					Insert Registered Legal Entity Name Here							
Document number: P35S					Document Title: **Internet of Things (IoT) / Operational Technology (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	Clauses 6.1, 6.2, 8	
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)	

1. Purpose

1.1. This policy defines the mandatory requirements for the secure use and management of Internet of Things (IoT) and Operational Technology (OT) devices within the organization. These devices may include smart sensors, security cameras, production machinery, 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 against disruption or manipulation through inadequately secured connected devices

1.2.2. Enforce secure deployment, monitoring, and maintenance of Internet of Things (IoT) and Operational Technology (OT) systems

1.2.3. Ensure compliance with ISO/IEC 27001:2022, the 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 Internet of Things (IoT) or Operational Technology (OT) devices. This includes:

2.1.1. Employees, contractors, or interns with physical or remote access to devices

2.1.2. Third-party providers, vendors, or service technicians installing or maintaining connected systems

2.1.3. General Managers or personnel responsible for oversight of security policies

2.2. The policy covers:

2.2.1. Internet of Things (IoT) devices such as smart locks, surveillance systems, smart meters, or printers

2.2.2. Operational Technology (OT) systems including PLCs, SCADA panels, or industrial gateways

2.2.3. Supporting hardware, management applications, and communications networks used by these systems

2.3. This policy applies across all work locations, including office environments, remote sites, production areas, and cloud platforms interfacing with these devices.

3. Objectives

3.1. Secure Deployment: Ensure all IoT/OT systems are securely configured before being introduced into the operational environment.

3.2. Limit Exposure: Prevent unauthorized access, misuse, or compromise 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 and vendors follow secure installation, configuration, and maintenance practices.

3.5. Regulatory Compliance: Demonstrate 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 Internet of Things (IoT) and Operational Technology (OT) systems

4.1.2. Approves this policy and ensures its enforcement across all work areas

4.1.3. Verifies that vendors and contractors follow secure installation and maintenance practices

4.1.4. Authorizes network access for any Internet of Things (IoT) or Operational Technology (OT) system

4.2. Designated employee or Operations Manager (if assigned)

4.2.1. Oversees the inventory, placement, and configuration of Internet of Things (IoT) and Operational Technology (OT) devices

4.2.2. Records each device's location, network assignment, and supporting documentation

4.2.3. Ensures that any changes, such as firmware updates or device replacements, are documented

[... 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. Annual Review

9.1.1. This policy must be reviewed at least annually by the General Manager

9.1.2. The review must assess whether the policy remains effective, covers current device types, and aligns with new risks or technologies

9.2. Trigger-Based Updates

9.2.1. Policy updates must also be initiated when:

9.2.2. New types of Internet of Things (IoT) or Operational Technology (OT) systems are introduced

9.2.3. Vendors issue security advisories or end-of-life notices

9.2.4. An incident or audit identifies gaps in Internet of Things (IoT) and Operational Technology (OT) controls

9.2.5. New laws or standards impose additional requirements

9.3. Documentation and Version Control

9.3.1. All updates must be documented, including the date, version number, and summary of changes

9.3.2. The General Manager must retain historical policy versions for audit purposes

9.4. Communication of Changes

9.4.1. Any updates to the policy must be communicated to all relevant personnel and vendors

9.4.2. Updated versions must be made accessible through shared folders or printed materials at installation sites or control centers

10. Related Policies and Linkages

10.1. This policy must be implemented in alignment with the following related SME policies:

10.1.1. P4S – Access Control Policy: Enforces device-level login controls, strong password use, and authorized access procedures for Internet of Things (IoT) and Operational Technology (OT) platforms

10.1.2. P9S – Remote Work Policy: Prevents the use of remote access to Internet of Things (IoT) and Operational Technology (OT) dashboards through insecure or unapproved channels

10.1.3. P17S – Data Protection and Privacy Policy: Applies where Internet of Things (IoT) devices, such as security cameras, process or record personal data, ensuring compliance with GDPR

10.1.4. P30S – Incident Response Policy: Defines procedures for detecting, reporting, and resolving Internet of Things (IoT) or Operational Technology (OT) incidents, including suspected tampering or operational failure

10.1.5. P36S – Social Media and External Communications Policy: Ensures that no device information or network layout is shared externally unless approved

10.2. Each related policy strengthens the enforcement and practical application of this policy by providing targeted procedural guidance.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 6.1 – Risk Identification and Treatment: Requires that risks related to Internet of Things (IoT) and Operational Technology (OT) systems be systematically assessed and mitigated

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

11.2. ISO/IEC 27002

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

11.2.2. Control 5.31 – Secure Configuration of Information Systems: Requires hardened configurations for Internet of Things (IoT) and Operational Technology (OT) devices and the avoidance of insecure defaults

11.3. NIST SP 800-53 Rev.5

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

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

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

11.3.4. PE-20 – Asset Monitoring: Physical and operational monitoring of Internet of Things (IoT) and Operational Technology (OT) assets

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

11.4. EU GDPR (2016/679)

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

11.5. EU NIS2 Directive (2022/2555)

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

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

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

11.6. EU DORA (2022/2554)

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

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

11.7. COBIT 2019

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

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

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