# Purpose

Argus is the Information Security Management System (ISMS) used for managing information security risks at the Electronics Department of NSCL. The purpose of this procedure is to ensure that Argus is established, implemented, operated, monitored, reviewed, maintained and improved according to the International Standard and to the information security requirements established by the Electronics Department.

# Scope

It is applicable to the ISMS 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

* An internal audit has been initiated

# Inputs

* The ISMS

# 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 | EEDH | Schedule and initiate internal audit (at least once annually). |
| 2 | Lead Auditor | Document the scope of the audit on the Internal Audit Plan (IAP). Conduct an opening meeting with the group leaders in the department. |
| 3 | Audit Team | Perform the audit as per the IAP. Determine whether the ISMS conforms to the ISO/IEC 27001 standard, and to the information security requirements established by the department, and is effectively implemented and managed. |
| 4 | Audit Team | Write up any preventive or corrective action requests. |
| 5 | Lead Auditor | Ensure that the IAP has been implemented. Complete the Audit Summary Matrix from the IAP as a record the elements of the standard and areas audited. |
| 6 | Lead Auditor | Conduct a closing meeting with the group leaders, and explain non-conformances if any. Documents all non-conformances and the audit plan in the Trouble Report System in accordance with *Argus Preventive and Corrective Action Procedure*. |
| 7 | EEDH | Request preventive or corrective actions from the appropriate groups. Follow up on the requested preventive and corrective actions. |
| 8 | EEDH | Close the internal audit. The preventive and corrective actions do not have to be completed to close the internal audit. |

# Outputs

* Audit findings
* Preventive and corrective actions

# Exit Criteria

* The internal audit is closed.

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