					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P05S					Documenttitel: **Wijzigingsbeheerbeleid**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 6.1, 8	
ISO/IEC 27002:2022	Beheersmaatregel 8	
NIST SP 800-53 Rev. 5	CM-2 t/m CM-5, CM-11	
EU NIS2	Artikel 21(2)(b)	
EU DORA	Artikelen 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Doel

1.1 Dit beleid waarborgt dat alle wijzigingen aan IT-systemen, configuraties, bedrijfstoepassingen of clouddiensten vóór implementatie worden gepland, op risico worden beoordeeld, getest en goedgekeurd.

1.2 Het doel is operationele verstoringen, beveiligingsrisico's en dienstonderbrekingen te beperken door een vereenvoudigd maar afdwingbaar proces vast te stellen dat ook toepasbaar is op kleine ondernemingen met beperkte middelen.

1.3 Dit beleid ondersteunt certificering volgens ISO/IEC 27001:2022 door vast te leggen hoe technische en operationele wijzigingen worden beheerd en gedocumenteerd.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 werknemers en afdelingsmanagers die wijzigingen voorstellen of uitvoeren

2.1.2 externe IT-dienstverleners die systemen of software beheren

2.1.3 de algemeen directeur (GM), die de eindverantwoordelijkheid draagt voor goedkeuring van wijzigingen

2.2 Dit beleid heeft betrekking op wijzigingen in:

2.2.1 software (updates, patches, nieuwe toepassingen)

2.2.2 hardware (vervangingen, upgrades)

2.2.3 netwerk- en firewallconfiguraties

2.2.4 clouddiensten, toegangsrechten of integraties met leveranciers

2.2.5 wijzigingen in kritieke bedrijfsprocessen waarbij informatiesystemen betrokken zijn

2.3 Zowel geplande als noodwijzigingen vallen binnen de reikwijdte van dit beleid.

3. Doelstellingen

3.1 Waarborgen dat alle wijzigingen in IT- en bedrijfssystemen geautoriseerd, gedocumenteerd en terug te draaien zijn indien zich problemen voordoen.

3.2 Ongeplande uitval, gegevensverlies of beveiligingsincidenten als gevolg van onbeheerde wijzigingen voorkomen.

3.3 Eenvoudige, herhaalbare procedures vaststellen voor het indienen, goedkeuren, testen en terugdraaien van wijzigingen.

3.4 Een auditbaar wijzigingslogboek bijhouden dat operationele verantwoording en naleving van wet- en regelgeving ondersteunt.

3.5 Risicogebaseerde besluitvorming mogelijk maken voor significante of gevoelige wijzigingen.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Draagt de eindverantwoordelijkheid voor alle majeure wijzigingen.

4.1.2 Beoordeelt en keurt niet-routinematige, kritieke of hoogrisicowijzigingen goed.

4.1.3 Beoordeelt het wijzigingslogboek elk kwartaal of na majeure incidenten.

4.2 IT-support of uitbestede IT-dienstverlener

4.2.1 Voert wijzigingen uit, waaronder configuratie-updates, patchbeheer en systeemmigraties.

4.2.2 Houdt een basiswijzigingslogboek bij met registraties van datums, typen wijzigingen, uitkomsten en goedkeurders.

4.2.3 Test wijzigingen vóór implementatie en past waar nodig rollbackplannen toe.

4.2.4 Informeert betrokken gebruikers vóór en na majeure wijzigingen.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisering

9.1 Jaarlijkse beoordeling

9.1.1 Dit beleid moet jaarlijks worden beoordeeld door de algemeen directeur (GM) of een aangewezen IT-contactpersoon om te waarborgen dat het aansluit op actuele systemen, werkprocessen en wettelijke en reglementaire vereisten.

9.2 Tussentijdse beoordelingen

9.2.1 Beoordelingen moeten ook worden gestart naar aanleiding van:

9.2.1.1 beveiligingsincidenten veroorzaakt door gebrekkig wijzigingsbeheer

9.2.1.2 invoering van nieuwe IT-systemen

9.2.1.3 wijzigingen in relevante normen zoals ISO, NIS2 of DORA

9.3 Documentatie van actualisaties

9.3.1 Wijzigingen in dit beleid moeten onder versiebeheer worden gebracht en worden goedgekeurd door de algemeen directeur (GM). Van elke versie moeten de datum, een samenvatting van de wijzigingen en de goedkeurder worden vastgelegd.

9.4 Communicatie van beleid

9.4.1 Eventuele actualisaties moeten worden gecommuniceerd aan alle betrokken werknemers en externe dienstverleners. Documentatie moet worden bijgewerkt op alle relevante referentielocaties (bijvoorbeeld medewerkersportaal, gedeelde schijven).

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid hangt nauw samen met de volgende SME-beleidslijnen:

10.1.1 P2S – Beleid inzake bevoegdheden en verantwoording: bepaalt de goedkeuringsbevoegdheid voor wijzigingen.

10.1.2 P4S – Toegangscontrolebeleid: waarborgt dat wijzigingen in toegangsrechten als gevolg van wijzigingen correct worden gedocumenteerd en geïmplementeerd.

10.1.3 P7S – Onboarding- en offboardingbeleid: coördineert wijzigingen in verband met rolwisselingen en toekenning van toegangsrechten.

10.1.4 P15S – Back-up- en herstelbeleid: waarborgt dat rollback- en herstelstappen kunnen worden uitgevoerd als een wijziging mislukt.

10.1.5 P30S – Incidentresponsbeleid (P30): bepaalt hoe mislukte of ongeautoriseerde wijzigingen als beveiligingsincidenten worden behandeld.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1 – Risicogebaseerde planning moet wijzigingsactiviteiten omvatten.

11.1.2 Clausule 8.1 – Operationele beheersmaatregelen moeten consequent worden toegepast op wijzigingsgerelateerde activiteiten om de integriteit van diensten te waarborgen.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.32 – Biedt richtsnoeren voor veilige wijzigingsbeheerprocessen, waaronder documentatie, testen en goedkeuring.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Baselineconfiguratie voor systemen voorafgaand aan wijziging.

11.3.2 CM-3 – Beheer van configuratiewijzigingen.

11.3.3 CM-4 – Analyse van beveiligingsimpact.

11.3.4 CM-5 – Wijzigingsgoedkeuring en documentatie.

11.3.5 CM-11 – Audit en monitoring van wijzigingen.

11.4 EU NIS2-richtlijn

11.4.1 Artikel 21(2)(b) – Vereist formele procedures voor technische en organisatorische beveiligingsmaatregelen, waaronder wijzigingsbeheer.

11.5 EU DORA

11.5.1 Artikelen 6(9) en 8(4)(b) – Vereisen dat financiële entiteiten wijzigings- en configuratiebeheer voor ICT-systemen in stand houden.

11.6 COBIT 2019

11.6.1 BAI06 – Wijzigingen beheren: legt nadruk op planning, risicobeoordeling en rollbackmogelijkheden.

11.6.2 DSS01 – Operaties beheren: waarborgt operationele integriteit tijdens technische overgangen en wijzigingen.