					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P05S					Dokumenttitel: **Politik for ændringsstyring**							
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 reguleringer

Standard/regulering	Punkt/artikel	Bemærkning
ISO/IEC 27001:2022	Punkt 6.1, 8	
ISO/IEC 27002:2022	Kontrol 8	
NIST SP 800-53 Rev. 5	CM-2 til CM-5, CM-11	
EU NIS2	Artikel 21(2)(b)	
EU DORA	Artikel 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS01	

1. Formål

1.1 Denne politik sikrer, at alle ændringer i IT-systemer, konfigurationer, forretningsapplikationer og cloudtjenester planlægges, risikovurderes, testes og godkendes før implementering.

1.2 Formålet er at reducere driftsforstyrrelser, sikkerhedsrisici og serviceafbrydelser ved at etablere en enkel, men konsekvent proces, der også er anvendelig for mindre virksomheder med begrænsede ressourcer.

1.3 Denne politik understøtter certificering efter ISO/IEC 27001:2022 ved at formalisere, hvordan tekniske og driftsmæssige ændringer styres og dokumenteres.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Medarbejdere og afdelingsledere, der foreslår eller gennemfører ændringer

2.1.2 Eksterne IT-tjenesteudbydere, der administrerer systemer eller software

2.1.3 Direktøren, som har det overordnede ansvar for godkendelse af ændringer

2.2 Politikken omfatter ændringer i:

2.2.1 Software (opdateringer, patches, nye applikationer)

2.2.2 Hardware (udskiftninger, opgraderinger)

2.2.3 Netværks- og firewallkonfigurationer

2.2.4 Cloudtjenester, brugeradgangsrettigheder og leverandørintegrationer

2.2.5 Kritiske ændringer i forretningsprocesser, der involverer informationssystemer

2.3 Både planlagte ændringer og nødændringer er omfattet af denne politik.

3. Mål

3.1 Sikre, at alle ændringer i IT- og forretningssystemer er godkendt, dokumenteret og kan tilbagerulles, hvis der opstår problemer.

3.2 Forebygge ikke-planlagt nedetid, datatab og sikkerhedshændelser forårsaget af ukontrollerede ændringer.

3.3 Fastlægge enkle og gentagelige procedurer for indsendelse, godkendelse, test og tilbagerulning af ændringer.

3.4 Opretholde en revisionsbar ændringslog, der understøtter driftsmæssig ansvarlighed og efterlevelse af gældende krav.

3.5 Muliggøre risikobaserede beslutninger ved væsentlige eller følsomme ændringer.

4. Roller og ansvar

4.1 Direktør

4.1.1 Har det endelige ansvar for alle større ændringer.

4.1.2 Gennemgår og godkender ikke-rutinemæssige, kritiske eller højrisikoændringer.

4.1.3 Gennemgår ændringsloggen kvartalsvist eller efter væsentlige hændelser.

4.2 IT-support eller ekstern IT-leverandør

4.2.1 Gennemfører ændringer, herunder konfigurationsopdateringer, patching og systemmigreringer.

4.2.2 Vedligeholder en grundlæggende ændringslog med registrering af datoer, ændringstyper, resultater og godkendere.

4.2.3 Tester ændringer før implementering og gennemfører tilbagerulning efter behov.

4.2.4 Informerer berørte brugere før og efter større ændringer.

[... 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

9.1.1 Denne politik skal gennemgås årligt af direktøren eller den udpegede IT-kontakt for at sikre overensstemmelse med aktuelle systemer, arbejdsgange og regulatoriske krav.

9.2 Ekstraordinære gennemgange

9.2.1 Gennemgang skal også iværksættes ved:

9.2.1.1 Sikkerhedshændelser forårsaget af utilstrækkelig håndtering af ændringer

9.2.1.2 Indførelse af nye IT-systemer

9.2.1.3 Ændringer i relevante standarder såsom ISO, NIS2 eller DORA

9.3 Dokumentation af opdateringer

9.3.1 Ændringer i denne politik skal versionsstyres og godkendes af direktøren. Hver version skal angive dato, resumé af ændringer og godkender.

9.4 Kommunikation af politikken

9.4.1 Eventuelle opdateringer skal kommunikeres til alle berørte medarbejdere og eksterne leverandører. Dokumentationen skal opdateres alle relevante steder (f.eks. medarbejderportal, fællesdrev).

10. Relaterede politikker og sammenhænge

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

10.1.1 P2S – Politik for styringsroller og ansvarsfordeling: Definerer godkendelseskompetence for ændringer.

10.1.2 P4S – Politik for adgangskontrol: Sikrer, at adgangsændringer som følge af ændringer dokumenteres og implementeres korrekt.

10.1.3 P7S – Politik for onboarding og fratrædelse: Koordinerer ændringer relateret til rolleskift og tildeling af adgang.

10.1.4 P15S – Politik for backup og gendannelse: Sikrer, at tilbagerulning og genopretning kan gennemføres, hvis en ændring mislykkes.

10.1.5 P30S – Politik for hændelseshåndtering: Regulerer, hvordan mislykkede eller uautoriserede ændringer behandles som sikkerhedshændelser.

11. Referencestandarder og styringsrammer

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – Risikobaseret planlægning skal omfatte ændringsaktiviteter.

11.1.2 Punkt 8.1 – Driftsmæssige kontroller skal anvendes konsekvent på ændringsrelaterede aktiviteter for at sikre tjenesternes integritet.

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.32 – Giver vejledning om sikre processer for ændringsstyring, herunder dokumentation, test og godkendelse.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Basiskonfiguration for systemer før ændring.

11.3.2 CM-3 – Styring af konfigurationsændringer.

11.3.3 CM-4 – Analyse af sikkerhedsmæssig påvirkning.

11.3.4 CM-5 – Godkendelse og dokumentation af ændringer.

11.3.5 CM-11 – Revision og overvågning af ændringer.

11.4 EU NIS2-direktivet

11.4.1 Artikel 21(2)(b) – Kræver formelle procedurer for tekniske og organisatoriske sikkerhedsforanstaltninger, herunder ændringsstyring.

11.5 EU DORA

11.5.1 Artikel 6(9) og 8(4)(b) – Kræver, at finansielle enheder opretholder styring af ændringer og konfigurationer for IKT-systemer.

11.6 COBIT 2019

11.6.1 BAI06 – Manage Changes: Fremhæver planlægning, risikovurdering og mulighed for tilbagerulning.

11.6.2 DSS01 – Manage Operations: Sikrer driftsmæssig integritet under tekniske overgange og ændringer.