					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P05					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**

Uitgelijnd met normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 6.1, 5	Behandelt risicobeheersmaatregelen, toegangsbeheersing en wijzigingsbeheer
ISO/IEC 27002:2022	Beheersmaatregel 8	Implementeert een gestructureerd wijzigingsbeheerproces
NIST SP 800-53 Rev.5	CM-2 tot en met CM-14	Maatregelen voor configuratiebeheer
EU AVG	Artikelen 32(1)(b–d), 25; overweging 78	Technische en organisatorische maatregelen voor systeem- en gegevensbeveiliging tijdens wijzigingen
EU NIS2	Artikel 21(2)(a, b, d, e)	Verplicht risicobeheer van ICT-wijzigingen
EU DORA	Artikelen 5, 8, 12	Regelt operationeel ICT-risico en incidentrapportage
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA	Gestructureerde eisen voor prestaties, naleving en IT-wijzigingsbeheer

1. Doel

1.1. Dit beleid stelt een formeel kader vast voor het initiëren, beoordelen, goedkeuren, implementeren en evalueren van wijzigingen in de informatiesystemen, infrastructuur, toepassingen en gerelateerde processen van de organisatie.

1.2. Het waarborgt dat alle wijzigingen op een gecontroleerde en auditeerbare wijze worden uitgevoerd, waarbij het risico op verstoring, beveiligingsincidenten of niet-naleving tot een minimum wordt beperkt.

1.3. Het ondersteunt ISO/IEC 27001:2022 Annex A Beheersmaatregel 8.32 door veilige, gedocumenteerde en op risico afgestemde wijzigingsbeheerprocessen af te dwingen.

1.4. Het beleid waarborgt tevens de traceerbaarheid van wijzigingsbesluiten en bevordert de operationele weerbaarheid tijdens geplande wijzigingen en noodwijzigingen.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle wijzigingen die systemen, gegevens en omgevingen binnen de reikwijdte van het ISMS raken, met inbegrip van:

2.1.1. IT-infrastructuur (on-premises, cloud en hybride)

2.1.2. Productie-, preproductie- en disaster recovery-omgevingen

2.1.3. Bedrijfstoepassingen, diensten, API's en integraties

2.1.4. Configuratie-instellingen, patching, softwarereleases en systeemmigraties

2.1.5. Noodreparaties en projectmatige of geplande wijzigingen

2.2. Het beleid is van toepassing op wijzigingen die worden geïnitieerd door:

2.2.1. Intern personeel (IT-operatie, ontwikkelaars en systeemeigenaren)

2.2.2. Externe leveranciers, managed service providers (MSP's) en opdrachtnemers

2.2.3. Projectteams tijdens systeemimplementaties, upgrades of servicetransities

2.3. Dit beleid is niet van toepassing op:

2.3.1. Tijdelijke test- of ontwikkelomgevingen zonder toegang tot productiegegevens

2.3.2. Persoonlijke gebruikersconfiguraties (geregeld in het Beleid inzake aanvaardbaar gebruik)

2.3.3. Wijzigingen in systemen buiten de beheersgrenzen van de organisatie, tenzij deze gevolgen hebben voor geïntegreerde bedrijfsmiddelen of nalevingsverplichtingen

3. Doelstellingen

3.1. Waarborgen dat alle wijzigingen vóór uitvoering worden beoordeeld, goedgekeurd, getest en gedocumenteerd.

3.2. De beschikbaarheid van systemen, de integriteit van gegevens en de continuïteit van de dienstverlening tijdens en na wijzigingsactiviteiten handhaven.

3.3. Vereisen dat voor alle wijzigingstypen vastgestelde wijzigingsclassificaties, rollbackplannen en risicobeoordelingen beschikbaar zijn.

3.4. Transparante besluitvorming en escalatie mogelijk maken via een gestructureerd governancemodel.

3.5. Auditgereed blijven door middel van traceerbare wijzigingsregistraties en evaluaties na implementatie.

3.6. Functiescheiding (SoD) afdwingen en het risico op ongeautoriseerde of conflicterende wijzigingen in kritieke systemen verminderen.

4. Rollen en verantwoordelijkheden

4.1. Topmanagement

4.1.1. Bekrachtigt het Wijzigingsbeheerbeleid en waarborgt de afstemming op strategische doelstellingen en wettelijke en regelgevende verplichtingen.

4.1.2. Keurt wijzigingsprogramma's met hoge impact of een organisatiebreed karakter goed als onderdeel van het governancetoezicht.

4.1.3. Stelt de benodigde middelen en budgetten beschikbaar voor tooling voor wijzigingsbeheersing en opleiding van personeel.

4.2. Change Advisory Board

4.2.1. Beoordeelt en autoriseert standaardwijzigingen en majeure wijzigingen en ziet erop toe dat risico's, impact en afhankelijkheden adequaat worden geëvalueerd.

4.2.2. Valideert rollbackplannen, testresultaten, communicatie aan belanghebbenden en planning.

4.2.3. Bestaat uit systeemeigenaren, informatiebeveiliging, IT-operatie, businessverantwoordelijken en vertegenwoordigers van compliance.

4.2.4. Mag onder gedocumenteerde voorwaarden besluitvorming over wijzigingen met laag risico of noodwijzigingen delegeren.

[... 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 actualisatie

9.1. Aanleidingen voor herziening en frequentie

9.1.1. Dit beleid moet jaarlijks worden herzien of bij:

9.1.1.1. Grote wijzigingen in IT of infrastructuur

9.1.1.2. Significante incidenten die verband houden met mislukte of ongeautoriseerde wijzigingen

9.1.1.3. Regelgevende actualisaties of nieuwe wettelijke verplichtingen met betrekking tot wijzigingen

9.1.1.4. Implementatie van nieuwe tooling of CMS-platformen

9.2. Proces voor herziening van het Wijzigingsbeheerbeleid

9.2.1. De changemanager leidt het herzieningsproces in samenwerking met:

9.2.1.1. IT, informatiebeveiliging en operatie

9.2.1.2. Interne audit en risicomanagement

9.2.1.3. CAB-vertegenwoordigers

9.2.2. Actualisaties moeten worden beoordeeld en goedgekeurd door het topmanagement en de ISMS-stuurgroep.

9.2.3. Opnieuw uitgegeven versies moeten worden bijgehouden in het documentenregister en aan betrokken partijen worden gecommuniceerd, met hernieuwde kennisname waar nodig.

9.3. Documentbeheer en versiebeheer

9.3.1. Alle versies moeten bevatten:

9.3.1.1. Beleids-ID, titel en classificatieniveau

9.3.1.2. Eigenaar en revisiehistorie

9.3.1.3. Wijzigingslogboek en ingangsdatum

9.3.1.4. Goedkeuringsbevoegdheid

9.3.2. Gearchiveerde versies moeten worden bewaard overeenkomstig het Documentbewaringsbeleid (minimaal 3 jaar).

10. Gerelateerde beleidslijnen en samenhang

10.1. Dit beleid houdt rechtstreeks verband met en ondersteunt de handhaving van:

10.1.1. P1 – Informatiebeveiligingsbeleid: stelt de vereiste vast voor formele beveiligingsmaatregelen en verantwoording op procesniveau, met inbegrip van governance voor wijzigingsbeheer.

10.1.2. P2 – Beleid inzake governancerollen en -verantwoordelijkheden: definieert goedkeuringsbevoegdheden en functiescheiding die relevant zijn voor autorisatie en toezicht op wijzigingen.

10.1.3. P4 – Beleid inzake toegangsbeheersing: waarborgt dat toegangsrechten voor uitvoerders en beoordelaars van wijzigingen het beginsel van minimale bevoegdheden volgen.

10.1.4. P6 – Risicobeheerbeleid: waarborgt dat alle wijzigingen aan een passende risicobeoordeling en mitigatiestrategie worden onderworpen.

10.1.5. P33 – Beleid inzake audit- en compliancemonitoring: regelt de validatie en auditbeoordeling van registraties en overtredingen met betrekking tot wijzigingsbeheer.

10.2. Deze beleidslijnen maken gezamenlijk een verdedigbare, traceerbare en veilige levenscyclus van wijzigingsbeheer mogelijk binnen het ISMS-kader.

11. Referentienormen en -raamwerken

11.1. ISO/IEC 27001:2022

11.1.1. Clausule 6.1 – Maatregelen voor het aanpakken van risico's en kansen: dit beleid ondersteunt de identificatie, evaluatie en beheersing van risico's met betrekking tot wijzigingen.

11.1.2. Clausule 5.15 – Toegangsbeheersing: waarborgt dat toegang tijdens wijzigingen gecontroleerd en traceerbaar is.

11.1.3. Annex A Beheersmaatregel 8.32 – Wijzigingsbeheer: dit beleid implementeert volledig de vereiste om wijzigingen in voorzieningen en systemen voor informatieverwerking op een geplande en gecontroleerde wijze te beheren.

11.2. ISO/IEC 27002:2022 – Beheersmaatregel 8

11.2.1. Versterkt de implementatie van een gestructureerd wijzigingsbeheerproces, waaronder wijzigingsclassificatie, goedkeuring, testen, rollback en documentatie.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM-familie (CM-1 tot en met CM-14): dit beleid is nauw afgestemd op maatregelen voor configuratiebeheer, waaronder baselineconfiguraties (CM-2), beheersing van configuratiewijzigingen (CM-3), beveiligingsimpactanalyse (CM-4) en toegangsbeperkingen (CM-5).

11.3.2. AU-familie (AU-2, AU-6, AU-12): de in dit beleid genoemde logging- en auditmechanismen ondersteunen de traceerbaarheid van gebeurtenissen en de nalevingsbeoordeling van wijzigingsgerelateerde activiteiten.

11.3.3. RA-3, RA-5: door wijzigingen gestuurde risicobeoordelingen en kwetsbaarheidsscans zijn ingebed in het evaluatieproces van wijzigingen.

11.3.4. PM-11 (Definitie van missie-/bedrijfsprocessen): waarborgt dat bedrijfscontinuïteit en operationele doelstellingen tijdens wijzigingen behouden blijven.

11.4. EU AVG (2016/679)

11.4.1. Artikel 32(1)(b–d): dit beleid ondersteunt de vereiste voor passende technische en organisatorische maatregelen om gegevensbeveiliging te waarborgen, in het bijzonder tijdens systeemwijzigingen.

11.4.2. Artikel 25 – Gegevensbescherming door ontwerp en standaardinstellingen: waarborgt dat wijzigingen die persoonsgegevens raken, privacy en beveiliging integreren in ontwerp en uitrol.

11.4.3. Overweging 78: vereist dat verwerkingsverantwoordelijken mechanismen implementeren, zoals beleid voor wijzigingsbeheer, om de voortdurende vertrouwelijkheid, integriteit en weerbaarheid van verwerkingssystemen te waarborgen.

11.5. EU NIS2-richtlijn (2022/2555)

11.5.1. Artikel 21(2)(a, b, d, e): verplicht technische en organisatorische maatregelen voor het beheren van ICT-risico's, waaronder risico's die voortvloeien uit systeemwijzigingen, software-updates en infrastructuuraanpassingen.

11.6. EU DORA (2022/2554)

11.6.1. Artikel 5 – Governance- en internebeheersingskader: dit beleid dwingt beginselen van operationeel risicobeheer af die samenhangen met ICT-wijzigingen en updates.

11.6.2. Artikel 8 – ICT-risicobeheerkader: verplicht financiële entiteiten alle wijzigingen die impact hebben op ICT-systemen te beheren binnen gestructureerde wijzigingsbeheerprocessen, zoals weerspiegeld in de classificatie-, test-, rollback- en documentatievereisten van dit beleid.

11.6.3. Artikel 12 – Incidentrapportage: waarborgt dat mislukte wijzigingen die leiden tot ICT-verstoringen traceerbaar zijn, worden gedocumenteerd en waar van toepassing worden gerapporteerd.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: dit beleid geeft rechtstreeks invulling aan de doelstellingen van BAI06 door gestructureerde workflows voor goedkeuring van wijzigingen, impactbeoordeling, communicatie en testen vast te stellen.

11.7.2. BAI02 – Managed Requirements Definition en BAI03 – Managed Solutions Identification and Build: waarborgen dat door de business geïnitieerde wijzigingen veilig worden beoordeeld en geïmplementeerd.

11.7.3. DSS01 – Managed Operations: ondersteunt de voortdurende systeemintegriteit tijdens de uitvoering van wijzigingen.

11.7.4. MEA01 en MEA03 – Monitoren, evalueren en assessen van prestaties en naleving: maakt doorlopend toezicht op de doeltreffendheid en handhaving van het wijzigingsbeheerbeleid mogelijk.