					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P05					Dokumenttitel: **Ændringsstyringspolitik**							
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	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 5.15	Omhandler risikobehandling, adgangskontrol og ændringsstyring
ISO/IEC 27002:2022	Kontrol 8	Implementerer en struktureret proces for ændringsstyring
NIST SP 800-53 Rev.5	CM-2 til CM-14	Kontroller for konfigurationsstyring
EU GDPR	Artikel 32(1)(b–d), 25; betragtning 78	Tekniske og organisatoriske foranstaltninger til system- og datasikkerhed ved ændringer
EU NIS2	Artikel 21(2)(a, b, d, e)	Krav til risikostyring af IKT-ændringer
EU DORA	Artikel 5, 8, 12	Regulerer operationel og IKT-risiko samt hændelsesrapportering
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Struktureret IT-ændringsstyring, performance, efterlevelse og kravstyring

1. Formål

1.1. Denne politik fastlægger en formel ramme for initiering, vurdering, godkendelse, implementering og gennemgang af ændringer i organisationens informationssystemer, infrastruktur, applikationer og relaterede processer.

1.2. Den sikrer, at alle ændringer gennemføres på en kontrolleret og revisionsbar måde, som minimerer risikoen for driftsforstyrrelser, sikkerhedskompromittering eller manglende efterlevelse af regulatoriske krav.

1.3. Den understøtter ISO/IEC 27001:2022, bilag A, kontrol 8.32 ved at håndhæve sikre, dokumenterede og risikotilpassede praksisser for ændringsstyring.

1.4. Politikken sikrer desuden sporbarhed i ændringsbeslutninger og fremmer operationel robusthed ved planlagte ændringer og nødændringer.

2. Omfang

2.1. Denne politik gælder for alle ændringer, der påvirker systemer, data og miljøer inden for ISMS-omfanget, herunder:

2.1.1. IT-infrastruktur (on-premises, cloud, hybrid)

2.1.2. Produktions-, præproduktions- og disaster recovery-miljøer

2.1.3. Forretningsapplikationer, tjenester, API'er og integrationer

2.1.4. Konfigurationsindstillinger, patching, softwareudgivelser og systemmigreringer

2.1.5. Nødrettelser samt projektbaserede eller planlagte ændringer

2.2. Den omfatter ændringer initieret af:

2.2.1. Interne medarbejdere (IT-drift, udviklere, systemejere)

2.2.2. Eksterne leverandører, managed service providers (MSP'er) og kontraktansatte

2.2.3. Projektteams i forbindelse med systemimplementeringer, opgraderinger eller serviceovergange

2.3. Denne politik gælder ikke for:

2.3.1. Midlertidige test- og udviklingsmiljøer uden adgang til produktionsdata

2.3.2. Personlige brugerkonfigurationer (omfattet af politikken for acceptabel brug (AUP))

2.3.3. Ændringer i systemer uden for organisationens kontrolafgrænsning, medmindre de påvirker integrerede aktiver eller efterlevelsesforpligtelser

3. Målsætninger

3.1. At sikre, at alle ændringer gennemgås, godkendes, testes og dokumenteres før gennemførelse.

3.2. At opretholde systemtilgængelighed, dataintegritet og servicekontinuitet under og efter ændringsaktiviteter.

3.3. At kræve definerede ændringsklassifikationer, tilbagerulningsplaner og risikovurderinger for alle ændringstyper.

3.4. At muliggøre transparent beslutningstagning og eskalering gennem struktureret styring.

3.5. At understøtte revisionsberedskab gennem sporbare ændringsregistreringer og gennemgang efter implementering.

3.6. At håndhæve funktionsadskillelse og reducere risikoen for uautoriserede eller modstridende ændringer i kritiske systemer.

4. Roller og ansvar

4.1. Direktion

4.1.1. Godkender P05 Ændringsstyringspolitik og sikrer overensstemmelse med strategiske mål og regulatoriske forpligtelser.

4.1.2. Godkender ændringsprogrammer med høj påvirkning eller tværgående karakter som led i det styringsmæssige tilsyn.

4.1.3. Tildeler nødvendige ressourcer og budget til værktøjer til ændringskontrol og uddannelse af personale.

4.2. Change Advisory Board (CAB)

4.2.1. Gennemgår og godkender standardændringer og større ændringer samt sikrer passende vurdering af risiko, påvirkning og afhængigheder.

4.2.2. Validerer tilbagerulningsplaner, testresultater, interessentkommunikation og planlægning.

4.2.3. Består af systemejere, informationssikkerhed, IT-drift, forretningsansvarlige og repræsentanter for compliance.

4.2.4. Kan delegere beslutninger for ændringer med lav risiko eller nødændringer under dokumenterede betingelser.

[... 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. Udløsende faktorer for gennemgang og hyppighed

9.1.1. Denne politik skal gennemgås årligt eller ved:

9.1.1.1. Større ændringer i IT eller infrastruktur

9.1.1.2. Væsentlige hændelser relateret til mislykkede eller uautoriserede ændringer

9.1.1.3. Regulatoriske opdateringer eller nye juridiske forpligtelser relateret til ændringer

9.1.1.4. Implementering af nye værktøjer eller CMS-platforme

9.2. Proces for gennemgang af ændringsstyringspolitikken

9.2.1. Den ændringsansvarlige leder gennemgangsprocessen i samarbejde med:

9.2.1.1. IT, informationssikkerhed og drift

9.2.1.2. Intern revision og risiko

9.2.1.3. CAB-repræsentanter

9.2.2. Opdateringer skal gennemgås og godkendes af direktionen og informationssikkerhedsstyregruppen (ISSC).

9.2.3. Genudstedte versioner skal registreres i dokumentregistret og kommunikeres til berørte parter med fornyet bekræftelse efter behov.

9.3. Dokumentstyring og versionsstyring

9.3.1. Alle versioner skal indeholde:

9.3.1.1. Politik-id, titel og klassifikationsniveau

9.3.1.2. Ejer og revisionshistorik

9.3.1.3. Ændringslog og ikrafttrædelsesdato

9.3.1.4. Godkendelsesmyndighed

9.3.2. Arkiverede versioner skal opbevares i overensstemmelse med politikken for dokumentopbevaring (minimum 3 år).

10. Relaterede politikker og sammenhænge

10.1. Denne politik er direkte forbundet med og understøtter håndhævelsen af:

10.1.1. P1 – Informationssikkerhedspolitik: Fastlægger kravet om formelle sikkerhedskontroller og ansvarlighed på procesniveau, herunder styring af ændringer.

10.1.2. P2 – Politik for roller og ansvar i styring: Definerer godkendelsesmyndighed og funktionsadskillelse, som er relevant for autorisation og tilsyn med ændringer.

10.1.3. P4 – Politik for adgangskontrol: Sikrer, at adgangsrettigheder for personer, der implementerer og gennemgår ændringer, følger princippet om mindst privilegium.

10.1.4. P6 – Politik for risikostyring: Sikrer, at alle ændringer er underlagt passende risikovurdering og afbødningsstrategier.

10.1.5. P33 – Politik for revisions- og complianceovervågning: Regulerer validering og revisionsmæssig gennemgang af registreringer og overtrædelser vedrørende ændringsstyring.

10.2. Disse politikker muliggør samlet en juridisk forsvarlig, sporbar og sikker livscyklus for ændringsstyring inden for ISMS-rammen.

11. Referencestandarder og rammeværk

11.1. ISO/IEC 27001:2022

11.1.1. Klausul 6.1 – Tiltag til håndtering af risici og muligheder: Denne politik understøtter identifikation, evaluering og kontrol af risici relateret til ændringer.

11.1.2. Klausul 5.15 – Adgangskontrol: Sikrer, at adgang i forbindelse med ændringer er kontrolleret og sporbar.

11.1.3. Bilag A, kontrol 8.32 – Ændringsstyring: Denne politik implementerer fuldt ud kravet om at styre ændringer i faciliteter og informationsbehandlingssystemer på en planlagt og kontrolleret måde.

11.2. ISO/IEC 27002:2022 – Kontrol 8

11.2.1. Understøtter implementeringen af en struktureret proces for ændringsstyring, herunder ændringsklassifikation, godkendelse, test, tilbagerulning og dokumentation.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM-familien (CM-1 til CM-14): Denne politik er tæt afstemt med kontroller for konfigurationsstyring, herunder baselinekonfigurationer (CM-2), kontrol af konfigurationsændringer (CM-3), analyse af sikkerhedspåvirkning (CM-4) og adgangsbegrænsninger (CM-5).

11.3.2. AU-familien (AU-2, AU-6, AU-12): De lognings- og revisionsmekanismer, der er beskrevet i denne politik, understøtter hændelsessporbarhed og efterlevelsesgennemgang for ændringsrelaterede aktiviteter.

11.3.3. RA-3, RA-5: Risikovurderinger og sårbarhedsscanninger udløst af ændringer er indlejret i ændringsevalueringsprocessen.

11.3.4. PM-11 (Definition af mission/forretningsproces): Sikrer, at forretningskontinuitet og operationelle målsætninger bevares under ændringer.

11.4. EU GDPR (2016/679)

11.4.1. Artikel 32(1)(b–d): Denne politik understøtter kravet om passende tekniske og organisatoriske foranstaltninger til sikring af datasikkerhed, særligt under systemændringer.

11.4.2. Artikel 25 – Databeskyttelse gennem design og standardindstillinger: Sikrer, at ændringer, der påvirker personoplysninger, integrerer databeskyttelse og sikkerhed i design og udrulning.

11.4.3. Betragtning 78: Kræver, at dataansvarlige implementerer mekanismer, såsom politikker for ændringskontrol, for at sikre løbende fortrolighed, integritet og robusthed i behandlingssystemer.

11.5. EU NIS2-direktivet (2022/2555)

11.5.1. Artikel 21(2)(a, b, d, e): Fastsætter krav om tekniske og organisatoriske foranstaltninger til håndtering af IKT-risici, herunder risici, der opstår ved systemændringer, softwareopdateringer og ændringer i infrastrukturen.

11.6. EU DORA (2022/2554)

11.6.1. Artikel 5 – Styrings- og intern kontrolramme: Denne politik håndhæver principper for operationel risikostyring knyttet til IKT-ændringer og opdateringer.

11.6.2. Artikel 8 – Ramme for IKT-risikostyring: Kræver, at finansielle enheder styrer alle ændringer, som påvirker IKT-systemer, under strukturerede ændringsstyringsprocesser, hvilket afspejles i denne politiks krav til klassifikation, test, tilbagerulning og dokumentation.

11.6.3. Artikel 12 – Hændelsesrapportering: Sikrer, at mislykkede ændringer, der medfører IKT-forstyrrelser, er sporbare, dokumenterede og rapporteres, hvor det er relevant.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: Denne politik opfylder direkte målsætningerne i BAI06 ved at etablere strukturerede workflows for ændringsgodkendelse, påvirkningsvurdering, kommunikation og test.

11.7.2. BAI02 – Managed Requirements Definition og BAI03 – Managed Solutions Identification and Build: Sikrer, at forretningsdrevne ændringer gennemgås og implementeres sikkert.

11.7.3. DSS01 – Managed Operations: Understøtter løbende systemintegritet under gennemførelse af ændringer.

11.7.4. MEA01 og MEA03 – Overvågning, evaluering og vurdering af performance og efterlevelse: Muliggør løbende tilsyn med effektiviteten af ændringsstyringspolitikken og dens håndhævelse.