| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P38 | | | | | Dokumenttitel:<br>**Richtlinie für sichere Kommunikation und Multi-Faktor-Authentifizierung** | | | | | | | |
| 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** |
| | | | |
| | | | |

Ausgerichtet an Standards und Vorschriften

| Standard/Regulation | Clause/Article | Comment |
|---|---|---|
| ISO/IEC 27001:2022 | 5.30, 5.31, 8.24 | |
| ISO/IEC 27002:2022 | 5.15, 5.17, 5.18, 8.24, 8.28 | |
| NIST SP 800-53 Rev.5 | IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31 | |
| EU GDPR | Art. 32(1)(b) | |
| EU NIS2 | Art. 21(2)(j) | |
| EU DORA | Art. 9(2)(d), Art. 11 | |
| COBIT 2019 | DSS05.04, DSS05.05, DSS05. | |

**1. Zweck**

1.1 Festlegung der Anforderungen für den Einsatz von Multi-Faktor-Authentifizierung oder kontinuierlicher Authentifizierung für den Systemzugriff im Einklang mit Artikel 21 Absatz 2 Buchstabe j der NIS2-Richtlinie.

1.2 Festlegung von Kontrollen für gesicherte Sprach-, Video-, Text- und Notfallkommunikation zum Schutz der Vertraulichkeit und Integrität von Informationen.

**2. Geltungsbereich**

2.1 Diese Richtlinie gilt für alle Authentifizierungsmechanismen und Kommunikationssysteme (Sprachanrufe, Videokonferenzlösungen, Messaging- und Notfallbenachrichtigungssysteme), die von der Organisation verwendet werden.

2.2 Sie gilt für alle Mitarbeitenden und Auftragnehmer sowie für alle externen Parteien, die die Kommunikationskanäle der Organisation nutzen oder auf deren Netzwerke und Informationssysteme zugreifen.

**3. Ziele**

3.1 Sicherstellung, dass nur angemessen authentifizierte Benutzer Zugriff auf Systeme erhalten, und Reduzierung des Risikos unbefugten Zugriffs durch die Umsetzung von Multi-Faktor-Authentifizierung.

3.2 Gewährleistung, dass interne Kommunikation und Notfallkommunikation über sichere Verfahren (z. B. verschlüsselte Kommunikationskanäle) übertragen werden, um Abhören oder Manipulation zu verhindern.

3.3 Erfüllung der Anforderungen der NIS2-Richtlinie an starke Authentifizierung und sichere Kommunikation zur Stärkung der allgemeinen Cyberresilienz.

**4. Rollen und Verantwortlichkeiten**

4.1 CISO / Informationssicherheit: Definition und Pflege von MFA-Mechanismen und sicheren Kommunikationsmitteln; Sicherstellung der technischen Durchsetzung dieser Richtlinie.

4.2 IT-Administratoren: Umsetzung von MFA für relevante Systeme und Konfiguration genehmigter sicherer Kommunikationsplattformen; Überwachung der Einhaltung.

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

**9. Überwachung und Audit**

9.1 Die Informationssicherheit hat Authentifizierungsprotokolle fortlaufend auf Anmeldeversuche mit nur einem Faktor oder auf anomale MFA-Fehlschläge zu überwachen. Protokolle sicherer Kommunikationssysteme sind, soweit anwendbar, auf unbefugte Zugriffsversuche oder Konfigurationsänderungen zu überwachen.

9.2 Die Interne Revision und die Compliance-Funktion überprüfen jährlich die Einhaltung der Anforderungen an die MFA-Umsetzung (insbesondere, dass alle kritischen Systeme MFA durchsetzen) und verifizieren, dass für sensible Kommunikation ausschließlich genehmigte sichere Kanäle genutzt werden. Feststellungen werden der Geschäftsleitung zusammen mit Empfehlungen berichtet.

**10. Überprüfung und Pflege**

10.1 Diese Richtlinie wird mindestens jährlich sowie nach jedem wesentlichen Sicherheitsvorfall oder neu identifizierten Risiko im Zusammenhang mit Authentifizierung oder Kommunikation überprüft (z. B. neue Bedrohungsvektoren gegen MFA oder Feststellung unsicherer Kommunikationsnutzung).

10.2 Überarbeitungen erfolgen nach Bedarf, um technologische Entwicklungen zu berücksichtigen (z. B. Einführung robusterer Lösungen zur kontinuierlichen Authentifizierung) oder aktualisierte regulatorische Vorgaben einzuhalten (z. B. künftige ENISA-Empfehlungen zur sicheren Kommunikation).

**11. Verwandte Richtlinien und Verknüpfungen**

11.1 P01 – Informationssicherheitsrichtlinie. Legt unternehmensweite Schutzmaßnahmen für Authentifizierung und Kommunikation fest.

11.2 P04 – Richtlinie zur Zugriffskontrolle. Etabliert die Zugriffsgovernance, die durch MFA nach P38 durchgesetzt wird.

11.3 P11 – Richtlinie zur Verwaltung von Benutzerkonten und Berechtigungen. Verknüpft MFA mit dem Lebenszyklus privilegierter Zugriffe.

11.4 P18 – Richtlinie zu kryptografischen Kontrollen. Legt genehmigte kryptografische Verfahren sowie das Schlüsselmanagement für sichere Kommunikation fest.

11.5 P21 – Netzwerksicherheitsrichtlinie. Schützt die für Sprach-, Video- und Messaging-Kommunikation genutzten Übertragungskanäle.

11.6 P22 – Richtlinie zur Protokollierung und Überwachung. Überwacht Authentifizierungsereignisse und die Nutzung sicherer Kanäle.

11.7 P32 – Richtlinie zu Business Continuity und Disaster Recovery. Schützt die Notfallkommunikation in Krisensituationen.

11.8 P08 – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit. Schult Benutzer zu MFA und zur sicheren Nutzung von Kommunikationskanälen.

**12. Referenzen**

12.1 NIS2-Richtlinie (EU 2022/2555), Artikel 21 Absatz 2 Buchstabe j (Verwendung von Multi-Faktor-Authentifizierung und gesicherter Kommunikation)

12.2 Durchführungsverordnung (EU) 2024/2690 der Kommission, Anhang, Abschnitt 11 (Anforderungen an die Zugriffskontrolle, einschließlich MFA für privilegierte Konten)

12.3 ISO/IEC 27001:2022 und ISO/IEC 27002:2022