					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P05S					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/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 8	
ISO/IEC 27002:2022	Kontroll 8	
NIST SP 800-53 Rev. 5	CM-2 till CM-5, CM-11	
EU:s NIS2-direktiv	Artikel 21.2 b	
EU:s DORA-förordning	Artiklar 6.9, 8.4 b	
COBIT 2019	BAI06, DSS01	

1. Syfte

1.1 Denna policy säkerställer att alla ändringar i IT-system, konfigurationer, verksamhetsapplikationer eller molntjänster planeras, riskbedöms, testas och godkänns innan de genomförs.

1.2 Syftet är att minska operativa störningar, säkerhetsrisker och tjänsteavbrott genom att fastställa en förenklad men tillämpbar process som även är anpassad för mindre företag med begränsade resurser.

1.3 Denna policy stödjer certifiering enligt ISO/IEC 27001:2022 genom att formalisera hur tekniska och operativa ändringar hanteras och dokumenteras.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Anställda och avdelningschefer som föreslår eller genomför ändringar

2.1.2 Externa IT-tjänsteleverantörer som hanterar system eller programvara

2.1.3 Verkställande direktören, som har det övergripande ansvaret för godkännande av ändringar

2.2 Policyn omfattar ändringar i:

2.2.1 Programvara (uppdateringar, patchar, nya applikationer)

2.2.2 Hårdvara (utbyten, uppgraderingar)

2.2.3 Nätverks- och brandväggskonfigurationer

2.2.4 Molntjänster, användarbehörigheter eller leverantörsintegrationer

2.2.5 Ändringar i kritiska verksamhetsprocesser som involverar informationssystem

2.3 Både planerade och akuta ändringar omfattas av denna policy.

3. Mål

3.1 Säkerställa att alla ändringar i IT- och verksamhetssystem är godkända, dokumenterade och möjliga att återställa om problem uppstår.

3.2 Förebygga oplanerade driftavbrott, dataförlust eller säkerhetsincidenter som orsakas av okontrollerade ändringar.

3.3 Fastställa enkla och repeterbara rutiner för inlämning av ändringsbegäran, godkännande, testning och återställning.

3.4 Upprätthålla en revisionsbar ändringslogg som stödjer operativt ansvarstagande och regelefterlevnad.

3.5 Möjliggöra riskbaserat beslutsfattande för betydande eller känsliga ändringar.

4. Roller och ansvar

4.1 Verkställande direktören

4.1.1 Har det yttersta ansvaret för alla större ändringar.

4.1.2 Granskar och godkänner icke-rutinmässiga, kritiska eller högriskändringar.

4.1.3 Granskar ändringsloggen kvartalsvis eller efter större incidenter.

4.2 IT-support eller outsourcad IT-leverantör

4.2.1 Genomför ändringar, inklusive konfigurationsuppdateringar, patchning och systemmigreringar.

4.2.2 Upprätthåller en grundläggande ändringslogg med uppgifter om datum, typ av ändring, utfall och godkännare.

4.2.3 Testar ändringar före genomförande och tillämpar återställningssteg vid behov.

4.2.4 Informerar berörda användare före och efter större ändringar.

[... 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 Årlig granskning

9.1.1 Denna policy ska granskas årligen av verkställande direktören eller utsedd IT-kontakt för att säkerställa anpassning till aktuella system, arbetsflöden och regulatoriska krav.

9.2 Granskning mellan ordinarie tillfällen

9.2.1 Granskning ska även initieras vid:

9.2.1.1 Säkerhetsincidenter som orsakas av bristfällig ändringshantering

9.2.1.2 Införande av nya IT-system

9.2.1.3 Ändringar i relevanta standarder såsom ISO, NIS2 eller DORA

9.3 Dokumentation av uppdateringar

9.3.1 Ändringar i denna policy ska versionshanteras och godkännas av verkställande direktören. Varje version ska ange datum, sammanfattning av ändringar och godkännare.

9.4 Kommunikation av policyn

9.4.1 Eventuella uppdateringar ska kommuniceras till alla berörda anställda och externa leverantörer. Dokumentation ska uppdateras på alla relevanta platser där policyn refereras eller tillhandahålls (t.ex. personalportal, delade enheter).

10. Relaterade policyer och kopplingar

10.1 Denna policy är nära kopplad till följande SME-policyer:

10.1.1 P2S – Policy för roller och ansvar inom styrning: Definierar befogenhet att godkänna ändringar.

10.1.2 P4S – Åtkomstkontrollpolicy: Säkerställer att åtkomständringar till följd av ändringar dokumenteras och genomförs korrekt.

10.1.3 P7S – Policy för introduktion och avslut: Samordnar ändringar som rör rollövergångar och behörighetstilldelning.

10.1.4 P15S – Policy för säkerhetskopiering och återställning: Säkerställer att återställnings- och återhämtningssteg kan genomföras om en ändring misslyckas.

10.1.5 P30S – Policy för incidenthantering: Styr hur misslyckade eller otillåtna ändringar hanteras som säkerhetsincidenter.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Riskbaserad planering ska omfatta ändringsaktiviteter.

11.1.2 Klausul 8.1 – Operativa kontroller ska tillämpas konsekvent för ändringsrelaterade aktiviteter för att säkerställa tjänsternas riktighet.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.32 – Ger vägledning för säkra ändringshanteringsprocesser, inklusive dokumentation, testning och godkännande.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Baskonfiguration för system före ändring.

11.3.2 CM-3 – Styrning av konfigurationsändringar.

11.3.3 CM-4 – Analys av säkerhetspåverkan.

11.3.4 CM-5 – Ändringsgodkännande och dokumentation.

11.3.5 CM-11 – Revision och övervakning av ändringar.

11.4 EU:s NIS2-direktiv

11.4.1 Artikel 21.2 b – Kräver formella rutiner för tekniska och organisatoriska säkerhetsåtgärder, inklusive ändringshantering.

11.5 EU:s DORA-förordning

11.5.1 Artiklar 6.9 och 8.4 b – Kräver att finansiella entiteter upprätthåller ändrings- och konfigurationshantering för IKT-system.

11.6 COBIT 2019

11.6.1 BAI06 – Hantera ändringar: Betonar planering, riskutvärdering och förmåga till återställning.

11.6.2 DSS01 – Hantera drift: Säkerställer operativ riktighet vid tekniska övergångar och ändringar.