					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P21S					Dokumenttitel: **Netzwerksicherheitsrichtlinie**							
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**

In Übereinstimmung mit Standards und regulatorischen Vorgaben

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Abschnitt 8	-
ISO/IEC 27002:2022	Maßnahme 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
EU-DSGVO	Artikel 32	-
EU NIS2	Artikel 21(2)(d), (e)	-
EU DORA	Artikel 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Zweck

1.1. Zweck dieser Richtlinie ist es, sicherzustellen, dass sämtliche interne und externe Netzwerkkommunikation durch klar definierte Sicherheitskontrollen vor unbefugtem Zugriff, Manipulation, Abhören und Missbrauch geschützt ist.

1.2. Sie legt Regeln für die sichere Gestaltung, Nutzung und Verwaltung der Netzwerkinfrastruktur fest, einschließlich Routern, drahtlosen Zugriffspunkten, Fernzugriffsverbindungen und segmentierten Netzwerken.

1.3. Sie dient dazu, die externe Angriffsfläche gegenüber internetbasierten Bedrohungen zu minimieren, die Vertraulichkeit von Daten bei der Übertragung über interne und externe Netzwerke zu gewährleisten und die Verfügbarkeit kritischer Dienste aufrechtzuerhalten.

1.4. Diese Richtlinie unterstützt die Zertifizierung nach ISO/IEC 27001:2022, trägt unmittelbar zur Erfüllung gesetzlicher und regulatorischer Verpflichtungen nach DSGVO, NIS2 und DORA bei und dient der technischen Absicherung gegenüber Kunden und Auditoren.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Komponenten des IT-Netzwerks der Organisation, einschließlich:

2.1.1. kabelgebundener und drahtloser Infrastruktur an Bürostandorten

2.1.2. Routern, Switches, Zugriffspunkten, Firewalls und Gateways

2.1.3. Fernzugriffsverbindungen einschließlich VPN, RDP und Cloud-Tunneln

2.1.4. Cloud-basierten Anwendungen, auf die aus internen oder externen Netzwerken zugegriffen wird

2.1.5. Geräten, die von Mitarbeitenden, Auftragnehmern oder Gästen mit dem Netzwerk verbunden werden

2.2. Diese Richtlinie regelt sowohl physische als auch logische Netzwerksegmente, einschließlich Gastzonen, Internet-of-Things-(IoT)-Geräten und Backoffice-Systemen.

2.3. Die Richtlinie gilt für sämtliches Personal mit Zugriff auf das Netzwerk der Organisation, einschließlich:

2.3.1. interner Mitarbeitender

2.3.2. Remote-Mitarbeitender und Beschäftigter in hybriden Arbeitsmodellen

2.3.3. externer Lieferanten, Berater und Dienstleister

2.3.4. Gästen mit temporärem WLAN-Zugang

3. Ziele

3.1. Sicherstellen, dass das Netzwerk der Organisation vor unbefugtem Zugriff und externen Cyberangriffen geschützt ist.

3.2. Durchsetzen einer angemessenen Segmentierung zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken, z. B. Gast-WLAN und Zugängen Dritter.

3.3. Ermöglichen einer sicheren Fernanbindung, ohne interne Systeme zu beeinträchtigen.

3.4. Verhindern der Ausbreitung von Schadsoftware und der Datenexfiltration über Netzwerkkanäle.

3.5. Bereitstellen von Überwachung, Alarmierung und Auditierbarkeit von Netzwerkaktivitäten zur Unterstützung der Vorfallserkennung und Compliance.

3.6. Sicherstellen, dass nur genehmigte und abgesicherte Geräte mit internen Netzwerken verbunden werden dürfen.

3.7. Erfüllen der Verpflichtungen aus ISO 27001, DSGVO und verwandten Cybersicherheitsrahmenwerken.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführer (GM)

4.1.1. ist Eigentümer dieser Richtlinie und stellt sicher, dass angemessene Ressourcen für die sichere Netzwerkauslegung und -verwaltung bereitgestellt werden

4.1.2. prüft Ausnahmen von Netzwerksicherheitskontrollen und genehmigt Vereinbarungen über Netzwerkzugänge für Lieferanten

4.1.3. prüft Vorfälle oder Auditfeststellungen im Zusammenhang mit Schwachstellen der Netzwerksicherheit

4.2. IT-Support-Dienstleister / interne IT-Funktion

4.2.1. implementiert, konfiguriert und betreibt alle Firewalls, Router, Switches und Wireless-Controller

4.2.2. verwaltet die Segmentierung zwischen internen, Gast- und externen Netzwerken

4.2.3. überwacht Protokolle und Warnmeldungen auf unbefugte Zugriffsversuche oder Netzwerkanomalien

4.2.4. stellt sicher, dass Firmware- und Konfigurationsaktualisierungen sicher und fristgerecht eingespielt werden

[... 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 mindestens einmal jährlich durch den Geschäftsführer (GM) gemeinsam mit dem IT-Support-Dienstleister und dem Datenschutzkoordinator überprüft werden.

9.2. Auslöser für außerplanmäßige Überprüfungen

9.2.1. Eine Überprüfung der Richtlinie muss außerdem ausgelöst werden durch:

9.2.1.1. wesentliche Änderungen an der Netzwerkarchitektur, z. B. neue VPN- oder Firewall-Systeme

9.2.1.2. einen netzwerkbezogenen Vorfall, z. B. Eindringen, Ausbreitung von Ransomware oder Datenexfiltration

9.2.1.3. rechtliche, regulatorische oder rahmenwerksbezogene Aktualisierungen, die den Netzwerkschutz betreffen

9.2.1.4. neue Lieferantenplattformen, die alternative Zugriffsmethoden oder Protokolle erfordern

9.3. Versionsmanagement und Dokumentation

9.3.1. Überarbeitungen der Richtlinie müssen mit Versionsnummer, Datum und Zusammenfassung der Änderungen dokumentiert werden.

9.3.2. Frühere Versionen müssen mindestens 3 Jahre archiviert werden.

9.3.3. Aktualisierungen müssen den betroffenen Mitarbeitenden mitgeteilt werden; bei wesentlichen Änderungen des erwarteten Benutzerverhaltens ist eine verpflichtende Bestätigung einzuholen.

10. Verwandte Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist gemeinsam mit den folgenden SME-Sicherheitsrichtlinien umzusetzen:

10.1.1. P9S – Richtlinie für Remote-Arbeit: Legt sichere Methoden für den Fernzugriff, VPN-Anforderungen und Endpunktschutz für Benutzer außerhalb der Betriebsstätten fest.

10.1.2. P12S – Richtlinie zum Asset-Management: Stellt sicher, dass alle netzwerkverbundenen Systeme identifiziert, kategorisiert und mit aktuellem Sicherheitsstatus nachverfolgt werden.

10.1.3. P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass Netzwerksegmentierung, Zugriffskontrollen und Protokollierung die Datenschutzgrundsätze und Anforderungen der DSGVO unterstützen.

10.1.4. P22S – Richtlinie zur Protokollierung und Überwachung: Legt Anforderungen für die Erfassung und Überprüfung von Protokollen aus Netzwerkkomponenten, Fernverbindungen und Wireless-Controllern fest.

10.1.5. P30S – Incident-Response-Richtlinie (P30): Definiert die erforderlichen Maßnahmen als Reaktion auf Netzwerkverletzungen, unbefugte Zugriffsversuche oder die Ausbreitung von Schadsoftware über interne Netzwerke.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Abschnitt 8.1 – verlangt die Umsetzung von Kontrollen zur Gewährleistung sicherer und resilienter Betriebsabläufe einschließlich der Netzwerke.

11.2. ISO/IEC 27002

11.2.1. Maßnahme 8.20 – gibt technische und prozessuale Leitlinien zur Absicherung von Netzwerkzugriff, Segmentierung und Überwachung vor.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – verlangt die Steuerung von Informationsflüssen innerhalb von Netzwerken und zwischen Systemen.

11.3.2. SC-7 – verlangt den Schutz von Netzgrenzen, sicheres Routing und Netzwerksegmentierung zur Reduzierung des Risikos unbefugten Zugriffs.

11.4. EU-DSGVO

11.4.1. Artikel 32 – verlangt geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit vernetzter Systeme und Dienste, die personenbezogene Daten verarbeiten.

11.5. EU-NIS2-Richtlinie

11.5.1. Artikel 21(2)(d) – verlangt risikobasierte technische Maßnahmen einschließlich Netzwerksicherheit und Zugriffskontrolle.

11.5.2. Artikel 21(2)(e) – verlangt Systemsegmentierung und -isolation, um die Ausbreitung von Cybervorfällen zu verhindern.

11.6. EU DORA

11.6.1. Artikel 9 – verlangt von Unternehmen die Umsetzung von Kontrollen für das Management von IKT-Risiken, einschließlich Kontrollen für sichere Netzwerke und Kommunikation.

11.6.2. Artikel 10 – verlangt, dass Strategien zur digitalen Resilienz den Schutz der Netzwerkinfrastruktur und der Fernanbindung umfassen.

11.7. COBIT 2019

11.7.1. DSS05.02 – verlangt einen wirksamen Schutz der IT-Infrastruktur und der Netzwerkumgebungen gegen interne und externe Bedrohungen.

11.7.2. APO13.01 – verlangt Risikomanagementstrategien, die Netzwerksegmentierung und Überwachung als Teil der Bedrohungsminderung einschließen.