för kryptografiska kontroller: Säkerställer att återställningsprocesser upprätthåller krav på kryptering och konfidentialitet.

10.1.6. P22 – Policy för loggning och övervakning: Stödjer detektering och eskalering av händelser som påverkar kontinuiteten.

10.1.7. P30 – Policy för incidenthantering: Definierar processer för begränsning, eskalering och rotorsaksanalys i linje med kontinuitetsutlösande händelser.

10.1.8. P33 – Policy för revision och övervakning av regelefterlevnad: Validerar riktighet och effektivitet i kontinuitets- och återställningspraxis i system och processer.

11. Referensstandarder och ramverk

11.1. Denna policy är anpassad till internationellt vedertagna standarder för verksamhetskontinuitet och katastrofåterställning och stödjer revisionsbarhet, resiliens och efterlevnad av rättsliga krav.

11.2. ISO/IEC 27002

11.2.1. Bilaga A, kontroll 5.29 – Informationssäkerhet under störningar: Kräver kontinuitet i säkerhetskontroller under ogynnsamma förhållanden.

11.2.2. Bilaga A, kontroll 5.30 – IKT-beredskap för verksamhetskontinuitet: Kräver förberedelse, testning och validering av IKT-förmåga för återställning.

11.3. ISO 22301:2019 – Ledningssystem för verksamhetskontinuitet

11.3.1. Tillhandahåller ramverket för att etablera, genomföra och upprätthålla verksamhetskontinuitetspraxis i linje med organisationens mål och risktolerans.

11.4. NIST SP 800-34 Rev.1 – Vägledning för beredskapsplanering

11.4.1. Beskriver vedertagen branschpraxis för beredskapsplaner för IT-system, inklusive utveckling av kontinuitetsstrategi, konsekvensanalys och testning av planer.

11.5. EU:s dataskyddsförordning (GDPR) (2016/679)

11.5.1. Artikel 32 – Säkerhet i samband med behandling: Kräver resiliens i system för behandling samt snabb återställning av tillgänglighet till och åtkomst till personuppgifter efter en incident.

11.6. EU:s NIS2-direktiv (2022/2555)

11.6.1. Artikel 21.2 f: Kräver åtgärder för verksamhetskontinuitet och krishantering för att stödja säkerheten i nätverks- och informationssystem.

11.7. EU:s DORA-förordning (2022/2554)

11.7.1. Artikel 10 – IKT-verksamhetskontinuitet: Kräver att finansiella entiteter utvecklar och testar IKT-kontinuitetsplaner, inklusive riskbaserade RTO/RPO och failover-förmågor.

11.8. COBIT 2019

11.8.1. DSS04 – Hantera kontinuitet: Omfattar alla aspekter av kontinuitetsplanering, inklusive hotidentifiering, konsekvensanalys, återställningsstrategi och regelbunden testning.