					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 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 GDPR	Articles 5, 25, 32	
EU NIS2	Articles 21, 23	
EU DORA	Articles 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

					[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		

1. **Purpose**
   1.1. This policy establishes the mandatory information security requirements for the deployment, operation, monitoring, and retirement 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 are protected from compromise, misuse, or operational sabotage.
   1.3. The policy aims to enforce strong 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 continuity disciplines.
2. **Scope**
   2.1. This policy applies to all IoT and OT systems—whether company-owned, leased, or third-party provided—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 controls, 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 monitoring physical operations
   2.3. The policy covers:
      2.3.1. All environments (on-premises, edge, cloud-managed)
      2.3.2. All stakeholders (internal users, integrators, third-party vendors, contractors)
      2.3.3. All lifecycle phases (design, procurement, deployment, operations, decommissioning)
3. **Objectives**
   3.1. To secure IoT and OT infrastructure from internal and external cybersecurity threats, including denial-of-service, 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 security-by-design and defense-in-depth principles across 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 sectoral 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, control validation, and cross-departmental coordination
   4.2. **OT Engineers / Facility and Plant Managers**
      4.2.1. Validate OT system configurations and enforce policy adherence in production areas

4.2.2. Maintain physical and logical safeguards for OT integrity and safety

4.3. **IT Administrators / Network Engineers**

4.3.1. Enforce network segmentation and firewall rules between IT and OT/IoT networks

[.....]

11. Reference Standards and Frameworks

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.

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

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

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

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

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

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

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

NIST SP 800-53 Rev.5

SC-7 – Boundary Protection: Ensures OT networks are segmented and shielded from unauthorized access.

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

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

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

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

EU GDPR (2016/679)

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

Article 25 – Data Protection by Design and by Default: Requires privacy safeguards embedded in IoT product design and firmware.

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

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

COBIT 2019

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

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

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