# Purpose

Unauthorized changes to Programmable Logics Controllers’ [PLC] logic can lead to catastrophic consequence including damage to the laboratory’s equipment, and human life. The purpose of this policy is to control modifications to PLCs.

# Scope

This policy is applicable to all the PLCs in operation.

# 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. Changes to software on production PLCs must be managed through a change control process.
  2. All deployments on production PLCs must be approved by the affected area managers.
  3. It must not be possible to deploy software on production PLCs unless physically or logically approved by the affected *area managers*.
  4. Network access to production PLCs must be restricted.

# Exceptions

# References

* 1. *M01 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**