Internet of Things (IoT) Security Framework for Industry 4.0

"IoT Security Framework Scope"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *Internet of Things (IoT) Security Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Scope 4](#_Toc177464641)

[2. Exclusions 4](#_Toc177464642)

[3. Boundaries 4](#_Toc177464643)

[4. Document Management 5](#_Toc177464644)

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

# Scope

The IoT Security Framework encompasses the management of security controls across the organisation's IoT ecosystem. This includes:

* **Device Security:** Encompasses all IoT devices deployed and managed by the organisation, including their authentication, communication, firmware/software integrity, physical security, and endpoint protection.
* **Data Security and Privacy:** Covers all data generated, collected, processed, stored, and transmitted by IoT devices, ensuring its confidentiality, integrity, and availability while adhering to privacy regulations.
* **Network Security:** Includes the entire network infrastructure supporting the IoT ecosystem, including network segmentation, firewalls, intrusion detection systems, and secure communication protocols.
* **Interoperability:** Addresses the seamless integration and communication between diverse IoT devices and platforms within the organisation's environment.
* **Lifecycle Management:** Covers the entire lifecycle of IoT devices, from onboarding and provisioning to maintenance, updates, and secure decommissioning.
* **Incident Management and Response:** Encompasses the processes and procedures for identifying, responding to, and recovering from security incidents related to the IoT ecosystem.
* **Compliance and Certification:** Includes adherence to relevant industry regulations and standards, as well as obtaining necessary certifications for IoT devices and systems.
* **Emerging Threats and Future Proofing:** Focuses on proactively addressing new and evolving security threats to the IoT ecosystem and ensuring the framework's adaptability to future challenges.
* **Policies Addressing Machine Learning and AI in IoT:** Governs the secure and ethical use of machine learning and AI technologies within the IoT ecosystem, addressing model security, data protection, and ethical considerations.

# Exclusions

* The framework does not cover physical security measures for non-IoT assets or infrastructure.
* It does not address specific legal or contractual obligations beyond general compliance requirements.
* The framework may not encompass highly specialised or niche IoT applications that require tailored security controls.

# Boundaries

* The framework applies to all IoT devices, systems, and data within the organisation's control, regardless of their location or ownership.
* It extends to third-party vendors and partners who interact with the organisation's IoT ecosystem.
* The framework's scope may evolve as the organisation's IoT environment expands or changes.

**Note:** This scope statement provides a high-level overview. Organisations should further refine and detail the scope based on their specific IoT deployment, risk profile, and business objectives.

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager