# Purpose

To provide rules and standards for the secure management, operation, and maintenance of National Superconducting Cyclotron Laboratory’s (NSCL) control system.

# Scope

This policy applies to all users and processes that access *Laboratory Control System (LCS)*.

# Definitions

* 1. *Access Control List (ACL)*: A list of *Users* and their associated access privileges used to control access to resources. A user may be listed in more than one *ACL*.
  2. *Control Console*: Dedicated computers, located in designated access controlled control rooms, used for accessing *LCS*.
  3. *Control Network*: The network interconnections and associated hardware exclusively used to interconnect all devices of *LCS* and to connect LCS to other networks.
  4. *Control System Security Manager (CSSM)*: A role assigned to a single individual selected by the laboratory director, The responsibilities of the CSSM are:
     1. *Authorizes all access to the control system based on NTA for Users and Processes*
     2. *Enforces this policy*
     3. *Maintains ACLs for LCS*
     4. *Works with recognized experts as appropriate to ensure control system security*
  5. *Field Console*: Dedicated computers, located in open restricted areas of the laboratory, used for accessing *LCS*.
  6. *Laboratory Control System (LCS)*: The system at NSCL that supervises and controls the equipment that is used in the production and delivery of rare isotope beams to the experiment. This includes the IOC’s, PLCs, embedded controllers, networks, etc
  7. *Machine*: The set of all devices controlled by *LCS*.
  8. *Machine State*: The combined values of all the machine *PVs* at any defined instant.
  9. *Need To Access (NTA)*: Need for access to *LCS* for a recognized NSCL business purpose as determined by *CSSM*.
  10. *Owner*: A person who is responsible for a *User Component*.
  11. *Process*: A computer program that accesses *LCS*.
  12. *Process Variable (PV)*: An analog or digital variable defined in *LCS* used to monitor or control an individual device or process state.
  13. *User*: An individual with authorized access to *LCS*.
  14. *User Component*: Devices or computers used to access *LCS* but not controlled by *LCS*.

# Policy Statement

* 1. The laboratory control system shall be accessible only to those authorized users and processes that have a legitimate laboratory business need.

# Policy Requirements

* 1. Access
     1. By default, all laboratory computer accounts recognized by LCS shall have read access to LCS PVs
     2. Each *Field Console* shall have an associated ACL that is maintained by the *CSSM*
     3. All write access to *LCS* *PVs* must be based on *NTA* and authorized by the *CSSM*
     4. Direct physical connections to the *Control Network* must be authorized by the *CSSM*.
     5. All access from outside the *Control Network* shall be controlled. The access shall be specified by the CSSM. The access should be controlled through secure gateway devices and associated ACLs.
     6. All *Processes* and *Users* that have write access to *LCS* must be documented and reviewed periodically.
     7. The *CSSM* is responsible for identifying changes to LCS, whether authorized or not, that may affect security.
     8. *Users* are responsible for gaining authorization from *CSSM* before making any changes to the *LCS* that may affect security.
     9. *Owners* are responsible for restricting access to *LCS* from their *User* *Components*.
     10. Access to *LCS* configuration data and *ACLs* shall be secured.
  2. Computers & Consoles
     1. Access to *LCS* through *Field Consoles* must be controlled. *Field Consoles* must automatically logout following a period of inactivity as specified by the *CSSM*.
     2. Generic accounts, having write access to LCS, are exclusively owned and controlled by CSSM and shall only be used for logging into specific *LCS Control* and *Field Consoles*. Generic account access to field consoles may only be used by experimenters with an active experimental need.
  3. Logging
     1. All write attempts to *LCS Process Variables* from outside the *Control Network* shall be automatically logged.
     2. All attempts to access the *Control Network* from outside the *Control Network* shall be automatically logged.
     3. All new direct physical connections to the *Control Network* shall be automatically logged.
     4. *CSSM* shall manage the security risks to *LCS* by maintaining a formal risk registry.

# Exceptions

# References

# Revision History

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

# Reviews

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

**Approved**

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

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