					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P35S					Dokumenttitel: **Richtlinie zur Sicherheit von Internet of Things (IoT) / Operational Technology (OT)**							
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 regulatorischen Vorgaben

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 6.1, 6.2, 8	
ISO/IEC 27002:2022	Maßnahmen 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
DSGVO	Artikel 32	
EU-NIS2	Artikel 21(2)(a), (d), (f)	
EU-DORA	Artikel 9(2), 10(1)	

1. Zweck

1.1. Diese Richtlinie legt verbindliche Anforderungen für die sichere Nutzung und Verwaltung von Geräten des Internet of Things (IoT) und der Operational Technology (OT) innerhalb der Organisation fest. Zu diesen Geräten können intelligente Sensoren, Sicherheitskameras, Produktionsmaschinen, HLK-Steuerungen oder sonstige netzwerkgebundene industrielle Systeme gehören.

1.2. Zweck dieser Richtlinie ist es:

1.2.1. physische und digitale Betriebsabläufe vor Störungen oder Manipulationen durch unzureichend abgesicherte vernetzte Geräte zu schützen

1.2.2. die sichere Bereitstellung, Überwachung und Wartung von IoT- und OT-Systemen sicherzustellen

1.2.3. die Einhaltung von ISO/IEC 27001:2022, der NIS2-Richtlinie und damit verbundener regulatorischer Rahmenwerke sicherzustellen

1.2.4. praktikable und durchsetzbare Kontrollen für KMU bereitzustellen, die in Büro-, Lager- oder Produktionsumgebungen tätig sind

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Personen, die an der Planung, Installation, Konfiguration, Nutzung, Unterstützung oder Entsorgung von IoT- oder OT-Geräten beteiligt sind. Dies umfasst:

2.1.1. Mitarbeitende, Auftragnehmer oder Praktikanten mit physischem Zugriff oder Fernzugriff auf Geräte

2.1.2. Drittdienstleister oder Servicetechniker, die vernetzte Systeme installieren oder warten

2.1.3. die Geschäftsführung oder Mitarbeitende, die für die Aufsicht über Sicherheitsrichtlinien verantwortlich sind

2.2. Die Richtlinie umfasst:

2.2.1. IoT-Geräte wie intelligente Schlösser, Überwachungssysteme, intelligente Zähler oder Drucker

2.2.2. OT-Systeme einschließlich SPS, SCADA-Bedienpanels oder Industrie-Gateways

2.2.3. unterstützende Hardware, Verwaltungsanwendungen und Kommunikationsnetze, die von diesen Systemen genutzt werden

2.3. Diese Richtlinie gilt für alle Arbeitsorte: Büroumgebungen, externe Standorte, Produktionsbereiche und Cloud-Plattformen mit Schnittstellen zu diesen Geräten.

3. Ziele

3.1. Sichere Bereitstellung: Sicherstellen, dass alle IoT-/OT-Systeme sicher konfiguriert sind, bevor sie in die Betriebsumgebung eingeführt werden.

3.2. Begrenzung der Exposition: Unbefugten Zugriff, Missbrauch oder die Kompromittierung vernetzter Geräte durch die Durchsetzung starker Zugriffskontrollen und Netzwerksegmentierung verhindern.

3.3. Kontinuierliche Überwachung: Transparenz über den Betrieb von IoT-/OT-Systemen aufrechterhalten, indem Aktivitäten protokolliert und ungewöhnliche Verhaltensweisen überwacht werden.

3.4. Lieferantenverantwortung: Sicherstellen, dass Drittdienstleister sichere Verfahren für Installation, Konfiguration und Wartung befolgen.

3.5. Regulatorische Konformität: Die vollständige Ausrichtung an geltenden Standards wie ISO 27001, der DSGVO (sofern personenbezogene Daten erhoben werden) und NIS2 zur Stärkung der Resilienz kritischer Infrastrukturen nachweisen.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführung (GM)

4.1.1. trägt die Gesamtverantwortung für die Sicherheit von IoT- und OT-Systemen

4.1.2. genehmigt diese Richtlinie und stellt ihre Durchsetzung in allen Arbeitsbereichen sicher

4.1.3. überprüft, dass Lieferanten und Auftragnehmer sichere Verfahren für Einrichtung und Wartung einhalten

4.1.4. autorisiert den Netzwerkzugang für jedes IoT-/OT-System

4.2. Benannter Mitarbeiter oder Betriebsleiter (sofern benannt)

4.2.1. überwacht die Inventarisierung, Platzierung und Konfiguration von IoT-/OT-Geräten

4.2.2. erfasst für jedes Gerät den Standort, die Netzwerkzuordnung und die Support-Dokumentation

4.2.3. stellt sicher, dass alle Änderungen (z. B. Firmware-Aktualisierungen oder Geräteaustausch) dokumentiert 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 die Geschäftsführung überprüft werden

9.1.2. Im Rahmen der Überprüfung ist zu bewerten, ob die Richtlinie weiterhin wirksam ist, aktuelle Gerätetypen abdeckt und mit neuen Risiken oder Technologien im Einklang steht

9.2. Anlassbezogene Aktualisierungen

9.2.1. Aktualisierungen der Richtlinie müssen ebenfalls eingeleitet werden, wenn:

9.2.2. neue Arten von IoT- oder OT-Systemen eingeführt werden

9.2.3. Lieferanten Sicherheitswarnmeldungen oder End-of-Life-Mitteilungen herausgeben

9.2.4. ein Vorfall oder Audit Lücken in den IoT-/OT-Kontrollen identifiziert

9.2.5. neue Gesetze oder Standards zusätzliche Anforderungen vorgeben

9.3. Dokumentation und Versionskontrolle

9.3.1. Alle Aktualisierungen müssen dokumentiert werden, einschließlich Datum, Versionsnummer und Zusammenfassung der Änderungen

9.3.2. Die Geschäftsführung muss frühere Richtlinienversionen für Audit-Zwecke aufbewahren

9.4. Kommunikation von Änderungen

9.4.1. Alle Aktualisierungen dieser Richtlinie müssen an alle relevanten Mitarbeitenden und Lieferanten kommuniziert werden

9.4.2. Aktualisierte Versionen müssen über gemeinsame Laufwerke oder in gedruckter Form an Installationsorten oder Leitstellen zugänglich gemacht werden

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist in Abstimmung mit den folgenden zugehörigen SME-Richtlinien umzusetzen:

10.1.1. P4S – Richtlinie zur Zugriffskontrolle: Erzwingt Anmeldekontrollen auf Geräteebene, die Verwendung starker Passwörter und Verfahren für autorisierten Zugriff auf IoT- und OT-Plattformen

10.1.2. P9S – Richtlinie für mobiles Arbeiten: Verhindert die Nutzung von Fernzugriff auf IoT-/OT-Dashboards über unsichere oder nicht genehmigte Kanäle

10.1.3. P17S – Richtlinie zu Datenschutz und Privatsphäre: Gilt, wenn IoT-Geräte (z. B. Sicherheitskameras) personenbezogene Daten verarbeiten oder aufzeichnen, und stellt die Einhaltung der DSGVO sicher

10.1.4. P30S – Incident-Response-Richtlinie (P30): Legt Verfahren zur Erkennung, Meldung und Behebung von IoT- oder OT-Vorfällen fest, einschließlich vermuteter Manipulation oder Betriebsstörung

10.1.5. P36S – Richtlinie zu sozialen Medien und externer Kommunikation: Stellt sicher, dass keine Geräteinformationen oder Netzwerktopologien extern offengelegt werden, sofern dies nicht genehmigt ist

10.2. Jede zugehörige Richtlinie stärkt die Durchsetzung und praktische Anwendung dieser Richtlinie durch gezielte verfahrensbezogene Vorgaben.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 6.1 – Risikoidentifizierung und Risikobehandlung: Verlangt, dass Risiken im Zusammenhang mit IoT- und OT-Systemen systematisch bewertet und behandelt werden

11.1.2. Klausel 8.1 – Operative Planung und Steuerung: Stellt eine sichere operative Steuerung vernetzter Geräte sicher

11.2. ISO/IEC 27002

11.2.1. Maßnahme 5.23 – Informationssicherheit bei der Nutzung von Operational Technology: Definiert die sichere Nutzung von OT in physischen und digitalen Umgebungen

11.2.2. Maßnahme 5.31 – Sichere Konfiguration von Informationssystemen: Verlangt gehärtete Konfigurationen für IoT-/OT-Geräte und die Vermeidung unsicherer Standardvorgaben

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Software-, Firmware- und Informationsintegrität: Verlangt die Integritätsprüfung von Firmware und Aktualisierungen

11.3.2. CM-7 – Prinzip der minimalen Funktionalität: Geräte dürfen keine ungenutzten oder unsicheren Funktionen aktiviert haben

11.3.3. AC-6 – Prinzip der minimalen Berechtigung: Der Gerätezugriff muss ausschließlich auf autorisierte Benutzer beschränkt sein

11.3.4. PE-20 – Asset-Überwachung: Physische und operative Überwachung von IoT- und OT-Assets

11.3.5. SC-7 – Schutz von Netzgrenzen: Segmentierung und Kontrolle der Netzwerkkommunikation für vernetzte Systeme

11.4. EU-DSGVO (2016/679)

11.4.1. Artikel 32 – Sicherheit der Verarbeitung: Wenn personenbezogene Daten erfasst werden (z. B. über Überwachungskameras), muss die Organisation geeignete technische und organisatorische Maßnahmen zur Absicherung dieser Verarbeitung umsetzen

11.5. EU-NIS2-Richtlinie (2022/2555)

11.5.1. Artikel 21(2)(a) – Risikomanagementmaßnahmen

11.5.2. Artikel 21(2)(d) – Sichere Gerätekonfiguration und -nutzung

11.5.3. Artikel 21(2)(f) – Sicherheit der Lieferkette und der Systeme

11.6. EU-DORA (2022/2554)

11.6.1. Artikel 9(2) – Geltungsbereich des IKT-Risikomanagements: Umfasst industrielle und eingebettete Geräte, die in Betriebsumgebungen eingesetzt werden

11.6.2. Artikel 10(1) – IKT-Kontinuität: Verlangt, dass Gerätekonfigurationen Resilienz und Wiederherstellungsmaßnahmen unterstützen

11.7. COBIT 2019

11.7.1. DSS01 – Betriebsmanagement: Gilt für die Überwachung technologischer Betriebsabläufe, einschließlich physischer Geräte

11.7.2. DSS05 – Sicherheitsdienste verwalten: Stellt sicher, dass vernetzte Systeme ordnungsgemäß überwacht und geschützt werden

11.7.3. APO13 – Sicherheitsmanagement: Stärkt Richtlinien zum Schutz betrieblicher Assets in KMU