					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P35					Dokumenttitel: **Richtlinie zur Sicherheit von IoT-/OT-Systemen**							
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**

An Standards und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Abschnitt 8	
ISO/IEC 27002:2022	Maßnahmen 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev. 5	SC-7, SI-4, CM-2, AC-6, PL-8	
EU-DSGVO	Artikel 5, 25, 32	
EU NIS2	Artikel 21, 23	
EU DORA	Artikel 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Zweck

1.1 Diese Richtlinie legt die verbindlichen Anforderungen an die Informationssicherheit für die Bereitstellung, den Betrieb, die Überwachung und die Außerbetriebnahme von Systemen des Internet of Things (IoT) und der Operational Technology (OT) innerhalb der Organisation fest.

1.2 Sie stellt sicher, dass diese Systeme in das übergeordnete Cybersicherheitsmanagementsystem der Organisation integriert und vor Kompromittierung, Missbrauch oder operativer Sabotage geschützt werden.

1.3 Ziel dieser Richtlinie ist die Durchsetzung wirksamer technischer, organisatorischer und prozessualer Kontrollen zum Schutz von IoT-/OT-Systemen, die mit physischer Infrastruktur, Produktionsprozessen und sicherheitskritischen Umgebungen verbunden sind.

1.4 Sie unterstützt regulatorische und vertragliche Verpflichtungen in den Bereichen Cybersicherheit, Sicherheit, Umweltsteuerung und Geschäftskontinuität.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle IoT- und OT-Systeme, unabhängig davon, ob sie sich im Eigentum des Unternehmens befinden, geleast oder von Dritten bereitgestellt werden, und in den operativen, administrativen oder produktiven Umgebungen der Organisation eingesetzt werden.

2.2 Zu den erfassten Systemen zählen unter anderem:

2.2.1 IoT-Geräte wie Umweltsensoren, Zutrittskontrollsysteme, intelligente Beleuchtung, Überwachungstechnik und Wearables

2.2.2 OT-Plattformen wie SPS, SCADA, verteilte Leitsysteme (DCS), HMI-Bedienpanels, MES-Schnittstellen und Feldsteuergeräte

2.2.3 industrielle Steuerungsnetzwerke oder cloudverbundene Assets zur Überwachung physischer Betriebsabläufe

2.3 Diese Richtlinie umfasst:

2.3.1 alle Umgebungen (On-Premises, Edge, cloudverwaltet)

2.3.2 alle Beteiligten (interne Benutzer, Integratoren, externe Lieferanten, Auftragnehmer)

2.3.3 alle Lebenszyklusphasen (Entwurf, Beschaffung, Bereitstellung, Betrieb, Außerbetriebnahme)

3. Ziele

3.1 Schutz der IoT-/OT-Infrastruktur vor internen und externen Cyberbedrohungen, einschließlich Denial-of-Service, unbefugtem Zugriff, der Ausbreitung von Ransomware und der Manipulation von Firmware.

3.2 Sicherstellung, dass IoT-/OT-Plattformen nicht als Vektor für IT-OT-Brückenangriffe dienen oder sicherheitskritische Systeme beeinträchtigen.

3.3 Anwendung der Grundsätze „Security by Design“ und „Defense in Depth“ über den gesamten Lebenszyklus dieser Technologien hinweg.

3.4 Ermöglichung einer zuverlässigen, sicheren und auditierbaren Integration von IoT- und OT-Plattformen in das Security Operations Center (SOC) und in die Incident-Response-Pläne der Organisation.

3.5 Sicherstellung, dass alle Bereitstellungen mit den Maßnahmen der ISO/IEC 27001 und den anwendbaren sektorspezifischen Leitlinien (z. B. IEC 62443, ISO 27019, NIST SP 800-82) übereinstimmen.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO) / Leiter Informationssicherheit

4.1.1 Definiert Richtlinien und technische Standards für die IoT-/OT-Cybersicherheit

4.1.2 Beaufsichtigt Risikobewertungen, Kontrollvalidierung und funktionsübergreifende Koordination

4.2 OT-Ingenieure / Facility- und Anlagenmanager

4.2.1 Prüfen OT-Systemkonfigurationen und setzen die Einhaltung dieser Richtlinie in Produktionsbereichen durch

4.2.2 Stellen physische und logische Schutzmaßnahmen sicher, um Integrität und Betriebssicherheit der OT zu gewährleisten

[... 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 muss mindestens jährlich überprüft und auf Grundlage folgender Auslöser aktualisiert werden:

9.1.1 Änderungen an OT- oder IoT-Systemarchitekturen, Lieferanten oder Plattformen

9.1.2 wesentliche regulatorische Aktualisierungen (z. B. Änderungen an DORA, NIS2, sektorspezifischen Richtlinien)

9.1.3 das Auftreten neuer Schwachstellen oder Bedrohungsmuster in Steuerungssystemen

9.1.4 Feststellungen aus internen oder externen Audits, Penetrationstests oder Red-Team-Übungen

9.2 Der CISO, der OT Security Lead und die zuständigen Bereichsleiter sind gemeinsam dafür verantwortlich, den Überprüfungsprozess einzuleiten.

9.3 Außerordentliche Überprüfungen müssen ausgelöst werden nach:

9.3.1 jedem IoT-/OT-bezogenen Vorfall, der zu Systemausfall oder Datenverlust führt

9.3.2 der Einführung wesentlicher neuer Geräte, Überwachungssoftware oder Firmware-Plattformen

9.3.3 der Integration intelligenter Edge-Computing-Lösungen oder KI-gestützter Automatisierung auf Feldebene

9.4 Alle Änderungen an der Richtlinie müssen:

9.4.1 in der Versionshistorie und im Register für Richtlinienänderungen dokumentiert werden

9.4.2 an alle betroffenen Benutzer, Lieferanten und IT-/OT-Betreiber kommuniziert werden

9.4.3 durch die Geschäftsleitung erneut genehmigt werden

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie gilt in Verbindung mit den folgenden Informationssicherheitsrichtlinien und wird durch diese unterstützt:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt grundlegende Sicherheitsprinzipien fest, die auch für die Sicherheit von IoT- und OT-Systemen gelten.

10.1.2 P3 – Richtlinie zur zulässigen Nutzung: Definiert Beschränkungen für die persönliche und nicht autorisierte Nutzung von Geräten, auch in operativen Umgebungen.

10.1.3 P6 – Richtlinie zum Risikomanagement: Regelt die Bewertung, Akzeptanz und Minderung von Risiken im Zusammenhang mit eingebetteten Systemen und Steuerungssystemen.

10.1.4 P12 – Richtlinie zum Asset-Management: Stellt sicher, dass alle IoT- und OT-Systeme formal inventarisiert und verantwortlichen Eigentümern zugewiesen werden.

10.1.5 P20 – Richtlinie zu Endpunktschutz / Schutz vor Schadsoftware: Gilt für verbundene Steuerungen, intelligente Gateways und Edge-Systeme in der Produktion.

10.1.6 P22 – Richtlinie zu Protokollierung und Überwachung: Erstreckt sich auf Verfahren zur Protokollerfassung und -prüfung in OT-Umgebungen.

10.1.7 P30 – Incident-Response-Richtlinie: Regelt unmittelbar, wie IoT-/OT-Sicherheitsverletzungen, Anomalien oder Systemausfälle eskaliert und behandelt werden müssen.

10.1.8 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Stellt Sicherungsmechanismen bereit, um die fortlaufende Einhaltung dieser Richtlinie zu validieren.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Standards und regulatorischen Rahmenwerken ausgerichtet, die Sicherheit, Resilienz und Compliance für Systeme des Internet of Things (IoT) und der Operational Technology (OT) in industriellen, produktiven und Unternehmensumgebungen sicherstellen.

11.2 ISO/IEC 27002:2022 – Maßnahmen 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Maßnahme 5.7 – Threat Intelligence: Unterstützt die Überwachung von OT-Umgebungen und die Identifizierung IoT-spezifischer Schwachstellen.

11.2.2 Maßnahme 5.23 – Informationssicherheit bei der Nutzung von Cloud-Diensten: Gilt, wenn IoT-Geräte mit Cloud-Plattformen für Telemetrie, Steuerung oder Analytik verbunden sind.

11.2.3 Maßnahme 5.27 – Sichere Systemarchitektur und Engineering-Prinzipien: Regelt „Security by Design“-Grundsätze für eingebettete Systeme und Steuerungsnetzwerke.

11.2.4 Maßnahme 5.31 – Sicherheit in Entwicklungs- und Supportprozessen: Erzwingt Software-/Firmware-Validierung, Patch-Kontrollen und Lieferantenanforderungen in OT-Bereitstellungen.

11.2.5 Maßnahme 5.36 – Einhaltung gesetzlicher und vertraglicher Anforderungen: Stellt die Einhaltung von Sicherheits-, Umwelt- und regulatorischen Vorgaben durch OT-Assets sicher.

11.2.6 Diese Maßnahmen etablieren gemeinsam bewährte Verfahren zur Absicherung von IoT-/OT-Systemen über ihren gesamten Lebenszyklus hinweg, einschließlich Architekturentwurf, sicherer Bereitstellung, Patch-Management, Anomalieerkennung und Einhaltung sektorspezifischer Anforderungen.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-7 – Boundary Protection: Stellt sicher, dass OT-Netzwerke segmentiert und vor unbefugtem Zugriff geschützt sind.

11.3.2 SI-4 – System Monitoring: Verlangt die Umsetzung kontinuierlicher Überwachung und von Mechanismen zur Anomalieerkennung in ICS-Umgebungen.

11.3.3 CM-2 – Baseline Configuration: Verlangt Konfigurationskontrolle und Härtung von IoT-/OT-Plattformen.

11.3.4 AC-6 – Least Privilege: Gilt für Benutzerzugriffe und die Fernwartung eingebetteter Steuerungssysteme durch Lieferanten.

11.3.5 PL-8 – Security and Privacy Architectures: Regelt die Planung sicherer Systemintegration, insbesondere für OT-Modernisierungsprojekte.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 5 – Grundsätze für die Verarbeitung personenbezogener Daten: Gilt für IoT-Plattformen, die sensorbasierte oder verhaltensbezogene Daten von Personen verarbeiten.

11.4.2 Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: Verlangt Datenschutzmaßnahmen, die in Produktdesign und Firmware von IoT-Geräten eingebettet sind.

11.4.3 Artikel 32 – Sicherheit der Verarbeitung: Verlangt Verschlüsselung, Zugriffskontrolle und sichere Kommunikation für Datenübertragungen intelligenter Geräte.

11.5 EU-NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21 und 23: Legen Sicherheitsverpflichtungen für wesentliche und wichtige Einrichtungen fest, die OT-Systeme nutzen. Dazu gehören Risikobewertung, Vorfallmeldung und die Validierung der Lieferkette von IoT-/OT-Lieferanten sowie der Firmware-Integrität.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – IKT-Risikomanagement: Verlangt die sichere Integration eingebetteter Systeme und von OT-Technologien in das IKT-Risikomanagementprogramm.

11.6.2 Artikel 10 – IKT-Sicherheitsanforderungen: Schreibt Schutzmaßnahmen für vernetzte OT-Plattformen vor, die in Finanz- und kritischen Dienstleistungsumgebungen eingesetzt werden.

11.7 COBIT 2019

11.7.1 DSS05.01 – Schutz vor Schadsoftware: Umfasst Erkennung und Reaktion auf ICS-spezifische Bedrohungen und IoT-Schadsoftwarekampagnen.

11.7.2 BAI09.01 – Sicherheitsanforderungen festlegen und aufrechterhalten: Entspricht der sicheren Bereitstellung und dem sicheren Betrieb intelligenter oder eingebetteter Infrastruktur.

11.7.3 APO13.02 – Informationssicherheitsplan festlegen und aufrechterhalten: Verlangt die Einbeziehung von OT-Systemen und ihrer Schwachstellen in die unternehmensweite Cybersicherheitsstrategie.