# Purpose

The purpose of this procedure is to define the risk assessment approach related to information assets of the Electronics Department.

# Scope

It is applicable to all information assets in the Electronics Department.

# Definitions

In this document, information security related terms have been marked in *underlined* *italics*. For their definitions, refer to the standard *EE-ISMS-S001 Terms and Definitions*.

# Entry Criteria

* A new information asset has been identified and needs to be evaluated for risks
* Or, new risks and associated threats have been identified
* Or, it is time for periodic risk assessment

# Inputs

* New information asset, risk, or threat
* Current risk assessment matrix

# Procedure

This procedure is based on The OCTAVE Allegro risk assessment methodology. One must read and understand the details of the methodology before executing this procedure. The EE Asset and Risk Profile must be referred to and updated when executing this procedure. It can be performed by anyone but is generally carried out by the Information Security Manager (referred to as the Assessor below).

|  |  |  |
| --- | --- | --- |
| **Step** | **Role** | **Action** |
| 1 | Assessor | **Risk Measurement Criteria.** The following risk impact areas have been identified and prioritized to measure a risk’s effect on EE Department’s mission (refer to ‘Impact Areas’ in the EE Asset and Risk Profile):   * NSCL’s Quality Objective: impact of a risk on lab’s quality objectives. See NSCL’s quality policy and objective. * NSCL’s and EE Department’s Reputation: * Employee Productivity: * Employee Safety and Health * Financial: Operating or one-time financial losses * Legal: Fines and lawsuits * Critical Project Impact: Impact of risks on schedule and cost of critical projects   If needed, refine the impact areas or the priorities, and update the EE Asset and Risk Profile. Changes to impact areas or their priorities must be approved by the Electronics Department Head. |
| 2 | Assessor | **Information Asset Profile**. Identify *information assets* in the department. For each asset perform the following:   * Assign an identifier * Describe the asset and the rationale for its selection * Identify the person responsible for the asset (its owner). * Record the security requirements for its Confidentiality, Integrity, and Availability. * Identify the most important security requirement * Record the above information in the Asset Risk Profiles (R01-Asset-Risk-Profiles.xlsx) |
| 3 | Assessor | **Information Asset Containers.** Identify the containers in which the information asset is stored, transported, or processed. Information containers can be categorized into:   * Technical (examples: software, databases, servers) * Physical (examples: paper, folders) * Human (examples: only Joe knows the formula or process).   For each category, identify both internal (inside the department) and external (such as vendors and partners) containers. |
| 4 | Assessor | **Identify Areas of Concern.** For each information-asset container, identify real-world conditions or situations that could affect the information asset.  Example: Incorrect file permissions on the on the file server containing the Electronics Department’s manuals’ directory, may allow an employee to delete or alter a manual. |
| 5 | Assessor | **Identify Threat Scenarios.** Expand the areas of concern by identifying the actors, means, motives, and outcomes. This can done by looking at following categories of threats:   * Human actors: The threats to department’s infrastructure or containers by a person. The person may use technical or physical means, and the motive can be deliberate or accidental. * Technical problems: The threats are from software defects, system crashes, hardware defects, or malicious code. * Other problems: Actor: These threats from power supply failures, telecommunications, third-party, or natural disasters.   The outcome in each case is one of the following:   * Disclosure of information * Modification of information * Interruption of information * Destruction or loss of information   Identify the probability of occurrence of each threat scenario and categorize it as Low, Medium, or High. |
| 6 | Assessor | **Identify Risks:** For each threat scenario, evaluate the consequences (impact) on the department. Note: Risk = Threat + Impact  Example:   * Threat Scenario: Malicious modification of PLC software. * Consequence: The interlocks will not function properly resulting in injury or death of personnel. |
| 7 | Assessor | **Analyze Risks.** Based on the Risk Measurement Criteria (Step 1), evaluate the consequences of every risk on each of the impact areas, and assign it an impact value. The impact values are shown below:   |  |  | | --- | --- | | Impact | Value | | No Impact | 0 | | Low | 1 | | Medium | 2 | | High | 3 |   Multiply the priority of an impact area and its impact value, and sum up all the products to obtain the Relative Risk Score for the risk.  Example:  Risk – Inadvertent modification of EPICS channel values   |  |  |  |  | | --- | --- | --- | --- | | Impact Area (IA) | IA Priority | Impact Value | Score | | Safety and Health | 5 | Low (1) | 5 | | Reputation | 4 | Med (2) | 8 | | Financial | 3 | High (3) | 9 | | Legal | 2 | None (0) | 0 | | Productivity | 1 | Low (1) | 1 | | Relative Risk Score | | | 23 | |
| 8 | Assessor | **Select Mitigation Approach.** Based on the relative risk score and probability of risk occurrence, categorize the risks by using the Relative Risk Matrix. Here is an example of such a matrix:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Probability | Relative Risk Score | | | | | 60+ | 40 to 59 | 20 to 39 | 0 to 19 | | High | Level I | Level I | Level II | Level III | | Medium | Level I | Level II | Level II | Level IV | | Low | Level II | Level II | Level III | Level IV |   Based on the risk category from the above matrix, choose one of the following mitigation strategies:   * Accept: Accept the consequences by taking no action. Risks that are accepted should have low impact (low risk score). * Mitigate: Implement controls to counter the underlying threat or minimize the impact or both. Some risks may be transferred to other parties (for example by purchasing insurance). * Defer: Risk is neither mitigated nor deferred because additional analysis needs to be performed. Deferred risks are monitored and re-evaluated in future. |

# Outputs

* Updated Asset and Risk Profile

# Exit Criteria

* Updated Asset and Risk Profile is approved by the Information Security Board

# Exceptions

All exceptions must be approved by the Electronics Department Head.

# References

* 1. *M01 NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P501 Information Security Policy,* NSCL Document Server, Electronics Folder
  3. *Asset Risk Profile, R01-Asset-Risk-Profile.xlsx,* NSCL Document Server, Electronics Folder
  4. *NSCL Quality Policy and Objectives*, NSCL Document Server, QMS Folder

# Revision History

|  |  |  |
| --- | --- | --- |
| Revision  Level | Date | Revision Changes |
|  |  |  |

# Reviews

|  |  |
| --- | --- |
| Reviewer | Review Date |
| Information Security Working Group |  |

**Approved**

**Department Head:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Approval Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Effective Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**