					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P32					Dokumenttitel: **Politik for forretningskontinuitet og genopretning efter hændelser**						
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**

Juridisk meddelelse (ophavsret og brugsbegrænsninger)

(C) 2025 Clarysec LLC. All rights reserved.

Dette dokument er Clarysec LLC's intellektuelle ejendom. Ingen del af dette dokument må kopieres, genbruges, distribueres eller ændres til kommercielle eller implementeringsmæssige formål uden udtrykkelig skriftlig tilladelse.
Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.
For licensiering kontakt: info@clarysec.com

Tilpasset relevante standarder og regler

Standard/regulering	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 til CP-11	
NIST SP 800-34 Rev.1	Beredskabsplanlægning	Rammeværk
ISO 22301:2019		Krav til ledelsessystem for forretningskontinuitet
EU GDPR	Artikel 32	
EU NIS2	Artikel 21(2)(f)	
EU DORA	Artikel 10	
COBIT 2019	DSS04	

1. Formål

1.1. Denne politik fastlægger obligatoriske kontroller og ansvarsområder for at sikre organisationens evne til at opretholde eller genoprette kritiske forretningsaktiviteter og understøttende IKT-tjenester under og efter en forstyrrende hændelse.

1.2. Formålet er at beskytte liv, driftsstabilitet, juridiske forpligtelser, kundeforpligtelser og organisationens omdømme ved at indarbejde robusthed gennem proaktiv planlægning og validerede genopretningskapabiliteter.

1.3. Denne politik udgør grundlaget for organisationens styringsramme for forretningskontinuitet og genopretning efter hændelser og sikrer overholdelse af gældende regulatoriske, kontraktlige og brancherelaterede krav.

2. Omfang

2.1. Denne politik gælder for alle organisatoriske enheder, informationssystemer, forretningsprocesser, medarbejdere og tredjepartstjenester, der klassificeres som kritiske eller væsentlige på baggrund af resultaterne af forretningskonsekvensanalyser.

2.2. Politikken omfatter:

2.2.1. Naturlige og menneskeskabte forstyrrelser, herunder cyberangreb, infrastruktursvigt, datacenterudfald, pandemier og afbrydelser i leverandørers tjenesteleverance

2.2.2. Planlægning, test og løbende forbedring af planer for forretningskontinuitet (BCP'er) og planer for genopretning efter hændelser (DRP'er)

2.2.3. Roller og ansvar for nødberedskab, koordinering af genopretning og eskalering af hændelser

2.3. Alle medarbejdere med ansvar for kontinuitet eller genopretning, herunder IT, procesejere, kriseansvarlige og leverandører, er omfattet af bestemmelserne i denne politik.

3. Mål

3.1. At sikre kontinuitet i forretningsaktiviteter og tjenester gennem foruddefinerede og testede procedurer, så driftsmæssige, omdømmemæssige og juridiske konsekvenser minimeres.

3.2. At genoprette IKT-tjenester inden for definerede Recovery Time Objectives (RTO'er) og Recovery Point Objectives (RPO'er), afstemt med forretningens risikotolerance.

3.3. At placere ejerskab for planlægning, gennemførelse og styring af forretningskontinuitet og genopretning efter hændelser på tværs af organisationen.

3.4. At sikre, at kontinuitetskapabiliteter regelmæssigt testes, vedligeholdes og forbedres på baggrund af realistiske scenarier og revisionskonstateringer.

3.5. At opfylde krav til efterlevelse af ISO, NIST, GDPR, DORA og NIS2 og understøtte rettidig omhu i relation til operationel robusthed og tilgængelighed.

4. Roller og ansvar

4.1. Direktionen

4.1.1. Godkender politikken for forretningskontinuitet og genopretning efter hændelser og sikrer strategisk sammenhæng.

4.1.2. Allokerer budget og ressourcer til understøttelse af forretningskontinuitet, nødberedskab og genopretningsøvelser.

4.2. Ansvarlig for forretningskontinuitet

4.2.1. Er ansvarlig for udvikling og vedligeholdelse af organisationsdækkende BCP'er samt koordinering af kontinuitetstest.

4.2.2. Vedligeholder tidsplanen for forretningskonsekvensanalyser, faciliterer træning og sikrer, at dokumentationen opfylder compliancekrav.

[... 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. Denne politik skal gennemgås årligt af den ansvarlige for forretningskontinuitet og CISO for at sikre overensstemmelse med:

9.1.1. Ændringer i forretningsdrift, kritiske systemer eller infrastruktur

9.1.2. Erfaringer fra hændelser, revisioner, tabletop-øvelser eller DR-test

9.1.3. Opdaterede regulatoriske eller kontraktlige forpligtelser (f.eks. DORA, GDPR, kundekrav til RTO/RPO)

9.1.4. Ændringer i organisationens risikovillighed eller strategi for forretningskontinuitet

9.2. Gennemgange skal omfatte:

9.2.1. Validering af planernes relevans og kontaktoplysninger

9.2.2. Fornyet vurdering af RTO'er, RPO'er og genopretningsniveauer

9.2.3. Evaluering af kapaciteten i backup- og DR-tjenester

9.2.4. Feedback fra interessenter, der har gennemført nylige genopretningsplaner eller test

9.3. Alle ændringer i politikken skal:

9.3.1. Være underlagt versionsstyring med dokumenteret begrundelse og godkendelse fra interessenter

9.3.2. Kommunikeres til nøglemedarbejdere og teams med opdaterede ansvarsområder

9.3.3. Afspejles i opdateret træning, awareness-materiale og driftsprocedurer

9.4. Midlertidige nødopdateringer skal udstedes, hvis der forekommer en større organisatorisk ændring, et retligt krav eller en kritisk konstatering, som gør gældende planer eller politikken uanvendelige.

10. Relaterede politikker og sammenhænge

10.1. Denne politik anvendes i sammenhæng med følgende nøgledokumenter:

10.1.1. P1 – Informationssikkerhedspolitik: Fastlægger kravet om risikobaseret og robust drift under alle forhold.

10.1.2. P5 – Politik for ændringsstyring: Sikrer, at enhver genopretningsrelateret ændring af konfiguration eller infrastruktur følger dokumenterede og godkendte workflows.

10.1.3. P14 – Politik for opbevaring og bortskaffelse af data: Regulerer livscyklusstyring af backupmedier og gendannede data, der anvendes i kontinuitetsaktiviteter.

10.1.4. P15 – Politik for backup og gendannelse: Håndhæver kontroller for backupfrekvens, sikkerhed og verifikation af gendannelse.

10.1.5. P18 – Politik for kryptografiske kontroller: Sikrer, at genopretningsprocesser opretholder standarder for kryptering og fortrolighed.

10.1.6. P22 – Politik for logning og overvågning: Understøtter detektion og eskalering af hændelser, der påvirker forretningskontinuiteten.

10.1.7. P30 – Politik for hændelseshåndtering: Definerer processer for inddæmning, eskalering og rodårsagsanalyse i overensstemmelse med udløsende forhold for kontinuitet.

10.1.8. P33 – Politik for revisions- og complianceovervågning: Validerer integriteten og effektiviteten af praksis for forretningskontinuitet og genopretning på tværs af systemer og processer.

11. Referencestandarder og rammeværker

11.1. Denne politik er tilpasset internationalt anerkendte standarder for forretningskontinuitet og genopretning efter hændelser og understøtter revisionssporbarhed, robusthed og juridisk efterlevelse.

11.2. ISO/IEC 27002

11.2.1. Bilag A, kontrol 5.29 – Informationssikkerhed under forstyrrelser: Kræver kontinuitet i sikkerhedskontroller under ugunstige forhold.

11.2.2. Bilag A, kontrol 5.30 – IKT-beredskab for forretningskontinuitet: Kræver forberedelse, test og validering af IKT-kapabiliteter til genopretning.

11.3. ISO 22301:2019 – Ledelsessystemer for forretningskontinuitet

11.3.1. Indeholder rammerne for at etablere, implementere og vedligeholde praksis for forretningskontinuitet, som er afstemt med organisatoriske mål og risikotærskler.

11.4. NIST SP 800-34 Rev.1 – Vejledning i beredskabsplanlægning

11.4.1. Beskriver bedste praksis for beredskabsplaner for IT-systemer, herunder udvikling af kontinuitetsstrategi, konsekvensanalyse og test af planer.

11.5. EU GDPR (2016/679)

11.5.1. Artikel 32 – Behandlingssikkerhed: Kræver robusthed i behandlingssystemer samt rettidig gendannelse af tilgængelighed og adgang til personoplysninger efter en hændelse.

11.6. EU NIS2-direktivet (2022/2555)

11.6.1. Artikel 21(2)(f): Kræver foranstaltninger for forretningskontinuitet og krisestyring til understøttelse af sikkerheden i netværks- og informationssystemer.

11.7. EU DORA (2022/2554)

11.7.1. Artikel 10 – IKT-forretningskontinuitet: Kræver, at finansielle enheder udvikler og tester IKT-kontinuitetsplaner, herunder risikobaserede RTO/RPO'er og failover-kapacitet.

11.8. COBIT 2019

11.8.1. DSS04 – Styring af kontinuitet: Omfatter alle aspekter af kontinuitetsplanlægning, herunder identifikation af trusler, konsekvensanalyse, genopretningsstrategi og regelmæssig test.