					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P05					Dokumenttitel: **Änderungsmanagement-Richtlinie**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 6.1, 5	Behandelt Maßnahmen zum Umgang mit Risiken, Zugriffskontrolle und Änderungsmanagement
ISO/IEC 27002:2022	Maßnahme 8	Implementiert einen strukturierten Änderungsmanagementprozess
NIST SP 800-53 Rev.5	CM-2 bis CM-14	Kontrollen zum Konfigurationsmanagement
EU-DSGVO	Artikel 32(1)(b–d), 25; Erwägungsgrund 78	Technische und organisatorische Maßnahmen zur System- und Datensicherheit bei Änderungen
EU NIS2	Artikel 21(2)(a, b, d, e)	Verlangt das Risikomanagement von IKT-Änderungen
EU DORA	Artikel 5, 8, 12	Regelt operationelle und IKT-Risiken sowie die Vorfallmeldung
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Strukturiertes IT-Änderungsmanagement im Hinblick auf Leistung, Compliance und Anforderungen

1. Zweck

1.1. Diese Richtlinie legt einen formalen Rahmen für die Einleitung, Bewertung, Genehmigung, Umsetzung und Überprüfung von Änderungen an den Informationssystemen, Infrastrukturen, Anwendungen und zugehörigen Prozessen der Organisation fest.

1.2. Sie stellt sicher, dass alle Änderungen kontrolliert und auditierbar durchgeführt werden, um das Risiko von Störungen, Sicherheitsbeeinträchtigungen oder Verstößen gegen regulatorische Anforderungen zu minimieren.

1.3. Sie unterstützt ISO/IEC 27001:2022, Anhang A, Maßnahme 8.32, indem sie sichere, dokumentierte und risikoorientierte Praktiken des Änderungsmanagements verbindlich vorgibt.

1.4. Die Richtlinie gewährleistet zudem die Nachvollziehbarkeit von Änderungsentscheidungen und stärkt die operationelle Resilienz bei geplanten oder notfallbedingten Änderungen.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Änderungen, die Systeme, Daten und Umgebungen innerhalb des ISMS-Geltungsbereichs betreffen, einschließlich:

2.1.1. IT-Infrastruktur (On-Premises, Cloud, hybrid)

2.1.2. Produktions-, Vorproduktions- und Disaster-Recovery-Umgebungen

2.1.3. Geschäftsanwendungen, Services, APIs und Integrationen

2.1.4. Konfigurationseinstellungen, Patch-Management, Software-Releases und Systemmigrationen

2.1.5. Notfallkorrekturen sowie projektbezogene oder geplante Änderungen

2.2. Sie regelt Änderungen, die veranlasst werden durch:

2.2.1. internes Personal (IT-Betrieb, Entwicklung, Systemverantwortliche)

2.2.2. externe Lieferanten, Managed Service Provider (MSPs) und Auftragnehmer

2.2.3. Projektteams während der Systemimplementierung, bei Upgrades oder Serviceübergängen

2.3. Diese Richtlinie gilt nicht für:

2.3.1. temporäre Test- oder Entwicklungsumgebungen ohne Zugriff auf Produktionsdaten

2.3.2. persönliche Benutzerkonfigurationen (geregelt in der Richtlinie zur zulässigen Nutzung)

2.3.3. Änderungen an Systemen außerhalb des Kontrollbereichs der Organisation, es sei denn, sie betreffen integrierte Assets oder Compliance-Verpflichtungen

3. Ziele

3.1. Sicherzustellen, dass alle Änderungen vor der Durchführung geprüft, genehmigt, getestet und dokumentiert werden.

3.2. Systemverfügbarkeit, Datenintegrität und Servicekontinuität während und nach Änderungsaktivitäten aufrechtzuerhalten.

3.3. Für alle Änderungstypen definierte Änderungsklassifizierungen, Rollback-Pläne und Risikobewertungen verbindlich vorzuschreiben.

3.4. Transparente Entscheidungsfindung und Eskalation durch eine strukturierte Governance zu ermöglichen.

3.5. Auditbereitschaft durch nachvollziehbare Änderungsaufzeichnungen und Überprüfungen nach der Implementierung zu unterstützen.

3.6. Funktionstrennung durchzusetzen und das Risiko unbefugter oder kollidierender Änderungen in kritischen Systemen zu reduzieren.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsleitung

4.1.1. Befürwortet die Änderungsmanagement-Richtlinie und stellt die Ausrichtung an strategischen Zielen und regulatorischen Verpflichtungen sicher.

4.1.2. Genehmigt Änderungen mit hoher Auswirkung oder funktionsübergreifende Änderungsprogramme im Rahmen ihrer Governance-Aufsicht.

4.1.3. Stellt die erforderlichen Ressourcen und Budgets für Werkzeuge zur Änderungssteuerung sowie für Schulungen des Personals bereit.

4.2. Change Advisory Board (CAB)

4.2.1. Prüft und genehmigt Standardänderungen und wesentliche Änderungen und stellt dabei eine angemessene Bewertung von Risiken, Auswirkungen und Abhängigkeiten sicher.

4.2.2. Validiert Rollback-Pläne, Testergebnisse, die Kommunikation mit Interessenträgern und die Terminplanung.

4.2.3. Setzt sich aus Systemverantwortlichen, Informationssicherheit, IT-Betrieb, Geschäftsvertretern und Compliance-Verantwortlichen zusammen.

4.2.4. Kann Entscheidungen für risikoarme oder Notfalländerungen unter dokumentierten Bedingungen delegieren.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1. Auslöser und Häufigkeit der Überprüfung

9.1.1. Diese Richtlinie muss jährlich oder bei Eintritt eines der folgenden Ereignisse überprüft werden:

9.1.1.1. wesentliche IT- oder Infrastrukturänderungen

9.1.1.2. erhebliche Vorfälle im Zusammenhang mit fehlgeschlagenen oder unbefugten Änderungen

9.1.1.3. regulatorische Aktualisierungen oder neue rechtliche Verpflichtungen im Zusammenhang mit Änderungen

9.1.1.4. Einführung neuer Werkzeuge oder CMS-Plattformen

9.2. Überprüfungsprozess der Änderungsmanagement-Richtlinie

9.2.1. Der Change Manager leitet den Überprüfungsprozess in Zusammenarbeit mit:

9.2.1.1. IT, Informationssicherheit und Betrieb

9.2.1.2. Interner Revision, Compliance und Risikomanagement

9.2.1.3. CAB-Vertretern

9.2.2. Aktualisierungen müssen durch die Geschäftsleitung und den Informationssicherheitslenkungsausschuss geprüft und genehmigt werden.

9.2.3. Neu herausgegebene Versionen müssen im Dokumentenregister nachverfolgt und den betroffenen Parteien mit erneuter Bestätigung mitgeteilt werden, soweit erforderlich.

9.3. Dokumentenlenkung und Versionierung

9.3.1. Alle Versionen müssen Folgendes enthalten:

9.3.1.1. Richtlinienkennung, Titel und Klassifizierungsstufe

9.3.1.2. verantwortliche Stelle und Revisionshistorie

9.3.1.3. Änderungsprotokoll und Inkrafttretensdatum

9.3.1.4. Genehmigungsbefugnis

9.3.2. Archivierte Versionen müssen gemäß der Richtlinie zur Dokumentenaufbewahrung aufbewahrt werden (mindestens 3 Jahre).

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist unmittelbar verknüpft mit und unterstützt die Durchsetzung von:

10.1.1. P1 – Informationssicherheitsrichtlinie: Legt die Anforderung an formale Sicherheitskontrollen und Rechenschaftspflicht auf Prozessebene fest, einschließlich der Governance des Änderungsmanagements.

10.1.2. P2 – Richtlinie zu Rollen und Verantwortlichkeiten in der Governance: Definiert Genehmigungsbefugnisse und Funktionstrennung im Zusammenhang mit Änderungsfreigabe und Aufsicht.

10.1.3. P4 – Zugriffsrichtlinie: Stellt sicher, dass Zugriffsberechtigungen für Personen, die Änderungen umsetzen und prüfen, dem Least-Privilege-Prinzip folgen.

10.1.4. P6 – Risikomanagement-Richtlinie: Stellt sicher, dass alle Änderungen einer angemessenen Risikobewertung und risikomindernden Maßnahmen unterliegen.

10.1.5. P33 – Richtlinie zur Audit- und Compliance-Überwachung: Regelt die Validierung und Auditprüfung von Änderungsmanagementaufzeichnungen und Verstößen.

10.2. Diese Richtlinien ermöglichen gemeinsam einen belastbaren, nachvollziehbaren und sicheren Änderungsmanagement-Lebenszyklus innerhalb des ISMS-Rahmenwerks.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001:2022

11.1.1. Klausel 6.1 – Maßnahmen zum Umgang mit Risiken und Chancen: Diese Richtlinie unterstützt die Identifizierung, Bewertung und Steuerung von mit Änderungen verbundenen Risiken.

11.1.2. Klausel 5.15 – Zugriffskontrolle: Stellt sicher, dass Zugriffe während Änderungen kontrolliert und nachvollziehbar sind.

11.1.3. Anhang A, Maßnahme 8.32 – Änderungsmanagement: Diese Richtlinie setzt die Anforderung vollständig um, Änderungen an Einrichtungen und Systemen der Informationsverarbeitung geplant und kontrolliert zu steuern.

11.2. ISO/IEC 27002:2022 – Maßnahme 8

11.2.1. Verstärkt die Umsetzung eines strukturierten Änderungsmanagementprozesses einschließlich Änderungsklassifizierung, Genehmigung, Tests, Rollback und Dokumentation.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM-Familie (CM-1 bis CM-14): Diese Richtlinie ist eng an Kontrollen des Konfigurationsmanagements ausgerichtet, einschließlich Basis-Konfigurationen (CM-2), Steuerung von Konfigurationsänderungen (CM-3), Analyse der Sicherheitsauswirkungen (CM-4) und Zugriffsbeschränkungen (CM-5).

11.3.2. AU-Familie (AU-2, AU-6, AU-12): Die in dieser Richtlinie referenzierten Protokollierungs- und Auditmechanismen unterstützen die Nachvollziehbarkeit von Ereignissen und die Überprüfung der Compliance bei änderungsbezogenen Aktivitäten.

11.3.3. RA-3, RA-5: Durch Änderungen ausgelöste Risikobewertungen und Schwachstellenscans sind in den Änderungsbewertungsprozess eingebettet.

11.3.4. PM-11 (Definition von Auftrag/Geschäftsprozess): Stellt sicher, dass Geschäftskontinuität und operative Ziele während Änderungen gewahrt bleiben.

11.4. EU-DSGVO (2016/679)

11.4.1. Artikel 32(1)(b–d): Diese Richtlinie unterstützt die Anforderung an angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit, insbesondere bei Systemänderungen.

11.4.2. Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: Stellt sicher, dass Änderungen, die personenbezogene Daten betreffen, Datenschutz und Sicherheit in Design und Rollout integrieren.

11.4.3. Erwägungsgrund 78: Verlangt, dass Verantwortliche Mechanismen – wie Richtlinien zur Änderungssteuerung – implementieren, um die fortlaufende Vertraulichkeit, Integrität und Resilienz von Verarbeitungssystemen sicherzustellen.

11.5. EU-NIS2-Richtlinie (2022/2555)

11.5.1. Artikel 21(2)(a, b, d, e): Verlangt technische und organisatorische Maßnahmen zum Management von IKT-Risiken, einschließlich solcher aus Systemänderungen, Softwareaktualisierungen und Infrastrukturänderungen.

11.6. EU DORA (2022/2554)

11.6.1. Artikel 5 – Governance- und internes Kontrollrahmenwerk: Diese Richtlinie setzt Grundsätze des operationellen Risikomanagements im Zusammenhang mit IKT-Änderungen und Aktualisierungen um.

11.6.2. Artikel 8 – IKT-Risikomanagementrahmen: Verlangt, dass Finanzunternehmen alle Änderungen mit Auswirkungen auf IKT-Systeme im Rahmen strukturierter Änderungsmanagementprozesse steuern – abgebildet in den Vorgaben dieser Richtlinie zu Klassifizierung, Tests, Rollback und Dokumentation.

11.6.3. Artikel 12 – Vorfallmeldung: Stellt sicher, dass fehlgeschlagene Änderungen, die zu IKT-Störungen führen, nachvollziehbar, dokumentiert und gegebenenfalls gemeldet werden.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: Diese Richtlinie erfüllt die Ziele von BAI06 unmittelbar durch die Festlegung strukturierter Workflows für Änderungsgenehmigung, Auswirkungsbewertung, Kommunikation und Tests.

11.7.2. BAI02 – Managed Requirements Definition und BAI03 – Managed Solutions Identification and Build: Stellen sicher, dass geschäftsgetriebene Änderungen sicher geprüft und umgesetzt werden.

11.7.3. DSS01 – Managed Operations: Unterstützt die fortlaufende Systemintegrität während der Durchführung von Änderungen.

11.7.4. MEA01 und MEA03 – Überwachen, Bewerten und Beurteilen von Leistung und Compliance: Ermöglicht die kontinuierliche Aufsicht über die Wirksamkeit und Durchsetzung der Änderungsmanagement-Richtlinie.