# Purpose

The information assets, their containers, and processing facilities should be sited in physically secure areas. They must be protected from unauthorized access, damage, interference, with appropriate security barriers and entry controls. The purpose of this policy is to protect the information assets from misuse, unauthorized access, and technical and environmental hazards.

# Scope

This policy is applicable to all *information assets* of 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*.

# Policy Statement

* 1. *Information assets* must be protected through security perimeters such as walls, card-controlled gates, or manned reception desk. The strength of the security perimeter must be commensurate with the sensitivity of the information.
  2. All users must be made aware of their responsibilities and obligations with respect to physical security.
  3. *Information asset owners* shall be accountable for the loss and damage of the *information asset*.
  4. *Information asset*, *information asset container*, or *information processing facility* must not be taken out of premises without prior authorization.
  5. *Information asset containers* must be protected from disruptions caused by failures in supporting utilities such as power and air-conditioning.
  6. Cables used for carrying data or for supporting information services, such as network and power cables, must be protected from interception and damage.
  7. Only authorized personnel must have access to *information asset containers*. Access rights to these containers must be periodically reviewed.
  8. *Information asset containers* must be protected from natural or man-made disasters such as fire, flood, earthquake, explosion, and civil unrest.
  9. Confidential information (in the form of removable media or documents) must be returned to a safe location or appropriately disposed of by the *information asset owners*.
  10. All users must follow NSCL’s health and safety regulations and standards.
  11. Users must guard all sensitive information through clean desk and clear screen procedures.
  12. All incoming and outgoing material must be inspected for potential hazards.
  13. Prior to disposing any equipment, all information assets stored on it must be removed. This includes peripherals such as printers, plotters, and fax machines.

# Exceptions

# References

* 1. *Electronics Department ISMS Manual*, 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**