					[Insert Registered Legal Entity Name Here]							
Document number: P35S					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	Clauses 6.1, 6.2, 8.1	
ISO/IEC 27002:2022	Controls 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
EU GDPR	Article 32	
EU NIS2	Article 21(2)(a), (d), (f)	
EU DORA	Article 9(2), 10(1)	

					[Insert Registered Legal Entity Name Here]							
Document number: P35S					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 defines the mandatory rules for securely using and managing Internet of Things (IoT) and Operational Technology (OT) devices within the organization. These devices may include smart sensors, security cameras, production machines, HVAC controllers, or any network-connected industrial systems.
   1.2. The purpose of this policy is to:
      1.2.1. Protect physical and digital operations from disruption or manipulation via poorly secured connected devices
      1.2.2. Enforce safe deployment, monitoring, and maintenance of IoT and OT systems
      1.2.3. Ensure compliance with ISO/IEC 27001:2022, NIS2 Directive, and related regulatory frameworks
      1.2.4. Provide practical, enforceable controls for SMEs operating in office, warehouse, or production environments
2. **Scope**
   2.1. This policy applies to all individuals involved in the planning, installation, configuration, use, support, or disposal of IoT or OT devices. This includes:
      2.1.1. Employees, contractors, or interns with physical or remote access to devices
      2.1.2. Third-party vendors or service technicians installing or maintaining connected systems
      2.1.3. General Managers or staff responsible for overseeing security policies
   2.2. The policy covers:
      2.2.1. IoT devices such as smart locks, surveillance systems, smart meters, or printers
      2.2.2. OT systems including PLCs (Programmable Logic Controllers), SCADA panels, or industrial gateways
      2.2.3. Supporting hardware, management apps, and communication networks used by these systems
   2.3. This policy applies across all work locations: office environments, remote sites, production floors, and cloud platforms interfacing with these devices.
3. **Objectives**
   3.1. **Secure Deployment**: Ensure all IoT/OT systems are securely configured before being introduced to the operational environment.
   3.2. **Limit Exposure**: Prevent unauthorized access, misuse, or takeover of connected devices by enforcing strong access controls and network segregation.
   3.3. **Continuous Monitoring**: Maintain visibility into IoT/OT operations by logging activity and monitoring for unusual behavior.
   3.4. **Vendor Accountability**: Ensure third-party providers follow secure installation, configuration, and maintenance practices.
   3.5. **Regulatory Compliance**: Demonstrate full alignment with applicable standards such as ISO 27001, GDPR (if personal data is collected), and NIS2 for critical infrastructure resilience.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Holds overall responsibility for the security of IoT and OT systems
      4.1.2.

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 6.1 – Risk Identification and Treatment: Requires that risks related to IoT and OT systems be systematically assessed and mitigated

Clause 8.1 – Operational Planning and Control: Ensures secure operational control over connected devices

ISO/IEC 27002:2022

Control 5.23 – Information Security for Use of Operational Technology: Defines secure use of OT across physical and digital environments

Control 5.31 – Secure Configuration of Information Systems: Requires hardened setups for IoT/OT devices and avoidance of insecure defaults

NIST SP 800-53 Rev.5

SI-7 – Software, Firmware, and Information Integrity: Requires integrity validation of firmware and updates

CM-7 – Least Functionality: Devices must not have unused or insecure features enabled

AC-6 – Least Privilege: Device access must be limited to authorized users only

PE-20 – Asset Monitoring: Physical and operational monitoring of IoT and OT assets

SC-7 – Boundary Protection: Segmentation and control of network communications for connected systems

EU GDPR (2016/679)

Article 32 – Security of Processing: If personal data is captured (e.g., through surveillance cameras), the organization must implement appropriate technical and organizational measures to secure such processing

EU NIS2 Directive (2022/2555)

Article 21(2)(a) – Risk Management Measures

Article 21(2)(d) – Secure Device Configuration and Use

Article 21(2)(f) – Supply Chain and System Security

EU DORA (2022/2554)

Article 9(2) – ICT Risk Management Scope: Includes industrial and embedded devices used in operational environments

Article 10(1) – ICT Continuity: Requires device configurations to support resilience and recovery operations

COBIT 2019

DSS01 – Manage Operations: Applies to the oversight of technology operations, including physical devices

DSS05 – Manage Security Services: Ensures that connected systems are properly monitored and protected

APO13 – Manage Security: Reinforces policies for safeguarding operational assets across SMEs