# Purpose

The objective of this policy is to control access to the department’s network.

# Scope

This policy covers all of department networks. It also applies to users who access the network locally or remotely.

# 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 not connect any new devices onto network without getting prior approval from the Electronics Department Head.
  2. Network connectivity among various local and remote devices must be controlled and managed by ITG.
  3. The network shall have appropriate secured gateways and firewalls to segregate various networks: control, office, production, commissioning, and test networks.
  4. Appropriate network routing controls must be defined for protection of department network from external world.
  5. A user must be authenticated before he or she is granted remote access.
  6. All communication during remote access must be encrypted.
  7. ITG must maintain remote access logs for a period of 3 months. ITG must monitor the remote access logs for intrusion detection.
  8. Remote access users must not allow non-NSCL users, such as family and friends, to access Electronics Department’s internal resources.

# Exceptions

# References

* 1. *M01 NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P501 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**