# Purpose

The objective of this policy is to control access to NSCL’s Control System.

# Scope

This policy applies to all NSCL users who require access to NSCL’s Control System.

# Definitions

* NSCL’s Control System: The system that supervises and controls NSCL’s operational facility. This includes the IOCs, PLCs, embedded controllers, networks, etc.
* Machine: The set of components used to produce isotope beams at NSCL. This includes the source, the accelerators (cyclotrons), the fragment separator, the detectors, and the utilities (cryogenics, vaccum, water etc).
* Machine State: The combined state of all the components of the machine. It is the collective values of all the Process Variables associated with all the devices in the machine.
* Control System User: Someone who accesses the state of the machine. This includes NSCL employees, students, experimenters, control applications, and controllers.
* Control Network: The network that connects all the devices on NSCL’s control system.
* Control Console:
* Field Console:

# Policy Statement

* 1. All control system users shall have read access to the state of the machine.
  2. All control system users, directly connected to the control network, shall be able to change the state of the machine.
  3. Control system users, who are not directly connected to the control network, must be authorized to be able to modify the state of the machine. Access to the list of such authorized users must be controlled. This may be implemented using Access Control Lists (ACLs) on EPICS gateways.
  4. Access to the control network shall be controlled. A device shall not be connected to the control network without the prior authorizations of the Operations Department Head and the Electronics Department Head.
  5. Access to Control Consoles shall be controlled. No one shall access a control console without the prior authorization of the Operations Department Head.
  6. The Experimenters shall be granted temporary authorizations to change the machine state and access the control consoles. The authorizations shall be revoked once the experiment has concluded.
  7. A Field Console must be locked or logged off if it is not in use or if the logged-in user is not physically present at the console.
  8. Generic accounts shall not be used to login to Control Consoles. However, it is permissible to use automatic logins instead.
  9. Physical access to Control Consoles must be restricted. This may be implemented using physical access control mechanisms such as access cards or keypad locks on doors of the control rooms (Main, ECR, Cryo etc).

# Exceptions

# References

# Revision History

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

# Reviews

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

**Approved**

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

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