					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P32S					Dokumenttitel: **Politik for forretningskontinuitet og katastrofeberedskab**						
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/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontrol 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
GDPR	Artikel 32, 33	
NIS2-direktivet	Artikel 21(2)(f)	
DORA-forordningen	Artikel 10	
COBIT 2019	DSS04	

1. Formål

1.1 Denne politik sikrer, at organisationen kan opretholde forretningsdriften og genetablere kritiske IT-tjenester under og efter forstyrrende hændelser såsom strømafbrydelser, cyberangreb, ransomwareangreb eller systemsvigt.

1.2 Den fastlægger en klar ramme for forretningskontinuitet og katastrofeberedskab (BC/DR), tilpasset SMV'er uden dedikerede IT-teams.

1.3 Denne politik hjælper organisationen med at opfylde gældende krav efter ISO/IEC 27001:2022, GDPR, NIS2, DORA og COBIT 2019 samt styrke den operationelle robusthed og kundernes tillid.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle forretningskritiske systemer og tjenester (f.eks. e-mail, cloudlagring, faktureringsplatforme, kunderegistre)

2.1.2 Alle medarbejdere og eksterne IT-tjenesteudbydere med ansvar for BC/DR-beredskab og gennemførelse

2.1.3 Alle typer forstyrrelser, herunder cyberhændelser, hardwarefejl, strømsvigt, oversvømmelse og manglende adgang til kontoret

2.2 Den omfatter:

2.2.1 backupstyring

2.2.2 planlægning af forretningskontinuitet (BCP)

2.2.3 aktiviteter for katastrofeberedskab

2.2.4 træning og test af medarbejdere

2.2.5 juridiske og regulatoriske responsprocedurer

3. Mål

3.1 Beskytte organisationens evne til at levere centrale tjenester trods uplanlagte forstyrrelser.

3.2 Sikre rettidig genetablering af systemer og data i overensstemmelse med fastlagte Recovery Time Objectives (RTO'er).

3.3 Sætte alle medarbejdere i stand til at følge kontinuitetsprocedurer under kriser med mindst mulig usikkerhed.

3.4 Opretholde efterlevelse af lovkrav om databeskyttelse og operationel robusthed, herunder GDPR artikel 32 og NIS2 artikel 21.

3.5 Etablere en praktisk og testbar strategi for kontinuitet og genetablering, der er egnet til SMV'er.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Ejer BC/DR-processen og denne politik

4.1.2 Godkender Business Continuity Plan (BCP)

4.1.3 Koordinerer hændelseshåndtering og intern kommunikation under forstyrrelser

4.1.4 Foretager regulatoriske anmeldelser efter behov (f.eks. anmeldelser efter GDPR ved brud på persondatasikkerheden)

4.2 IT-leverandør/systemadministrator

4.2.1 Vedligeholder og tester sikkerhedskopier

4.2.2 Gennemfører procedurer for katastrofeberedskab, når de aktiveres

4.2.3 Dokumenterer alle genetableringshandlinger og hændelser i forbindelse med systemgendannelse

4.2.4 Rapporterer kritiske IT-hændelser til direktøren straks

[... 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 Årlig gennemgang af politik og plan

9.1.1 Direktør (GM) skal sikre, at denne politik og den tilknyttede Business Continuity Plan (BCP) formelt gennemgås mindst én gang om året.

9.1.2 Gennemgangen skal omfatte:

9.1.2.1 evaluering af nye eller fremspirende risici

9.1.2.2 fornyet validering af RTO'er/RPO'er

9.1.2.3 verifikation af leverandør- og kontaktoplysninger

9.1.2.4 tilpasning til ændringer i IT-systemer, juridiske forpligtelser eller drift

9.2 Opdateringer udløst af hændelser

9.2.1 Denne politik skal også opdateres som reaktion på:

9.2.1.1 større hændelser eller forstyrrelser, særligt hvis målene ikke blev opfyldt

9.2.1.2 nye juridiske eller regulatoriske forpligtelser (f.eks. ændringer i DORA)

9.2.1.3 ændringer i kritiske systemer, cloudplatforme eller personale

9.2.1.4 konstateringer fra årlige BCP/DR-tests

9.3 Proces for ændringsstyring

9.3.1 Alle ændringer skal godkendes af GM

9.3.2 Der skal føres en versionshistorik med dato, beskrivelse af ændringen og godkender

9.3.3 Den opdaterede politik skal redistribueres til alt relevant personale, herunder IT-leverandøren og afdelingsledere

9.4 Dokumentation af erfaringer

9.4.1 Efter test eller reelle driftsforstyrrelser skal dokumenterede erfaringer indgå i fremtidige revisioner

9.4.2 Disse gennemgange skal også omfatte vurderinger af leverandørers performance og kontrol af, om responsen var tilstrækkelig

10. Relaterede politikker og sammenhænge

10.1 Denne politik er tæt integreret med følgende SME-politikker:

10.1.1 P1S – Informationssikkerhedspolitik: Definerer de overordnede sikkerhedsmål, som praksis for kontinuitet og genetablering skal understøtte.

10.1.2 P4S – Politik for adgangskontrol: Muliggør nødmæssig tilbagekaldelse eller genetablering af brugeradgang under scenarier med driftsforstyrrelser.

10.1.3 P6S – Politik for risikostyring: Danner grundlag for at identificere, evaluere og prioritere risici relateret til kontinuitet.

10.1.4 P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Sikrer, at medarbejdere er forberedte på at handle under forstyrrelser og forstår BCP.

10.1.5 P15S – Politik for backup og gendannelse: Indeholder specifikke tekniske procedurer til at beskytte datatilgængelighed og gendannelse.

10.1.6 P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at planlægning af kontinuitet respekterer beskyttelsen af personoplysninger og overholder GDPR under og efter hændelser.

10.1.7 P22S – Politik for logning og overvågning: Understøtter detektion af hændelser, der kan aktivere BC/DR-processer, og giver forensiske revisionsspor efter forstyrrelser.

10.1.8 P30S – Politik for hændelseshåndtering: Går direkte forud for aktivering af genetableringsprocessen ved cyberhændelser eller driftsmæssige hændelser.

10.1.9 P31S – Politik for bevissikring og it-forensik: Sikrer, at digitale beviser indsamles under kontinuitetsscenarier af hensyn til efterlevelse, forsikring eller undersøgelse.

10.2 Disse politikker udgør tilsammen en sammenhængende og revisionsklar ramme for robusthed, ansvarlighed og kontinuitet i kontroller på tværs af alle SME-aktiviteter.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:

11.1.1 Klausul 6.1 – Kræver risikobaseret planlægning og behandling, herunder forretningskontinuitet og genetablering.

11.1.2 Klausul 6.3 – Fremhæver løbende forbedring efter forstyrrelser.

11.1.3 Klausul 8.1 – Kræver operationelle kontroller, herunder dokumenterede kontinuitetsforanstaltninger.

11.2 ISO/IEC 27002:

11.2.1 Kontrol 5.29 – Kræver etablering og vedligeholdelse af ordninger for forretningskontinuitet.

11.2.2 Kontrol 5.30 – Kræver test og gennemgang af disse ordninger.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Definerer krav til beredskabsplanlægning.

11.3.2 CP-4 – Kræver træning i beredskabsplaner for organisationens personale.

11.3.3 CP-6 – Omfatter krav til alternativ opbevaringslokation.

11.3.4 CP-7 – Omfatter krav til alternativ behandlingslokation.

11.4 GDPR:

11.4.1 Artikel 32 – Kræver foranstaltninger, der sikrer den løbende tilgængelighed og robusthed af behandlingssystemer og -tjenester.

11.4.2 Artikel 33 – Udløser forpligtelser til anmeldelse af brud på persondatasikkerheden, hvor svigt i kontinuitet medfører kompromittering af personoplysninger.

11.5 NIS2-direktivet (2022/2555):

11.5.1 Artikel 21(2)(f) – Kræver planlægning af kontinuitet og kapaciteter til krisestyring som forudsætning for beredskab over for cyberrisici.

11.6 DORA-forordningen (2022/2554):

11.6.1 Artikel 10 – Kræver implementering af test af digital operationel robusthed og genetableringskapaciteter, særligt for SMV'er i den finansielle sektor.

11.7 COBIT 2019:

11.7.1 DSS04 – Manage Continuity: Giver vejledning i virksomhedsrettet styring til at opretholde og validere operationel robusthed, herunder ejerskab, test, leverandørintegration og gennemgange efter hændelser.