Richtlinie zur Netzwerksicherheit

- Musterbeispiel -

Versionsnummer: Draft 0.9
Freigabedatum durch das Leitungsorgan: 17.01.2025

Inhalt

Änderungshistorie

Datum	Version	Beschreibung der Änderimg	Grund für die Änderung	Autor
17.01.2025	0.9	Initiale Erstellung	Erstellung eines Templates für eine Richtlinie zur Netzwerksicherheit gemäß DORA-VO	M. Hofmann

1 Einleitung

1.1 Zweck der Richtlinie

Diese Richtlinie soll die Netzwerksicherheit innerhalb der Organisation gewährleisten, um die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen und Dienste zu schützen. Ziel ist es, den Netzwerkzugriff zu sichern, Schwachstellen zu minimieren und Bedrohungen frühzeitig zu erkennen und abzuwehren.

1.2 Geltungsbereich

Diese Richtlinie gilt für alle Abteilungen und Mitarbeiter, die das Netzwerk der Organisation nutzen oder auf sensible Informationen und Systeme zugreifen. Sie umfasst sowohl physische Netzwerkkomponenten als auch virtuelle und Cloud-basierte Netzwerkressourcen.

1.3 Bezug zur DOR-Strategie

Die Richtlinie unterstützt die Ziele der DOR-Strategie, indem sie Maßnahmen zur Sicherstellung der kontinuierlichen Netzwerksicherheit implementiert und die Erfüllung regulatorischer Anforderungen (z.B. DORA) sicherstellt.

1.4 Grundsätze der Proportionalität

Die Anforderungen der Netzwerksicherheitsrichtlinie werden entsprechend der Größe, des Risikoprofils und der Komplexität der Organisation angepasst.

2 Dokumentenlenkung

2.1 Änderung & Überprüfung

Die Netzwerksicherheitsrichtlinie wird mindestens einmal jährlich überprüft und bei Bedarf angepasst, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen und regulatorischen Standards entspricht. Das Leitungsorgan hat die damit verbundenen operativen Aufgaben an das Team Netzwerk-Infrastruktur delegiert. Erforderliche Änderungen an der Richtlinie werden von diesem Team ausgearbeitet und zur Genehmigung vorlegt.

2.2 Genehmigung und Freigabe

Das Leitungsorgan trägt die Verantwortung für die Genehmigung und Freigabe der Netzwerksicherheitsrichtlinie. Das formale Freigabedatum wird in der Richtlinie dokumentiert.

2.3 Veröffentlichung

Die Richtlinie wird gemäß der internen Prozesse zur Dokumentenlenkung veröffentlicht und allen relevanten Mitarbeitern zugänglich gemacht.

3 Einhaltung und Kontrolle der Vorgaben

Die Einhaltung der Vorgaben dieser Richtlinie wird im Rahmen des Internen Kontrollsystems überwacht und durch Implementierungsindikatoren gemessen.

3.1 Risiken und Kontrollen

Technische oder organisatorische Schwachstellen im Bereich Netzwerksicherheit können zu inakzeptablen Risiken für die Organisation führen. Die nachfolgenden Schlüsselkontrollen wirken den wesentlichen Risiken entgegen, die mit einer unzureichenden Beachtung der Vorgaben dieser Richtlinie verbunden sein können.

Risiko	**Kontrolle**
Unbefugter Zugriff auf kritische Netzwerkelemente und sensible Daten durch fehlerhafte oder absichtlich umgangene Authentifizierungs- und Zugangskontrollen	Implementierung eines umfassenden Audit-Prozesses zur regelmäßigen Überprüfung der Zugriffsrechte und Berechtigungen aller Netzwerknutzer und -rollen, um die Einhaltung der Authentifizierungsrichtlinien sicherzustellen.
Aktualitätsverlust der Netzwerksicherheitsvorgaben und unzureichende technisch-organisatorische Schutzmaßnahmen	Jährlicher Prüfprozess, der sicherstellt, dass die Netzwerksicherheitsrichtlinie sowie deren technische und organisatorische Umsetzung mit aktuellen Sicherheitsstandards und dem Stand der Technik übereinstimmen.
Gefährdung der Rückverfolgbarkeit und Nichteinhaltung der Richtlinie aufgrund fehlender Transparenz bei sicherheitsrelevanten Netzwerkänderungen	Sicherstellung einer vollständigen und revisionssicheren Dokumentation aller sicherheitsrelevanten Änderungen im Netzwerk im Rahmen des Change-Managements, um Transparenz und Compliance zu wahren.

3.2 Implementierungsindikatoren

Die Implementierungsindikatoren umfassen spezifische Messgrößen, um den Fortschritt und die Einhaltung der Netzwerksicherheitsrichtlinie zu überwachen. Diese Indikatoren werden kontinuierlich analysiert und bei Bedarf angepasst.

Implementierungsindikator	Formel	Zielwert
Anteil der Systeme mit regelmäßigen Sicherheitsupdates und Patch-Management: Misst den Anteil der regelmäßig gepatchten Netzwerkkomponenten, um Angriffsrisiken zu minimieren.	$\text{Patch-Compliance-Rate} = \frac{\text{Anzahl der gepatchten Netzwerkgeräte}}{\text{Gesamtzahl der Netzwerkgeräte}} \times 100$	≥ 95%
Anzahl der Zugriffsverletzungen pro Quartal: Überwacht unautorisierte Zugriffsversuche, um Sicherheitslücken frühzeitig zu erkennen.	$\text{Zugriffsverletzungsrate} = \frac{\text{Anzahl der unautorisierten Zugriffsversuche}}{\text{Gesamtzahl der Zugriffe pro Quartal}} \times 100$	≤ 2%
Anteil der Netzwerkgeräte mit aktivierter MFA für privilegierte Zugriffe: Stellt sicher, dass privilegierte Zugriffe mit MFA abgesichert sind.	$\text{MFA-Implementierungsrate} = \frac{\text{Anzahl der Geräte mit aktivierter MFA}}{\text{Gesamtzahl der MFA-fähigen Geräte}} \times 100$	100%

3.3 Maßnahmen bei Nichteinhaltung

Nichtbeachtung der Richtlinie führt zu disziplinarischen Maßnahmen, die von Schulungen bis zu rechtlichen Konsequenzen reichen können, abhängig vom Schweregrad des Verstoßes.

4 Hauptteil: Vorgaben im Bereich Netzwerksicherheit

4.1 Definitionen

Ein **Netzwerk** ist ein Verbund aus Hardware- und Softwarekomponenten, der darauf abzielt, den Austausch und die gemeinsame Nutzung von Daten und Ressourcen zwischen verschiedenen Geräten und Benutzern zu ermöglichen.

Netzwerkkomponenten sind technische Bausteine eines Netzwerks, die den Datenaustausch zwischen Geräten ermöglichen, z. B. Router, Switches, Firewalls und Netzwerkprotokolle. Sie sichern eine verlässliche Kommunikation und unterstützen Unternehmensprozesse.

Netzwerkzugriff ist die Berechtigung, auf Netzwerkressourcen und -dienste zuzugreifen, geregelt durch Maßnahmen wie Zugangskontrollen und Multi-Faktor-Authentifizierung (MFA), um die Integrität und Vertraulichkeit der Daten zu schützen.

Netzwerknutzer sind Personen oder Systeme, die berechtigten Zugriff auf Netzwerkressourcen wie Dateien, Anwendungen oder Dienste haben. Sie werden durch Zugriffsrechte und Sicherheitsmaßnahmen verwaltet, um autorisierte Aktivitäten sicherzustellen und den Schutz des Netzwerks zu gewährleisten.

Netzwerkadministrator ist eine Person, die für die Verwaltung, Überwachung und Sicherstellung des sicheren Betriebs eines Netzwerks verantwortlich ist. Zu den Aufgaben gehören die Konfiguration und Wartung von Netzwerkkomponenten wie Routern, Switches und Firewalls sowie das Einrichten und Überwachen von Sicherheitsrichtlinien und Zugriffsrechten. Netzwerkadministratoren gewährleisten durch diese Maßnahmen die Verfügbarkeit, Vertraulichkeit und Integrität der Netzwerkressourcen.

Netzwerküberwachung ist das kontinuierliche Monitoring von Netzwerkaktivitäten, um Leistung, Sicherheit und Verfügbarkeit sicherzustellen, Bedrohungen frühzeitig zu erkennen und Sicherheitsvorgaben einzuhalten.

Multi-Faktor-Authentifizierung (MFA) kombiniert mindestens zwei Authentifizierungsfaktoren (z. B. Passwort und Fingerabdruck), um unbefugte Zugriffe zu verhindern und die Sicherheit in sensiblen Systemen zu erhöhen.

Verschlüsselung wandelt Daten mithilfe eines Algorithmus in eine unlesbare Form um, die nur mit einem Entschlüsselungsschlüssel zugänglich ist, um Vertraulichkeit und Integrität der Daten zu gewährleisten.

Netzwerk-Segmentierung teilt ein Netzwerk in isolierte Subnetze, um den Datenfluss zwischen diesen Netzen zu begrenzen und sensible Daten und Ressourcen zu schützen. Dies erhöht die Sicherheit und erleichtert die Netzwerkverwaltung.

4.2 Rollen und Verantwortlichkeiten

4.2.1 Netzwerknutzer

Aufgaben	Kompetenzen	Verantwortlichkeiten
• Sicherer Zugang und Nutzung des Netzwerks gemäß Richtlinie • Schutz des eigenen Endgeräts durch regelmäßige Updates und Antivirus-Software • Umgang mit sicherheitsrelevanten Tools, z.B. VPN-Nutzung	• Grundkenntnisse in Sicherheitsanforderungen und Netzwerkrichtlinien • Fähigkeit, Bedrohungen wie Phishing zu erkennen und zu melden	• Einhaltung aller Zugangs- und Nutzungsvorgaben • Meldung von verdächtigen Aktivitäten an die interne Meldestelle • Sicherstellung der Vertraulichkeit und Integrität verarbeiteter Daten

4.2.2 Netzwerkadministrator

Aufgaben	Kompetenzen	Verantwortlichkeiten
• Umsetzung der Netzwerksicherheitsrichtlinie • Berücksichtigung externer Vorgaben sowie Best Practices und Standards • Sicherstellung der Einhaltung der Sicherheitsanforderungen durch Dienstleister • Überwachung der Umsetzung im Netzwerkbetrieb • Management von Bedrohungen, Schwachstellen und Risiken im Netzwerk	• Kenntnis rechtlicher und regulatorischer Anforderungen im Bereich Netzwerksicherheit • Expertise in Best Practices und Standards für Netzwerksicherheit • Festlegung der zu implementierenden Netzwerksicherheits-maßnahmen	• Implementierung und Durchsetzung der Netzwerksicherheitsrichtlinie • Überwachung und Steuerung der Dienstleister im Netzwerkbetrieb

4.2.3 IKT-Risikokontrollfunktion

Aufgaben	Kompetenzen	Verantwortlichkeiten
• Überwachung der Einhaltung der Netzwerksicherheitsrichtlinie durch Einheiten und Dienstleister • Regelmäßige Überprüfung der Konformität mit regulatorischen Anforderungen • Identifikation von Abweichungen und Einleitung von Korrekturmaßnahmen	• Kompetenz zur Durchführung von Soll-Soll-Vergleichen und Risikobewertungen • Kompetenz zur Vergabe von internen Feststellungen und Verfolgung von Korrekturmaßnahmen • Berichtskompetenz zum Leitungsorgan	• Implementierung und Durchsetzung der Netzwerksicherheits-richtlinie • Überwachung und Steuerung der Dienstleister im Netzwerkbetrieb

4.3 Segregation of Duties

Die Sicherstellung einer sachgerechten Trennung von Verantwortlichkeiten im Kontext Netzwerksicherheit wird wie folgt umgesetzt:

- In der ersten Verteidigungslinie ist das Team für Netzwerk-Infrastruktur verantwortlich für die Erstellung und Umsetzung der Netzwerksicherheitsrichtlinie. Dabei berücksichtigt das Team externe rechtliche und regulatorische Vorgaben sowie relevante Best Practices und Standards. Zusätzlich sorgt es dafür, dass alle beteiligten Dienstleister die festgelegten Sicherheitsanforderungen einhalten und überwacht deren Umsetzung im Netzwerkbetrieb. Das Leitungsorgan überprüft und bestätigt die Richtlinie, wobei es die Angemessenheit und Übereinstimmung mit den strategischen Zielen und regulatorischen Anforderungen sicherstellt. Gemäß Artikel 5(2) DORA wird die Freigabe durch das Leitungsorgan dokumentiert.
- Die IKT-Risikokontrollfunktion in der zweiten Verteidigungslinie überwacht die Einhaltung der Netzwerksicherheitsrichtlinie durch alle betroffenen Einheiten und Dienstleister und überprüft regelmäßig die Konformität mit regulatorischen Anforderungen im Rahmen von Soll-Soll-Vergleichen. Dabei werden mögliche Schwachstellen oder Abweichungen identifiziert, und Maßnahmen zur Behebung werden initiiert.
- Die Interne Revision bildet die dritte Verteidigungslinie und bewertet regelmäßig und anlassbezoggen die Angemessenheit und Einhaltung der Netzwerksicherheitsrichtlinie sowie die Wirksamkeit der implementierten Kontrollen. Dies erfolgt im Rahmen unabhängiger Audits, um eine objektive und umfassende Prüfung sicherzustellen.

4.4 Standards und Best Practices

Die Ausgestaltung der technisch-organisatorischen Maßnahmen im Bereich Netzwerksicherheit erfolgt in Anlehnung an folgende Standards:

- ISO/IEC 27002
- CIS Controls v8
- NIST Cybersecurity Framework
- BSI Grundschutz

Die Standards dienen dabei nicht als starre Vorgaben, sondern werden situativ und bedarfsorientiert herangezogen, um bei der Ausgestaltung konkreter Implementierungsoptionen eine optimale Anpassung an die spezifischen Sicherheitsanforderungen zu gewährleisten.

4.5 Grundsätze der Netzwerksicherheit

4.5.1 Netzwerksegmentierung

IKT-Systeme und Netzwerke sind so zu trennen und zu segmentieren, dass Sicherheitsvorfälle lokal begrenzt bleiben und sich nicht auf andere Netzwerkbereiche ausweiten können. Dafür sind physische und logische Trennungen einzurichten, die den Zugang zu sensiblen Bereichen streng kontrollieren und beschränken (vgl. DORA-VO, Artikel 13(a) RTS Risk Management).

4.5.2 Netzwerkdokumentation

Alle Netzwerkverbindungen und Datenflüsse sind vollständig zu dokumentieren, um Transparenz über die Kommunikationswege innerhalb der Netzwerkinfrastruktur zu gewährleisten. Diese Dokumentation dient dazu, potenzielle Sicherheitslücken frühzeitig zu erkennen und geeignete Maßnahmen zu ermöglichen (vgl. DORA-VO, Artikel 13(b) RTS Risk Management).

4.5.3 Dedizierte Administrationsnetzwerke für IKT-Assets

Die Administration von IKT-Assets ist über ein separates, dediziertes Netzwerk durchzuführen, um den Schutz administrativer Zugriffe auf kritische Systeme zu gewährleisten. Diese Isolation minimiert das Risiko unbefugter Zugriffe und Datenmissbrauchs und sichert die IKT-Assets umfassend ab (vgl. DORA-VO, Artikel 13(c) RTS Risk Management).

4.5.4 Kontrollen für den Zugriffsschutz im Netzwerk

Es sind Maßnahmen einzurichten, die verhindern und erkennen, wenn nicht autorisierte Geräte oder Systeme sowie Endgeräte, die die Sicherheitsanforderungen nicht erfüllen, eine Verbindung zum Netzwerk herstellen. Diese Kontrollen sollen unerlaubte Zugriffe schnell identifizieren und blockieren, um die Sicherheit des Netzwerks zu gewährleisten (vgl. DORA-VO, Artikel 13(d) RTS Risk Management).

4.5.5 Verschlüsselung von Netzwerkverbindungen zur Sicherung sensibler Daten

Es ist sicherzustellen, dass Netzwerkverbindungen über Unternehmensnetzwerke, öffentliche Netzwerke, interne Netzwerke, Drittanbieternetze und drahtlose Netzwerke risikoorientiert verschlüsselt werden. Dabei sind die Ergebnisse der Datenklassifizierung, der IKT-Risikobewertung sowie die festgelegten Verschlüsselungsanforderungen gemäß der Richtlinie zu kryptografischen Kontrollen zu berücksichtigen. Diese Verschlüsselung dient dem Schutz der Vertraulichkeit und Sicherheit sensibler Daten während der Übertragung und sichert das Netzwerk vor unbefugtem Zugriff und Datenmissbrauch (vgl. DORA-VO, Artikel 13(e) RTS Risk Management).

4.5.6 Netzwerkdesign

Es ist ein Netzwerkdesign sicherzustellen, das den IKT-Sicherheitsanforderungen und führenden Praktiken entspricht. Dieses Design muss Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks gewährleisten und eine robuste, widerstandsfähige Netzwerkumgebung schaffen (vgl. DORA-VO, Artikel 13(f) RTS Risk Management).

4.5.7 Schutzmaßnahmen für sicheren Netzwerkverkehr

Es ist sicherzustellen, dass der Netzwerkverkehr zwischen internen Netzwerken und externen Verbindungen geschützt erfolgt. Dafür sind Maßnahmen wie der Einsatz von Firewalls, Netzwerksegmentierung, Intrusion-Detection-Systemen und verschlüsselten Tunnelprotokollen (z. B. VPNs) zu implementieren. Diese Maßnahmen sollen die Sicherheit der Datenübertragung gewährleisten und das Risiko unbefugten Zugriffs oder einer Datenkompromittierung minimieren (vgl. DORA-VO, Artikel 13(g) RTS Risk Management).

4.5.8 Rollen und Verantwortlichkeiten im Firewall-Management

Es sind klare Rollen und Verantwortlichkeiten für die Festlegung, Implementierung, Genehmigung, Änderung und regelmäßige Überprüfung von Firewall-Regeln und Verbindungsfiltern zu definieren. Diese Zuweisung soll sicherstellen, dass alle Aktivitäten im Bereich Netzwerkzugriff strukturiert und kontrolliert ablaufen, um die Sicherheit der Netzwerkumgebung zu gewährleisten und unbefugte Zugriffe zu verhindern (vgl. DORA-VO, Artikel 13(h) RTS Risk Management).

4.5.9 Jährliche Überprüfung der Netzwerkinfrastruktur und des Sicherheitsdesigns

Es sind jährliche Überprüfungen der Netzwerkinfrastruktur und des Sicherheitsdesigns durchzuführen, um potenzielle Schwachstellen frühzeitig zu identifizieren. Diese regelmäßigen Prüfungen sollen sicherstellen, dass Sicherheitsrisiken proaktiv erkannt und notwendige Maßnahmen zur Stärkung der Netzwerkumgebung ergriffen werden (vgl. DORA-VO, Artikel 13(i) RTS Risk Management).

4.5.10 Maßnahmen zur Isolation von Netzwerkkomponenten und Subnetzwerken

Es sind Maßnahmen festzulegen, um bei Bedarf Subnetzwerke, Netzwerkkomponenten und Geräte vorübergehend zu isolieren. Diese Isolationsmaßnahmen sollen sicherstellen, dass potenzielle Sicherheitsvorfälle eingedämmt und Bedrohungen schnell kontrolliert werden, um die Integrität und Verfügbarkeit des Netzwerks zu schützen (vgl. DORA-VO, Artikel 13(j) RTS Risk Management).

4.5.11 Sichere Konfiguration und Härtung von Netzwerkkomponenten

Es ist eine sichere Konfigurationsgrundlage für alle Netzwerkkomponenten zu etablieren und das Netzwerk sowie die Geräte gemäß den Herstelleranweisungen, geltenden Standards und bewährten Praktiken zu härten. Diese Maßnahmen sollen sicherstellen, dass alle Netzwerkressourcen gegen bekannte Schwachstellen geschützt und auf dem neuesten Sicherheitsstand sind, um unbefugte Zugriffe und Sicherheitsvorfälle zu minimieren (vgl. DORA-VO, Artikel 13(k) RTS Risk Management).

4.5.12 Begrenzung und Sperrung von Sitzungen

Es sind Verfahren zu etablieren, um System- und Remote-Sitzungen nach einer festgelegten Inaktivitätszeit automatisch zu sperren und gegebenenfalls zu beenden. Diese Maßnahmen sollen verhindern, dass durch verlassene Sitzungen unbefugte Zugriffe entstehen, und die Sicherheit der Netzwerkumgebung stärken (vgl. DORA-VO, Artikel 13(l) RTS Risk Management).

4.5.13 Netzwerksicherheit in IKT-Verträgen

Es ist sicherzustellen, dass alle Netzwerksicherheitsanforderungen in IKT-Verträgen zur Bereitstellung und zum Betrieb von Netzwerkservices festgelegt und vertraglich geregelt sind. Dabei sind IKT- und Informationssicherheitsmaßnahmen, Service-Level-Vereinbarungen sowie Managementanforderungen für Netzwerkdienstleistungsverträge klar zu definieren und festzulegen. Diese Maßnahme soll gewährleisten, dass Drittanbieter und Dienstleister die definierten Sicherheitsstandards einhalten und die Integrität der Netzwerkumgebung gewahrt bleibt (vgl. DORA-VO, Artikel 13(m) RTS Risk Management).

4.5.14 Netzwerkservices durch interne oder externe Dienstleister

Es ist im IKT-Vertrag zu dokumentieren, ob Netzwerkdienste von einem gruppeninternen IKT-Dienstleister oder von einem externen IKT-Dienstleister bereitgestellt werden. Diese Dokumentation erzeugt Transparenz über die anzuwendende Governance und trägt zu einer klaren Zuständigkeitsverteilung und bei (vgl. DORA-VO, Artikel 13(m) RTS Risk Management).

4.5.15 Sicherstellung einer zuverlässigen und schnellen Datenübertragung

Es sind Verfahren, Protokolle und Tools einzurichten, die eine präzise und schnelle Datenübertragung sicherstellen und dabei größere Unterbrechungen oder unangemessene Verzögerungen vermeiden. Diese Maßnahmen sollen eine stabile Netzwerkkommunikation gewährleisten und die Leistungsfähigkeit der Netzwerkumgebung unterstützen (vgl. DORA-VO, Artikel 2(1d) RTS Risk Management).

4.5.16 Schutz von Informationen bei der Datenübertragung

Es ist sicherzustellen, dass Informationen während der Übertragung geschützt sind, beispielsweise durch Verschlüsselung von Daten in Transit. Diese Maßnahme soll gewährleisten, dass die Vertraulichkeit und Integrität sensibler Daten bei der Übertragung gewahrt bleiben und unbefugter Zugriff verhindert wird (vgl. DORA-VO, Artikel 14(1) RTS Risk Management).

4.5.16.1 Sicherstellung der Datensicherheit während der Netzwerkübertragung

Es sind Maßnahmen zur Sicherstellung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten während der Netzwerkübertragung umzusetzen. Zusätzlich sind Verfahren einzurichten, um regelmäßig die Einhaltung dieser Anforderungen zu überprüfen und sicherzustellen, dass die übertragenen Daten jederzeit zuverlässig und sicher geschützt sind (vgl. DORA-VO, Artikel 14(1a) RTS Risk Management).

4.5.16.2 Schutz vor Datenlecks und Informationsübertragung mit externen Parteien

Es sind Maßnahmen zur Verhinderung und Erkennung von Datenlecks sowie zur sicheren Übertragung von Informationen zwischen der Institution und externen Parteien umzusetzen. Diese Maßnahmen sollen sicherstellen, dass sensible Informationen während der Übertragung geschützt sind und unbefugte Zugriffe oder Datenabflüsse frühzeitig erkannt und verhindert werden (vgl. DORA-VO, Artikel 14(1b) RTS Risk Management).

4.5.17 Berücksichtigung von Datenklassifizierung und IKT-Risikobewertung

Es ist sicherzustellen, dass der Schutz von Informationen während der Übertragung entsprechend der genehmigten Datenklassifizierung und den Ergebnissen der IKT-Risikobewertung erfolgt. Diese Maßnahmen sollen gewährleisten, dass Übertragungsanforderungen basierend auf der Sensibilität der Daten und identifizierten Risiken angepasst werden, um die Vertraulichkeit und Integrität der Informationen zu schützen (vgl. DORA-VO, Artikel 14(2) RTS Risk Management).

4.5.18 Regelmäßige Sicherheitstests über die Netzwerksicherheit

Es sind regelmäßige Sicherheitstests durchzuführen, um die Netzwerksicherheit sicherzustellen. Diese Tests sollen potenzielle Schwachstellen identifizieren und gewährleisten, dass die Netzwerkschutzmaßnahmen stets auf dem neuesten Stand und wirksam sind (vgl. DORA-VO, Artikel 25(1)).

4.6 Schulung und Kommunikation

Regelmäßige Schulungen zur Netzwerksicherheit für alle Mitarbeiter. Kommunikationsstrategien beinhalten regelmäßige Updates und Erinnerungen zur Einhaltung der Netzwerksicherheitsvorgaben.

5 Anhang

5.1 Verpflichtende Dokumentationen

- Netzwerk-Topologie und Zugriffsberechtigungen
- Protokolle über Netzwerksicherheitsüberprüfungen
- Dokumentation über die Schulungsmaßnahmen zur Netzwerksicherheit
- Ggf. weitere konkretisierende Vorgaben zur Netzwerksicherheit

5.2 Abstimmungsbeteiligte

- Team Netzwerk-Infrastruktur
- Leitungsorgan
- IKT-Risikokontrollfunktion
- Ggf. weitere Beauftragte (z.B. ISB, ZAM, BCB)