| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P05S | | | | | Dokumenttitel:<br>**Änderungsmanagement-Richtlinie** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>01.01.2025 | | | Dokumentenverantwortlicher: | | | | | | | |
| X | Richtlinie | | Standard | | Verfahren | | Formular | | Register | | Sonstiges | |

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

| **Genehmigungen** | | | |
|---|---|---|---|
| **Name** | **Position** | **Datum** | **Unterschrift** |
| | | | |
| | | | |

**Rechtlicher Hinweis (Urheberrecht und Nutzungsbeschränkungen)**

(C) 2025 Clarysec LLC. All rights reserved.

Dieses Dokument ist geistiges Eigentum der Clarysec LLC. Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Genehmigung für kommerzielle oder Implementierungszwecke kopiert, wiederverwendet, verbreitet oder verändert werden.
Die unbefugte Nutzung ist streng untersagt und kann rechtliche Schritte nach sich ziehen.
Für Lizenzierungsanfragen kontaktieren Sie bitte: info@clarysec.com

Ausrichtung an Standards und Vorschriften, soweit anwendbar

| Standard/Vorschrift | Klausel/Artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klausel 6.1, 8 | |
| ISO/IEC 27002:2022 | Maßnahme 8 | |
| NIST SP 800-53 Rev. 5 | CM-2 bis CM-5, CM-11 | |
| EU NIS2 | Artikel 21(2)(b) | |
| EU DORA | Artikel 6(9), 8(4)(b) | |
| COBIT 2019 | BAI06, DSS | |

**1. Zweck**

1.1 Diese Richtlinie stellt sicher, dass alle Änderungen an IT-Systemen, Konfigurationen, Geschäftsanwendungen oder Cloud-Diensten vor der Umsetzung geplant, risikobewertet, getestet und genehmigt werden.

1.2 Ziel ist es, betriebliche Störungen, Sicherheitsrisiken und Serviceausfälle durch die Einführung eines vereinfachten, aber verbindlichen Verfahrens zu reduzieren, das auch für kleine Unternehmen mit begrenzten Ressourcen geeignet ist.

1.3 Diese Richtlinie unterstützt die Zertifizierung nach ISO/IEC 27001:2022, indem sie festlegt, wie technische und betriebliche Änderungen verwaltet und dokumentiert werden.

**2. Geltungsbereich**

**2.1 Diese Richtlinie gilt für:**

2.1.1 Mitarbeiter und Abteilungsleiter, die Änderungen beantragen oder umsetzen

2.1.2 Externe IT-Support-Dienstleister, die Systeme oder Software verwalten

2.1.3 Den Geschäftsführer (GM), der die Gesamtverantwortung für Änderungsgenehmigungen trägt

**2.2 Sie umfasst Änderungen an:**

2.2.1 Software (Updates, Patches, neue Anwendungen)

2.2.2 Hardware (Austausch, Upgrades)

2.2.3 Netzwerk- und Firewall-Konfigurationen

2.2.4 Cloud-Diensten, Benutzerzugriffsrechten oder Lieferantenintegrationen

2.2.5 Kritischen Änderungen von Geschäftsprozessen unter Einbeziehung von Informationssystemen

2.3 Sowohl geplante als auch Notfalländerungen fallen in den Geltungsbereich dieser Richtlinie.

**3. Ziele**

3.1 Sicherzustellen, dass alle Änderungen an IT- und Geschäftssystemen autorisiert, dokumentiert und bei Problemen rückgängig gemacht werden können.

3.2 Ungeplante Ausfallzeiten, Datenverlust oder Informationssicherheitsvorfälle zu verhindern, die durch unkontrollierte Änderungen verursacht werden.

3.3 Einfache und wiederholbare Verfahren für Änderungsanträge, Genehmigung, Tests und Rollback festzulegen.

3.4 Ein auditierbares Änderungsprotokoll zu führen, das die betriebliche Rechenschaftspflicht und die Einhaltung regulatorischer Anforderungen unterstützt.

3.5 Risikobasierte Entscheidungen für wesentliche oder sensible Änderungen zu ermöglichen.

## 4. Rollen und Verantwortlichkeiten

### 4.1 Geschäftsführer

4.1.1 Trägt die letztendliche Rechenschaftspflicht für alle wesentlichen Änderungen.

4.1.2 Prüft und genehmigt nicht routinemäßige, kritische oder risikoreiche Änderungen.

4.1.3 Prüft das Änderungsprotokoll vierteljährlich oder nach größeren Vorfällen.

### 4.2 IT-Support oder ausgelagerter IT-Support-Dienstleister

4.2.1 Setzt Änderungen um, einschließlich Konfigurationsaktualisierungen, Patch-Management und Systemmigrationen.

4.2.2 Führt ein grundlegendes Änderungsprotokoll mit Aufzeichnungen zu Datum, Änderungsart, Ergebnissen und Genehmigern.

4.2.3 Testet Änderungen vor der Umsetzung und führt bei Bedarf Rollback-Schritte durch.

4.2.4 Informiert betroffene Benutzer vor und nach wesentlichen Änderungen.

[ ... 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 Jährliche Überprüfung

9.1.1 Diese Richtlinie muss jährlich durch den Geschäftsführer oder den benannten IT-Ansprechpartner überprüft werden, um die Ausrichtung an aktuellen Systemen, Arbeitsabläufen und regulatorischen Anforderungen sicherzustellen.

### 9.2 Anlassbezogene Überprüfungen

#### 9.2.1 Überprüfungen müssen außerdem ausgelöst werden durch:

9.2.1.1 Informationssicherheitsvorfälle, die durch mangelhafte Änderungssteuerung verursacht wurden

9.2.1.2 Einführung neuer IT-Systeme

9.2.1.3 Änderungen relevanter Standards wie ISO, NIS2 oder DORA

### 9.3 Dokumentation von Aktualisierungen

9.3.1 Änderungen an dieser Richtlinie müssen versionskontrolliert und vom Geschäftsführer genehmigt werden. Jede Version muss Datum, Zusammenfassung der Änderungen und Genehmiger festhalten.

### 9.4 Kommunikation der Richtlinie

9.4.1 Alle Aktualisierungen müssen allen betroffenen Mitarbeitern und externen Dienstleistern mitgeteilt werden. Die Dokumentation muss an allen Referenzstellen aktualisiert werden (z. B. Mitarbeiterportal, gemeinsame Laufwerke).

## 10. Zugehörige Richtlinien und Verknüpfungen

### 10.1 Diese Richtlinie steht in engem Zusammenhang mit den folgenden SME-Richtlinien:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert die Genehmigungsbefugnis für Änderungen.

10.1.2 P4S – Zugriffskontrollrichtlinie: Stellt sicher, dass Zugriffsänderungen infolge von Änderungen dokumentiert und korrekt umgesetzt werden.

10.1.3 P7S – Richtlinie für Onboarding und Offboarding: Koordiniert Änderungen im Zusammenhang mit Rollenwechseln und der Vergabe von Zugriffsberechtigungen.

10.1.4 P15S – Richtlinie für Backup und Wiederherstellung: Stellt sicher, dass Rollback- und Wiederherstellungsschritte ausgeführt werden können, wenn eine Änderung fehlschlägt.

10.1.5 P30S – Incident-Response-Richtlinie: Regelt, wie fehlgeschlagene oder nicht autorisierte Änderungen als Informationssicherheitsvorfälle behandelt werden.

## 11. Referenzstandards und Rahmenwerke

### 11.1 ISO/IEC 27001

11.1.1 Klausel 6.1 – Die risikobasierte Planung muss Änderungsaktivitäten einschließen.

11.1.2 Klausel 8.1 – Betriebliche Kontrollen müssen bei änderungsbezogenen Aktivitäten konsistent angewendet werden, um die Serviceintegrität sicherzustellen.

### 11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.32 – Gibt Leitlinien für sichere Änderungsmanagementprozesse einschließlich Dokumentation, Tests und Genehmigung vor.

### 11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Basiskonfiguration für Systeme vor der Änderung.

11.3.2 CM-3 – Kontrolle von Konfigurationsänderungen.

11.3.3 CM-4 – Analyse der Sicherheitsauswirkungen.

11.3.4 CM-5 – Änderungsgenehmigung und Dokumentation.

11.3.5 CM-11 – Audit und Überwachung von Änderungen.

### 11.4 EU-NIS2-Richtlinie

11.4.1 Artikel 21(2)(b) – Verlangt formale Verfahren für technische und organisatorische Sicherheitsmaßnahmen, einschließlich Änderungsmanagement.

### 11.5 EU DORA

11.5.1 Artikel 6(9) und 8(4)(b) – Verlangen von Finanzunternehmen, Änderungs- und Konfigurationsmanagement für IKT-Systeme aufrechtzuerhalten.

### 11.6 COBIT 2019

11.6.1 BAI06 – Änderungen verwalten: Betont Planung, Risikobewertung und Rollback-Fähigkeit.

11.6.2 DSS01 – Betrieb verwalten: Stellt die betriebliche Integrität bei technischen Übergängen und Änderungen sicher.