# Purpose

The purpose of this policy is to control access to information assets, and the relevant systems including but not limited to computing facilities, networks, and applications. Information assets can be accessed through several technical mechanisms such as computer applications, networks, servers, workstations, etc; or through non-technical mechanisms such physical access, keys, verbal communications etc.

# Scope

This policy applies to all NSCL Electronics Department users.

# 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. Access to every information asset in the Electronics Department must be controlled. An information asset must be accessible to an information consumer only if the consumer has the appropriate authorization. This holds for all systems, manual or automated, that provide access to information assets.
  2. Access controls to an information asset must not be modified without prior authorization of the Electronics Department Head (EEDH).
  3. Any change in access controls must have prior approval of the Electronics Department Head.
  4. Users are responsible for the information in their possession, and must protect it from unauthorized access.
  5. Information assets, containers, and access mechanisms must be adequately protected from unauthorized access.
  6. EEDH must review access to all information assets on a periodic basis, at least once a year.
  7. Users must not connect any equipment to the Electronic Department’s networks without prior authorization from the department head.
  8. Networks that are essential to the operation of the facility, such as Control and DAQ Networks, must be isolated from all other networks.
  9. Information assets and their containers must not be directly accessible from the Internet without prior authorization from the Electronics Department Head.
  10. All failed attempts to access information systems must be logged. Such failed attempts must be reviewed periodically
  11. Information systems must automatically logout users after certain period of inactivity. Users must re-authenticate themselves after the timeout.

# Exceptions

* 1. Access to information assets that are classified as *public* need not be controlled.

# References

* 1. *NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P0501 Information Security Policy,* 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**