					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P05					Dokumenttitel: **Ändringshanteringspolicy**							
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**

I linje med standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 5	Omfattar riskbehandling, åtkomstkontroll och ändringshantering
ISO/IEC 27002:2022	Kontroll 8	Etablerar en strukturerad process för ändringshantering
NIST SP 800-53 Rev.5	CM-2 till CM-14	Kontroller för konfigurationshantering
EU:s dataskyddsförordning (GDPR)	Artikel 32(1)(b–d), 25; skäl 78	Tekniska och organisatoriska åtgärder för system- och datasäkerhet vid ändringar
EU:s NIS2-direktiv	Artikel 21(2)(a, b, d, e)	Ställer krav på riskhantering av IKT-ändringar
EU:s DORA-förordning	Artikel 5, 8, 12	Reglerar operativ risk, IKT-risk och incidentrapportering
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA	Strukturerad hantering av IT-ändringar avseende prestanda, regelefterlevnad och krav

1. Syfte

1.1. Denna policy fastställer ett formellt ramverk för att initiera, bedöma, godkänna, genomföra och granska ändringar i organisationens informationssystem, infrastruktur, applikationer och relaterade processer.

1.2. Den säkerställer att alla ändringar genomförs på ett kontrollerat och granskningsbart sätt, vilket minimerar risken för störningar, säkerhetsbrister eller bristande regelefterlevnad.

1.3. Den stöder ISO/IEC 27001:2022 bilaga A, kontroll 8.32, genom att kräva säker, dokumenterad och riskanpassad praxis för ändringshantering.

1.4. Policyn säkerställer även spårbarhet i ändringsbeslut och stärker den operativa motståndskraften vid planerade eller akuta ändringar.

2. Omfattning

2.1. Denna policy gäller för alla ändringar som påverkar system, data och miljöer inom ISMS omfattning, inklusive:

2.1.1. IT-infrastruktur (lokal, molnbaserad och hybrid)

2.1.2. Produktions-, förproduktions- och katastrofåterställningsmiljöer

2.1.3. Verksamhetsapplikationer, tjänster, API:er och integrationer

2.1.4. Konfigurationsinställningar, patchning, programvarureleaser och systemmigreringar

2.1.5. Akuta korrigeringar samt projektbaserade eller planerade ändringar

2.2. Den omfattar ändringar som initieras av:

2.2.1. Intern personal (IT-drift, utvecklare och systemägare)

2.2.2. Externa leverantörer, leverantörer av hanterade tjänster (MSP:er), entreprenörer och tredjepartstjänsteleverantörer

2.2.3. Projektteam vid systemimplementering, uppgraderingar eller tjänsteövergångar

2.3. Denna policy gäller inte för:

2.3.1. Tillfälliga test- och utvecklingsmiljöer utan åtkomst till produktionsdata

2.3.2. Personliga användarkonfigurationer (omfattas av policy för godtagbar användning)

2.3.3. Ändringar i system utanför organisationens kontrollgräns, om de inte påverkar integrerade tillgångar eller krav på regelefterlevnad

3. Mål

3.1. Att säkerställa att alla ändringar granskas, godkänns, testas och dokumenteras före genomförande.

3.2. Att upprätthålla systemtillgänglighet, dataintegritet och tjänstekontinuitet under och efter ändringsaktiviteter.

3.3. Att kräva definierade ändringsklassificeringar, återgångsplanering och riskbedömningar för alla typer av ändringar.

3.4. Att möjliggöra transparent beslutsfattande och eskalering genom strukturerad styrning.

3.5. Att stödja revisionsberedskap genom spårbara ändringsposter och granskning efter implementering.

3.6. Att upprätthålla funktionsuppdelning och minska risken för otillåtna eller motstridiga ändringar i kritiska system.

4. Roller och ansvar

4.1. Verkställande ledning

4.1.1. Godkänner ändringshanteringspolicyn och säkerställer anpassning till strategiska mål och regulatoriska krav.

4.1.2. Godkänner ändringsprogram med hög påverkan eller tvärfunktionell omfattning som en del av styrning och tillsyn.

4.1.3. Avsätter nödvändiga resurser och budget för verktyg för ändringskontroll och utbildning av personal.

4.2. Ändringsråd

4.2.1. Granskar och godkänner standardändringar och större ändringar samt säkerställer lämplig utvärdering av risk, påverkan och beroenden.

4.2.2. Validerar återgångsplaner, testresultat, kommunikation till intressenter och schemaläggning.

4.2.3. Består av systemägare, informationssäkerhetsfunktion, IT-drift, verksamhetsspecialister och representanter för regelefterlevnad.

4.2.4. Får delegera beslut om lågriskändringar eller akuta ändringar enligt dokumenterade villkor.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav på granskning och uppdatering

9.1. Utlösande faktorer och granskningsfrekvens

9.1.1. Denna policy ska granskas årligen eller vid:

9.1.1.1. Större ändringar i IT eller infrastruktur

9.1.1.2. Betydande incidenter relaterade till misslyckade eller otillåtna ändringar

9.1.1.3. Regulatoriska uppdateringar eller nya rättsliga skyldigheter kopplade till ändringar

9.1.1.4. Införande av nya verktyg eller plattformar för systemet för ändringshantering

9.2. Granskningsprocess för ändringshanteringspolicyn

9.2.1. Ändringsansvarig ska leda granskningsprocessen i samarbete med:

9.2.1.1. IT, säkerhet och drift

9.2.1.2. Internrevision och riskhantering

9.2.1.3. CAB-representanter

9.2.2. Uppdateringar ska granskas och godkännas av verkställande ledning och styrgruppen för informationssäkerhet (ISSC).

9.2.3. Återutgivna versioner ska registreras i dokumentregistret och kommuniceras till berörda parter med förnyad bekräftelse vid behov.

9.3. Dokumentstyrning och versionshantering

9.3.1. Alla versioner ska innehålla:

9.3.1.1. Policy-ID, titel och klassificeringsnivå

9.3.1.2. Ägare och revisionshistorik

9.3.1.3. Ändringslogg och ikraftträdandedatum

9.3.1.4. Godkännandeinstans

9.3.2. Arkiverade versioner ska bevaras i enlighet med policyn för dokumentbevarande (minst 3 år).

10. Relaterade policyer och kopplingar

10.1. Denna policy är direkt kopplad till och stöder tillämpningen av:

10.1.1. P1 – Informationssäkerhetspolicy: Fastställer kravet på formella säkerhetskontroller och ansvarstagande på processnivå, inklusive styrning av ändringshantering.

10.1.2. P2 – Policy för styrningsroller och ansvar: Definierar godkännandebefogenheter och funktionsuppdelning som är relevanta för ändringsgodkännande och tillsyn.

10.1.3. P4 – Åtkomstkontrollpolicy: Säkerställer att åtkomstbehörigheter för dem som genomför och granskar ändringar följer principen om minsta privilegium.

10.1.4. P6 – Riskhanteringspolicy: Säkerställer att alla ändringar omfattas av lämplig riskbedömning och riskreducerande strategier.

10.1.5. P33 – Policy för övervakning av revision och regelefterlevnad: Reglerar validering och revisionsgranskning av poster och överträdelser inom ändringshantering.

10.2. Dessa policyer möjliggör sammantaget en försvarbar, spårbar och säker livscykel för ändringshantering inom ISMS-ramverket.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001:2022

11.1.1. Klausul 6.1 – Åtgärder för att hantera risker och möjligheter: Denna policy stöder identifiering, utvärdering och kontroll av risker relaterade till ändringar.

11.1.2. Klausul 5.15 – Åtkomstkontroll: Säkerställer att åtkomst vid ändringar är kontrollerad och spårbar.

11.1.3. Bilaga A, kontroll 8.32 – Ändringshantering: Denna policy genomför fullt ut kravet att hantera ändringar i informationsbehandlingsanläggningar och system på ett planerat och kontrollerat sätt.

11.2. ISO/IEC 27002:2022 – Kontroll 8

11.2.1. Förstärker genomförandet av en strukturerad process för ändringshantering, inklusive ändringsklassificering, godkännande, testning, återgång och dokumentation.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM-familjen (CM-1 till CM-14): Denna policy är nära anpassad till kontroller för konfigurationshantering, inklusive baskonfigurationer (CM-2), styrning av konfigurationsändringar (CM-3), analys av säkerhetspåverkan (CM-4) och åtkomstbegränsningar (CM-5).

11.3.2. AU-familjen (AU-2, AU-6, AU-12): De loggnings- och revisionsmekanismer som refereras i denna policy stöder spårbarhet för händelser och granskning av regelefterlevnad för ändringsrelaterade aktiviteter.

11.3.3. RA-3, RA-5: Riskbedömningar och sårbarhetsskanningar som utlöses av ändringar är inbyggda i processen för ändringsutvärdering.

11.3.4. PM-11 (Definition av uppdrag/verksamhetsprocess): Säkerställer att verksamhetskontinuitet och operativa mål bevaras under ändringar.

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

11.4.1. Artikel 32(1)(b–d): Denna policy stöder kravet på lämpliga tekniska och organisatoriska åtgärder för att säkerställa datasäkerhet, särskilt vid systemändringar.

11.4.2. Artikel 25 – Inbyggt dataskydd och dataskydd som standard: Säkerställer att ändringar som påverkar personuppgifter integrerar dataskydd och säkerhet i design och driftsättning.

11.4.3. Skäl 78: Kräver att personuppgiftsansvariga inför mekanismer, såsom policyer för ändringskontroll, för att säkerställa fortlöpande konfidentialitet, riktighet och motståndskraft i behandlingssystem.

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

11.5.1. Artikel 21(2)(a, b, d, e): Ställer krav på tekniska och organisatoriska åtgärder för att hantera IKT-risker, inklusive sådana som uppstår genom systemändringar, programvaruuppdateringar och ändringar i infrastrukturen.

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

11.6.1. Artikel 5 – Ramverk för styrning och intern kontroll: Denna policy upprätthåller principer för operativ riskhantering kopplade till IKT-ändringar och uppdateringar.

11.6.2. Artikel 8 – Ramverk för hantering av IKT-risker: Kräver att finansiella entiteter hanterar alla ändringar som påverkar IKT-system inom strukturerade processer för ändringshantering, vilket återspeglas i denna policys krav på klassificering, testning, återgång och dokumentation.

11.6.3. Artikel 12 – Incidentrapportering: Säkerställer att misslyckade ändringar som leder till IKT-störningar är spårbara, dokumenterade och rapporterade där så är tillämpligt.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: Denna policy uppfyller direkt BAI06-målen genom att etablera strukturerade arbetsflöden för ändringsgodkännande, påverkansbedömning, kommunikation och testning.

11.7.2. BAI02 – Managed Requirements Definition och BAI03 – Managed Solutions Identification and Build: Säkerställer att verksamhetsdrivna ändringar granskas och genomförs på ett säkert sätt.

11.7.3. DSS01 – Managed Operations: Stöder fortlöpande systemintegritet vid genomförande av ändringar.

11.7.4. MEA01 och MEA03 – Monitor, Evaluate, and Assess Performance and Compliance: Möjliggör kontinuerlig tillsyn över ändringshanteringspolicyns effektivitet och efterlevnad.