# Purpose

The purpose of this procedure is to establish, implement, operate, monitor, review, maintain and improve Argus, the Information Security Management System (ISMS), used for managing information security risks at the Electronics Department of NSCL.

# 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



# Inputs



# Procedure

The following procedure must be executed at least once annually. It is based on the ISO/IEC 27001 standard. The Electronics Department Head is responsible for executing the procedure.

|  |  |  |
| --- | --- | --- |
| **Step** | **Role** | **Action** |
| 1 |  | **Establish Argus (the ISMS)** |
| 1.a | EEDH | **ISMS Scope.** Define the scope and boundary of the iSMS in terms of the organization, its locations, assets and technologies, and exclusions from the scope. Argus’ scope is defined in “ISMS-EE-P001: Argus Scope”. |
| 1.b | EEDH | **ISMS Policy**. Formulate a policy, approved by the management, which establishes an overall sense of direction with regard to information security. It should establish the risk evaluation criteria, and take into account legal, regulatory and contractual requirements, Argus’ ISMS policy is defined in “ISMS-EE-P002: Argus ISMS Policy”. |
| 1.c | EEDH | **Risk Assessment Approach.** Define an approach to identify, evaluate, and treat risks faced by the organization. This methodology, for Argus, is defined in “ISMS-EE-P003: Risk Assessment Policy” and “ISMS-EE-R001: Risk Assessment Procedure”. |
| 1.d | EEDH | **Identify Risks.** Identify the risks by following the approach from the previous step. This involves identifying the information assets of the organization, threats to them, their vulnerabilities, and the impact of the threats. For Argus, the risks are documented in “ISMS-EE-D002: Argus Risk Profile”. |
| 1.e | EEDH | **Analyze Risks.** Analyze and evaluate the risks from last step. Establish the risk level by assessing the probability of security failures and their consequences. Determine whether the risks have to treated or accepted. The risk analysis of Argus is documented in “ISMS-EE-D002: Argus Risk Profile”.. |
| 1.f | EEDH | **Risk Treatment:** Identify and evaluate the options for the treatment of non-acceptable risks by applying appropriate controls. In Argus, the treatment options of the identified risks are defined in “ISMS-EE-D002: Argus Risk Profile” |
| 1.g | EEDH | **Controls Selection.** Select the control objectives and controls for the treatment of risks. For Argus, this is done in “ISMS-EE-D002: Argus Risk Profile”. Section *Argus Controls* describes these controls in more detail. |
| 1.h | EEDH | **Management Approval.** Obtain management’s approval for the residual risk, and for implementing and operating the ISMS. |
| 1.i | EEDH | **Statement of Applicability:** Prepare the Statement of Applicability (SoA), which lists the selected, already-implemented, and excluded controls. |
| 2 | EEDH | **Implement and Operate Argus** |
| 2.a | EEDH | **Risk Treatment Plan:** Develop a Risk treatment plan (RTP) that identifies the management action, resources, responsibilities, and priorities for managing information security risks. |
| 2.b | EEDH | **Implement RTP:**  Implement the RTP to achieve the identified control objectives (see 1.g) |
| 2.c | EEDH | **Implement Controls:** Implement the controls (1.g) to achieve the control objectives. |
| 2.d | EEDH | **Measurement**: Measurement of effectiveness of controls |
| 2.e | EEDH | **Training:** Implement training and awareness programs. |
| 2.f | EEDH | **Manage Argus:** Manage operations and resources for Argus |
| 2.g | EEDH | **Incident Management:** Implement the procedures, , to enable prompt detection of security events and response to security incidents. |
| 3 | EEDH | **Monitor and Review** |
| 3.a | EEDH | Execute monitoring and review procedures described in |
| 3.b | EEDH | **Reviews:** Undertake regular reviews of the effectiveness of the ISMS taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties. |
| 3.c | EEDH | **Measure Controls:** Measure the effectiveness of controls to verify that security requirements have been met. |
| 3.d | EEDH | **Review:** Review the risk assessments, the residual risks, and the identified acceptable levels of risks, taking into account changes to the Electronics Department, technology, business objectives and processes, identified threats, effectiveness of implemented controls, and external events such as changes to legal or regulatory environment. |
| 3.e | EEDH | **Internal Audit:** Conduct internal audits as per …. |
| 3.f | EEDH | **Management Review:** Conduct management review of Argus as per… |
| 3.g | EEDH | **Update Plans:** Update security plans to take into account the findings of the monitoring and review activities |
| 3.h | EEDH | **Record Actions:** Record actions and events that can have an impact on the effectiveness and performance of Argus |
| 4 | EEDH | **Maintain and Improve Argus** |
| 4.a | EEDH | **Implement Improvements:** Implement identified improvements to ISMS |
| 4.b | EEDH | **Corrective and Preventive Actions:** Take corrective and preventive actions as per ….. |
| 4.c | EEDH | **Communicate:** Communicate the actions and improvements to all stakeholders |
| 4.d | EEDH | **Ensure Results:** Ensure that the improvements achieve their intended objectives |
|  |  |  |

# Outputs

* Improved ISMS

# Exit Criteria

* Improvements are approved, and a new iteration of PDCA is to begin

# 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**