					Insert Registered Legal Entity Name Here							
Document number: P35					Document Title: **IoT / OT Security Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	
ISO/IEC 27002:2022	Controls 5.7, 5.23, 5.27, 5.31, 5	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
EU GDPR	Articles 5, 25, 32	
EU NIS2	Articles 21, 23	
EU DORA	Articles 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13	

1. Purpose

1.1 This policy establishes mandatory information security requirements for the deployment, operation, monitoring, and decommissioning of Internet of Things (IoT) and Operational Technology (OT) systems within the organization.

1.2 It ensures that such systems are integrated into the organization's broader cybersecurity management system and protected against compromise, misuse, and operational sabotage.

1.3 This policy mandates robust technical, organizational, and procedural controls to protect IoT/OT systems that interface with physical infrastructure, production processes, and safety-critical environments.

1.4 It supports regulatory and contractual obligations across cybersecurity, safety, environmental control, and business continuity disciplines.

2. Scope

2.1 This policy applies to all IoT and OT systems, whether company-owned, leased, or provided by third parties, used within the organization's operational, administrative, or production environments.

2.2 Covered systems include, but are not limited to:

2.2.1 IoT devices such as environmental sensors, access control systems, smart lighting, surveillance equipment, and wearables

2.2.2 OT platforms such as PLCs, SCADA, DCS, HMI panels, MES interfaces, and field controllers

2.2.3 Industrial control networks or cloud-connected assets used to monitor physical operations

2.3 This policy covers:

2.3.1 All environments (on-premises, edge, cloud-managed)

2.3.2 All stakeholders (internal users, integrators, external vendors, contractors, and third-party service providers)

2.3.3 All lifecycle phases (design, procurement, deployment, operations, decommissioning)

3. Objectives

3.1 To protect IoT and OT infrastructure against internal and external cyberattacks, including denial-of-service attacks, unauthorized access, ransomware propagation, and firmware tampering.

3.2 To ensure that IoT/OT platforms do not become vectors for IT/OT bridge attacks or compromise safety-critical systems.

3.3 To apply secure-by-design and defense-in-depth principles throughout the lifecycle of these technologies.

3.4 To enable reliable, secure, and auditable integration of IoT and OT platforms within the organization's security operations center (SOC) and incident response plans.

3.5 To ensure that all deployments align with ISO/IEC 27001 controls and applicable sector-specific guidance (e.g. IEC 62443, ISO 27019, NIST SP 800-82).

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO) / Security Lead

4.1.1 Defines policies and technical standards for IoT/OT cybersecurity

4.1.2 Oversees risk assessments for new projects, control validation, and cross-functional coordination

4.2 OT Engineers / Facilities and Plant Managers

4.2.1 Validate OT system configurations and enforce compliance with this policy in production areas

4.2.2 Maintain physical and logical safeguards to preserve OT integrity and safety

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 This policy must be reviewed at least annually and updated based on:

9.1.1 Changes in OT or IoT system architecture, vendors, or platforms

9.1.2 Major regulatory updates (e.g. revisions to DORA, NIS2, or sector-specific directives)

9.1.3 Emergence of new vulnerabilities or threat patterns in control systems

9.1.4 Findings from internal or external audits, penetration tests, or red team exercises

9.2 The CISO, OT Security Lead, and relevant Department Heads are jointly responsible for initiating the review process.

9.3 Interim reviews must be triggered after:

9.3.1 Any IoT/OT-related incident resulting in system failure or data loss

9.3.2 Introduction of significant new equipment, monitoring software, or firmware platforms

9.3.3 Integration of smart edge computing or AI-enhanced automation at field level

9.4 All policy changes must be:

9.4.1 Documented in the version history and Policy Change Register

9.4.2 Communicated to all affected users, vendors, and IT/OT operators

9.4.3 Reapproved by Top Management

10. Related Policies and Linkages

10.1 This policy operates in conjunction with, and is supported by, the following information security policies:

10.1.1 P1 – Information Security Policy: Establishes foundational security principles that extend to IoT and OT system security.

10.1.2 P3 – Acceptable Use Policy: Defines restrictions on personal and unauthorized device use, including within operational environments.

10.1.3 P6 – Risk Management Policy: Guides the assessment, acceptance, and mitigation of risks related to embedded and control systems.

10.1.4 P12 – Asset Management Policy: Ensures all IoT and OT systems are formally inventoried and assigned responsible owners.

10.1.5 P20 – Endpoint Protection / Malware Policy: Applies to connected controllers, smart gateways, and edge systems in production.

10.1.6 P22 – Logging and Monitoring Policy: Extends to log capture and review procedures for OT environments.

10.1.7 P30 – Incident Response Policy: Directly governs how IoT/OT breaches, anomalies, or system failures must be escalated and managed.

10.1.8 P33 – Audit and Compliance Monitoring Policy: Provides assurance mechanisms to validate ongoing compliance with this policy.

11. Reference Standards and Frameworks

11.1 This policy is aligned with internationally recognized standards and regulatory frameworks that ensure the security, resilience, and compliance of Internet of Things (IoT) and Operational Technology (OT) systems in industrial, production, and enterprise environments.

11.2 ISO/IEC 27002:2022 – Controls 5.7, 5.23, 5.27, 5.31, 5

11.2.1 Control 5.7 – Threat Intelligence: Informs monitoring of OT environments and identification of IoT-specific vulnerabilities.

11.2.2 Control 5.23 – Information Security for Use of Cloud Services: Applies where IoT devices interface with cloud platforms for telemetry, control, or analytics.

11.2.3 Control 5.27 – Secure System Architecture and Engineering Principles: Governs secure-by-design principles for embedded systems and control networks.

11.2.4 Control 5.31 – Security in Development and Support Processes: Enforces software and firmware validation, patch controls, and vendor requirements in OT deployments.

11.2.5 Control 5.36 – Compliance with Legal and Contractual Requirements: Ensures OT asset compliance with safety, environmental, and regulatory requirements.

11.2.6 These controls collectively establish industry best practices for securing IoT/OT systems throughout their lifecycle, including architecture design, secure deployment, patching, anomaly detection, and compliance with sector-specific requirements.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Boundary Protection: Ensures OT networks are segmented and protected against unauthorized access.

11.3.2 SI-4 – System Monitoring: Requires implementation of continuous monitoring and anomaly detection mechanisms in ICS environments.

11.3.3 CM-2 – Baseline Configuration: Requires configuration control and device hardening of IoT/OT platforms.

11.3.4 AC-6 – Least Privilege: Applies to user access and remote vendor servicing of embedded control systems.

11.3.5 PL-8 – Security and Privacy Architectures: Governs secure system integration planning, particularly for OT modernization projects.

11.4 EU GDPR (2016/679)

11.4.1 Article 5 – Principles Relating to Processing of Personal Data: Applies to IoT platforms processing sensor-based or behavioral data linked to individuals.

11.4.2 Article 25 – Data Protection by Design and by Default: Requires data protection and data minimization safeguards embedded in IoT product design and firmware.

11.4.3 Article 32 – Security of Processing: Requires encryption, access control, and secure communications for smart device data transmissions.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Articles 21 and 23: Impose security obligations on essential and important entities using OT systems. These include risk assessment, incident reporting and management, and supply chain validation of IoT/OT vendors and firmware integrity.

11.6 EU DORA (2022/2554)

11.6.1 Article 9 – ICT Risk Management: Requires secure integration of embedded systems and OT technologies within the ICT risk governance program.

11.6.2 Article 10 – ICT Security Requirements: Mandates protective measures for interconnected OT platforms used in financial and critical service environments.

11.7 COBIT 2019

11.7.1 DSS05.01 – Protect Against Malware: Includes detection of and response to ICS-specific threats and IoT malware campaigns.

11.7.2 BAI09.01 – Establish and Maintain Security Requirements: Maps to secure provisioning and operation of smart or embedded infrastructure.

11.7.3 APO13.02 – Establish and Maintain an Information Security Plan: Requires inclusion of OT systems and their vulnerabilities in the enterprise-wide cybersecurity strategy.