Internet of Things (IoT) security Framework for Industry 4.0

"Records Appraisal Procedure"

|  |  |
| --- | --- |
| 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. Introduction 4](#_Toc177467689)

[2. Scope 4](#_Toc177467690)

[3. Objectives 4](#_Toc177467691)

[4. Responsibilities 4](#_Toc177467692)

[5. Appraisal Process 4](#_Toc177467693)

[6. Appraisal Criteria 5](#_Toc177467694)

[7. Disposal Methods 5](#_Toc177467695)

[8. Responsibilities 5](#_Toc177467696)

[9. Breaches of Policy 5](#_Toc177467697)

[10. Summary 5](#_Toc177467698)

[11. Document Management 5](#_Toc177467699)

# Introduction

This procedure outlines the process for appraising records within the context of the IoT Security Framework. Appraisal is the systematic evaluation of records to determine their ongoing value and retention requirements. It ensures that records of continuing business, legal, or historical significance are preserved while those of no further value are disposed of appropriately.

# Scope

This procedure applies to all records generated or maintained in relation to the implementation and operation of the IoT Security Framework. This includes, but is not limited to, policy documents, procedures, risk assessments, audit reports, incident logs, and any other records relevant to the framework.

# Objectives

* Ensure efficient and effective records management within the IoT ecosystem.
* Identify and preserve records of long-term value for business, legal, or historical purposes.
* Comply with relevant legal and regulatory requirements regarding record retention and disposal.
* Minimise storage costs and optimise resource utilisation.

# Responsibilities

* **Data Owners:** Responsible for classifying and assigning retention periods to records within their purview, in accordance with the organisation's data retention schedule.
* **Information Security Officer:** Oversees the appraisal process and ensures compliance with the organisation's information security policies.
* **Records Management Team:** Provides guidance and support to data owners during the appraisal process.
* **IT Department:** Assists with the secure disposal of electronic records.

# Appraisal Process

The appraisal process will be conducted periodically, at least annually, or as triggered by specific events such as changes in regulations or business needs. The following steps will be followed:

1. **Identify Records:** Compile a comprehensive inventory of all records related to the IoT Security Framework.
2. **Classify Records:** Categorise records based on their content, function, and sensitivity.
3. **Assess Value:** Evaluate the business, legal, and historical value of each record category.
4. **Assign Retention Periods:** Determine the appropriate retention period for each record category based on legal requirements, business needs, and historical significance.
5. **Document Appraisal Decisions:** Record the appraisal decisions, including retention periods and disposal methods, in the organisation's data retention schedule.
6. **Implement Disposal:** Dispose of records that have reached the end of their retention period in a secure and compliant manner.

# Appraisal Criteria

The following criteria will be considered when assessing the value of records:

* **Business Value:** Records that support ongoing business operations, decision-making, or legal obligations.
* **Legal Value:** Records required to comply with laws, regulations, or contractual agreements.
* **Historical Value:** Records that document the organisation's history, activities, or achievements.
* **Evidential Value:** Records that provide evidence of actions, decisions, or transactions.
* **Informational Value:** Records that contain valuable information or knowledge.

# Disposal Methods

Records will be disposed of in a secure and environmentally responsible manner. The following methods may be used:

* **Secure Destruction:** Physical destruction of paper records or secure erasure of electronic records.
* **Archival Storage:** Transfer of records with long-term historical value to a secure archival facility.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for selecting and configuring appropriate encryption protocols and key management solutions.
* **Device Manufacturers/Vendors:** Responsible for implementing secure communication capabilities in their devices.
* **Users:** Responsible for adhering to this policy and reporting any security incidents or concerns.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

# Summary

This Records Appraisal Procedure ensures that records related to the IoT Security Framework are managed effectively and efficiently. By adhering to this procedure, the organisation can minimise risks, optimise resources, and preserve valuable information while complying with legal and regulatory requirements.

# 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