# Purpose

The objective of this procedure to restrict access to the laboratory control system so that it is accessible only to authorized users and processes as per the Control System Access Policy [10.1].

# Scope

This procedure applies to the design of the laboratory control system. CSSM is responsible for the implementation of this procedure.

# Definitions

* 1. *Secure Interconnection Device (SID)*: A device that enables connections among two or more computer networks in a secure and controlled fashion. The connections could be at any networking layer. Examples: Firewalls, SSH gateways, EPICS gateways, and HTTP proxy servers.

See the Control System Access Policy [10.1] for more definitions.

# Entry Criteria:

# Not applicable

# Inputs

Not applicable

# Procedure

**Risks**:

* 1. Identify and analyze risks to *LCS*.
  2. List the residual risks in the risk registry.
  3. Obtain *CSSM*’s acceptance for residual risks before implementing any mitigating controls.

**Access Control:**

* 1. Isolate the Control Network from other networks. The only way to access the *Control* *Network* from outside the *Control Network* should be through *SIDs*. Configure the *SIDs*, using ACLs, to limit the connections to/from the *Control Network*. An example architecture is shown in the following diagram:

The Internet

NSCL Core

MSU Core

Firewall

EPICS Gateway-2

SSH Gateway

Firewall

* 1. Minimize the number of *SIDs* as much as possible.
  2. Develop laboratory’s hardening standards for the *SID* platforms, based on the industry standards [10.2, 10.3]. Secure the *SIDs* as per the laboratory’s hardening standards.
  3. Restrict access to *SID* configurations using *ACLs*.
  4. *CSSM* is the owner and responsible authority for the *SIDs*. Obtain approval from the *CSSM* before making changes to a *SID’s* configuration
  5. Setup network services, such as DHCP, on the *Control Network* such that only authorized devices on the *Control Network* can avail the services.

**Computers and Consoles**

* 1. Restrict logins to the *Field and Control Consoles* to authorized users only.
  2. Disallow remote logins to *Field and Control Consoles*.
  3. Set up the *Field Consoles* to automatically logoff the user, or lock the screen, after a period of inactivity.
  4. This step is optional. Set up *Control Consoles* to automatically login to a generic account immediately after start up. Disable the passwords on such generic accounts.
  5. Restrict the generic accounts such that they can login to only the *Field and Control Consoles*.

**Logging**:

* 1. Configure *SIDs* to log all connections and operations. EPICS Gateways need not log read operations.
  2. Configure network infrastructure, such as Ethernet switches, on the *Control Network* such that a log entry is automatically created whenever a device is connected to the network.

# Outputs

Not applicable

# Exit Criteria

Not applicable

# Exceptions

* 1. All exceptions to this procedure must be approved by *CSSM.*

# References

* 1. *Control System Access Policy*, NSCL Document Server, Electronics Folder
  2. *Guide to General Server Security,* NIST
  3. *Securing Network Servers*, SEI CMU

# Revision History

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

# Reviews

|  |  |
| --- | --- |
| Reviewer | Review Date |
|  |  |

**Approved**

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

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