					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P21					Dokumenttitel: **Richtlinie zur Netzwerksicherheit**							
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/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	N/A
ISO/IEC 27002:2022	Maßnahmen 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
EU DSGVO	Artikel 32	N/A
EU NIS2	Artikel 21(2)(d)	N/A
EU DORA	Artikel 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Zweck

1.1 Zweck dieser Richtlinie ist es, die Anforderungen der Organisation zum Schutz ihrer internen und externen Netzwerke vor unbefugtem Zugriff, Dienstausfällen, Abfangen von Daten und Missbrauch festzulegen.

1.2 Sie stellt sicher, dass die gesamte Netzwerkinfrastruktur — einschließlich physischer, virtueller, cloudbasierter und hybrider Umgebungen — durch mehrschichtige Kontrollen wie Segmentierung, Durchsetzung von Firewall-Regeln, sicheres Routing und zentrale Überwachung geschützt wird.

1.3 Diese Richtlinie setzt Klausel 8.1 der ISO/IEC 27001 sowie die Maßnahmen 8.20 bis 8.22 aus Anhang A um und gewährleistet die Einhaltung anwendbarer gesetzlicher und regulatorischer Verpflichtungen gemäß Artikel 32 DSGVO, Artikel 21 NIS2 und Artikel 9 DORA.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Netzwerke und zugehörigen Infrastrukturkomponenten, einschließlich:

2.1.1 Router, Switches, drahtlose Zugangspunkte und Firewalls

2.1.2 Cloud-virtuelle Netzwerke (z. B. AWS VPC, Azure VNET), VPN-Konzentratoren und SD-WAN-Systeme

2.1.3 Interne LANs, demilitarisierte Zonen, Fernzugriffspfade sowie standortübergreifende Verbindungen oder Verbindungen zu Dritten

2.1.4 Unterstützende Systeme wie DNS, DHCP, Proxy-Server und Monitoring-Appliances

2.2 Diese Richtlinie ist verbindlich für sämtliches Personal und externe Dienstleister, die Netzwerke der Organisation verwalten, konfigurieren, überwachen oder an diese angebunden sind, unabhängig davon, ob dies On-Premises oder in der Cloud erfolgt.

2.3 Alle Systeme und Anwendungen, die mit den Netzwerken der Organisation verbunden sind — unabhängig von Standort oder Eigentumsverhältnissen — müssen diese Anforderungen an die Netzwerksicherheit einhalten.

3. Ziele

3.1 Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) der über Netzwerke übertragenen Daten durch starke Zugriffskontrollen, sicheres Routing und Überwachung.

3.2 Verhinderung von unbefugtem Zugriff, lateraler Bewegung und Ausnutzung vernetzter Ressourcen durch die Durchsetzung von Segmentierung, Zonenbildung und Schutz von Netzgrenzen.

3.3 Aufrechterhaltung konsistenter Netzwerkkonfigurationen auf Grundlage von Industriestandards und Bedrohungsinformationen zur Abwehr sich weiterentwickelnder Cyberbedrohungen.

3.4 Absicherung externer Kommunikation, Cloud-Konnektivität und Fernzugriffen durch verschlüsselte Kommunikationskanäle, strenge Authentifizierung und Sicherheitsprüfungen von Endpunkten.

3.5 Gewährleistung von Transparenz über Netzwerkaktivitäten durch zentrale Protokollierung, Echtzeit-Verkehrsanalyse und automatisierte Alarmierung.

3.6 Sicherstellung der regulatorischen Compliance durch Ausrichtung sämtlicher Prozesse des Netzwerkbetriebs an den Anforderungen aus ISO/IEC 27001:2022, DSGVO, NIS2, DORA und COBIT 2019.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist verantwortlich für diese Richtlinie und stellt sicher, dass sie überprüft wird und mit der übergreifenden Cybersicherheitsstrategie der Organisation abgestimmt ist.

4.1.2 Genehmigt Netzwerksegmentierungsmodelle, Firewall-Regelwerke für sensible Systeme und Ausnahmeanträge.

4.2 Leiter Netzwerksicherheit / Leiter Infrastruktursicherheit

4.2.1 Verantwortet die Architektur der Netzwerkverteidigung einschließlich Firewalls, Intrusion-Detection-/Prevention-Systemen (IDS/IPS), VPNs und sicherem Routing.

4.2.2 Beaufsichtigt Netzwerksegmentierung, VLAN-Zuweisungen, Verkehrszonierung und externe Konnektivität.

4.2.3 Stellt die fortlaufende Überprüfung der Filterung ein- und ausgehenden Verkehrs sowie die Durchsetzung von Zero-Trust-Grundsätzen über alle Netzwerkebenen sicher.

[... 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 Diese Richtlinie ist jährlich durch den Leiter Netzwerksicherheit in Zusammenarbeit mit dem CISO zu überprüfen und auf Grundlage folgender Aspekte zu aktualisieren:

9.1.1 Neu entstehende Bedrohungen (z. B. neue Angriffstechniken, Schwachstellen in Protokollen)

9.1.2 Änderungen der Infrastruktur (z. B. Cloud-Migrationen, Einführung von SD-WAN)

9.1.3 Regulatorische oder normative Änderungen mit Auswirkungen auf den Netzwerkschutz

9.1.4 Audit-Feststellungen, Trends bei Sicherheitsvorfällen oder durch Kontrollen verursachte Leistungseinbußen

9.2 Überprüfungen müssen außerdem ausgelöst werden durch:

9.2.1 Wesentliche Änderungen der Netzwerkarchitektur

9.2.2 Einführung neuer Firewall-, VPN- oder Cloud-Netzwerkplattformen

9.2.3 Außerbetriebnahme wesentlicher Assets oder vertrauenswürdiger Zonen

9.3 Aktualisierungen müssen im ISMS-Dokumentenregister dokumentiert und an folgende Stellen kommuniziert werden:

9.3.1 Infrastruktur- und Netzwerkbetrieb

9.3.2 SOC- und Security-Engineering-Teams

9.3.3 Anwendungsteams mit Systemabhängigkeiten von Netzwerkflüssen

9.3.4 Alle Drittanbieter mit aktiver Interkonnektivität

9.4 Alle vorherigen Versionen dieser Richtlinie müssen sicher archiviert und mit Hinweisen zur Versionshistorie versehen werden, um Auditierbarkeit und Nachvollziehbarkeit von Änderungen sicherzustellen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 - Richtlinie zur Informationssicherheit. Legt grundlegende Sicherheitsprinzipien fest und schreibt mehrschichtige Schutzmaßnahmen vor, einschließlich netzwerkbasierter Zugriffs- und Bedrohungskontrollen.

10.2 P4 - Richtlinie zur Zugriffskontrolle. Stellt sicher, dass Netzwerksegmentierung im Einklang mit Benutzerrollen, dem Prinzip der minimalen Rechtevergabe und Regeln zur Kontobereitstellung durchgesetzt wird.

10.3 P5 - Änderungsmanagement-Richtlinie. Regelt Änderungen an Firewalls, Anpassungen von VPN-Regeln und Routing-Änderungen durch einen dokumentierten und auditierbaren Prozess.

10.4 P12 - Richtlinie zum Asset-Management. Unterstützt die Identifizierung und Klassifizierung vernetzter Systeme und stellt sicher, dass alle verbundenen Assets innerhalb der durch Richtlinien definierten Geltungsbereiche verwaltet werden.

10.5 P22 - Richtlinie zur Protokollierung und Überwachung. Regelt Erfassung, Korrelation und Aufbewahrung von Netzwerkprotokollen einschließlich Firewall-Ereignissen, Zugriffsversuchen und Anomalieerkennung.

10.6 P30 - Incident-Response-Richtlinie. Definiert die Verfahren zur Eskalation, Eindämmung und Beseitigung als Reaktion auf netzwerkbasierte Bedrohungen oder Eindringversuche, wie DDoS, laterale Bewegung oder unbefugten Zugriff.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an internationalen Standards und regulatorischen Vorgaben ausgerichtet, die sichere Netzwerkbetriebsprozesse, Segmentierung, Perimeterschutz und sicheren Fernzugriff definieren.

11.2 ISO/IEC 27001

11.2.1 Klausel 8.1 - Operative Planung und Steuerung: Verlangt, dass technische Kontrollen, einschließlich Netzwerkschutzmaßnahmen, in operative Prozesse eingebettet werden.

11.3 ISO/IEC 27002:2022

11.3.1 Maßnahmen 8.20-8.22: Enthalten Leitlinien zum Schutz von Netzwerken, zur Segmentierung von Diensten und zur Absicherung von Netzwerkdiensten durch Zugriffskontrollen und Überwachung.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Schutz von Netzgrenzen: Verlangt Perimeterkontrollen, Segmentierung und sichere Verbindungen.

11.4.2 AC-4 - Durchsetzung des Informationsflusses: Unterstützt Zonenbildung und regelbasierte Verkehrsbeschränkungen.

11.4.3 SC-32 - Partitionierung von Informationssystemen: Fördert die logische Trennung von Informationssystemen.

11.5 EU DSGVO (2016/679)

11.5.1 Artikel 32 - Sicherheit der Verarbeitung: Verlangt technische Maßnahmen — wie Firewalls und Segmentierung — zum Schutz personenbezogener Daten.

11.6 EU-NIS2-Richtlinie (2022/2555)

11.6.1 Artikel 21(2)(d): Verlangt wirksame Sicherheit von Netzwerk- und Informationssystemen, Perimeterschutz, sichere Konfiguration und Kontrollen zur Trennung.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 9 - Management von IKT-Risiken: Verpflichtet Finanzunternehmen, Netzwerke und Verbindungen vor unbefugtem Zugriff, Datenabfluss und Betriebsstörungen zu schützen.

11.8 COBIT 2019

11.8.1 DSS01.03 - Infrastruktur überwachen: Verlangt proaktive Kontrolle über Netzwerkzustand und Konnektivität.

11.8.2 DSS05.01 - Vor Schadsoftware schützen: Umfasst Segmentierung und Schutz von Netzgrenzen zur Minimierung der Ausbreitung.

11.8.3 MEA03 - Einhaltung überwachen, bewerten und beurteilen: Verstärkt die Durchsetzung von Netzwerkrichtlinien und Compliance-Bewertungen.