# **Change** **Management Policy**

**Version:** 1.0

**Datum:** [Einfügedatum]

**Verantwortlich:** SOC Manager

**Genehmigt durch:** [Name des Sicherheitsbeauftragten]

## **1. Zweck der Policy**

Diese Change Management Policy beschreibt die Prozesse und Verfahren zur Identifikation, Planung, Genehmigung, Umsetzung und Überwachung von Änderungen an der Infrastruktur, den Tools und Prozessen des Security Operations Centers (SOC). Ziel ist es, potenzielle Risiken zu minimieren, die Stabilität und Sicherheit des SOC zu gewährleisten und die Einhaltung regulatorischer Anforderungen sicherzustellen.

## **2. Geltungsbereich**

Diese Policy gilt für alle Mitarbeiter, Drittanbieter und Partner, die Änderungen an den SOC-Systemen oder -Prozessen vornehmen. Sie umfasst folgende Bereiche:

• Software- und Hardwareänderungen.

• Änderungen an Sicherheitsrichtlinien, Playbooks und Prozessen.

• Updates oder Upgrades an SOC-Tools (z. B. SIEM, SOAR).

• Änderungen an der Netzwerk- und Infrastrukturkonfiguration.

## **3. Ziele**

1. Sicherstellung, dass alle Änderungen strukturiert und kontrolliert durchgeführt werden.
2. Vermeidung von Ausfallzeiten oder Sicherheitsrisiken durch nicht autorisierte Änderungen.
3. Dokumentation und Nachverfolgbarkeit aller Änderungen.
4. Förderung der Kommunikation zwischen Teams, die von Änderungen betroffen sind.

## **4. Rollen und Verantwortlichkeiten**

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeiten** |
| Change Initiator | Identifiziert die notwendige Änderung, erstellt den Änderungsantrag (Change Request). |
| **Change Manager** | Überwacht den gesamten Änderungsprozess, koordiniert Genehmigungen und Implementierung. |
| **Change Advisory Board (CAB)** | Prüft und genehmigt Änderungen, bewertet potenzielle Risiken und Auswirkungen. |
| **Implementierungsteam** | Führt die genehmigten Änderungen gemäß dem festgelegten Plan durch. |
| **SOC Manager** | Stellt sicher, dass die Policy eingehalten wird und dokumentiert alle Änderungen. |

## **5. Änderungsprozess**

**5.1 Änderungsantrag (Change Request)**

* **Beschreibung:** Der Change Initiator erstellt einen Änderungsantrag im Change-Management-Tool oder per Vorlage.

• **Inhalt des Antrags:**

• Beschreibung der geplanten Änderung.

• Grund für die Änderung.

• Betroffene Systeme und Prozesse.

• Risikobewertung und potenzielle Auswirkungen.

• Rollback-Plan für den Fall einer Fehlfunktion.

**5.2 Bewertung und Genehmigung**

• Änderungen werden vom CAB bewertet, wobei folgende Kriterien berücksichtigt werden:

• Kritikalität der Änderung.

• Risiko für den SOC-Betrieb.

• Übereinstimmung mit den Sicherheitsrichtlinien.

• Genehmigungen erfolgen durch den Change Manager und die relevanten Stakeholder.

**5.3 Implementierung**

* Änderungen werden außerhalb der Geschäftszeiten durchgeführt, um Störungen zu minimieren.

• Dokumentation aller durchgeführten Schritte, einschließlich Testprotokolle.

• Kommunikation an alle betroffenen Teams vor und nach der Implementierung.

**5.4 Überwachung und Überprüfung**

• Nach Abschluss der Änderung wird die Funktionalität der Systeme überprüft.

• Bei Problemen wird der Rollback-Plan ausgeführt.

* Eine Post-Implementation Review (PIR) wird durchgeführt, um den Erfolg der Änderung zu bewerten.

## **6. Notfalländerungen**

* Notfalländerungen (z. B. für die Behebung kritischer Sicherheitslücken) dürfen ohne vorherige CAB-Genehmigung durchgeführt werden.
* Der SOC Manager muss alle Notfalländerungen dokumentieren und zur nachträglichen Bewertung an den CAB weiterleiten.

## **7. Eskalation**

* Änderungen, die potenziell hohe Risiken bergen oder mehrere Teams betreffen, werden direkt an die Geschäftsführung eskaliert.
* Der Change Manager koordiniert die Eskalation und informiert alle relevanten Stakeholder.

## **8. Überprüfung und Aktualisierung**

• Diese Policy wird jährlich überprüft und bei Bedarf aktualisiert.

• Änderungen an der Policy werden durch den SOC Manager und den CAB genehmigt.

## **9. Dokumentation und Tools**

• Alle Änderungen werden in einem zentralen Change-Management-Tool dokumentiert.

* Tools wie Jira, ServiceNow oder ein internes SOC-Dokumentationssystem werden empfohlen.

## **10. Compliance**

Diese Policy stellt die Einhaltung folgender Standards sicher:

• ISO/IEC 27001: Informationssicherheits-Managementsystem.

• NIS2: Netzwerk- und Informationssicherheit.

• DORA: Digital Operational Resilience Act.