# Purpose

Whenever a security breach occurs or a weakness in the security of information systems is noticed, it must be reported and escalated to the proper authorities, so that corrective action can be taken. This policy ensures that security incidents that may have potential impact on the normal operations of the department are identified, contained, and addressed in a timely fashion.

# Scope

This policy is applicable to all users of the 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*.

# Policy Statement

* 1. Users must report security incidents promptly.
  2. Security incidents must be analyzed, preventive and corrective actions must be taken to minimize the recurrence of the incident in a timely manner.
  3. All incidents and their analyses must be logged.
  4. Based on the incident, evidence should be collected, retained, and presented as per the processes in the relevant jurisdictions.
  5. Report on security incidents must be reviewed periodically by the management.
  6. Disciplinary action, if appropriate, must be initiated to address security incidents.

# Exceptions

# References

* 1. *M01 NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *EE-ISMS-S001 Terms and Definitions,* NSCL Document Server, Electronics Folder

# Revision History

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

# Reviews

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

**Approved**

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

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