1. **Policy**

*The laboratory control system is only to be accessed by authorized users and processes that have a legitimate laboratory business need.*

* 1. **Scope**

*This policy applies to all users and processes with access to the laboratory control system.*

* 1. **Purpose**

*To provide rules and standards for the secure management, operation, and maintenance of the laboratory control system.*

* 1. **Policy Requirements**
     1. **Access**
        1. *By default, all laboratory computer accounts recognized by the LCS shall have read access to the LCS PV’s.*
        2. *Each field console shall have an associated ACL that is maintained by the CSSM.*
        3. *All write access to the LCS PV’s 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 through secure gateway devices and associated ACL’s controlled and specified by the CSSM.*
        6. *All Processes and Users that have write access to the LCS must be documented and reviewed periodically.*
        7. *The CSSM is responsible to identify changes to the LCS, whether authorized or not, that may affect security.*
        8. *Users are responsible for gaining authorization from the CSSM before making any changes to the LCS that may affect security.*
        9. *Owners are responsible for restricting access to the LCS from their User Components.*
        10. Access to ACL’s and LCS configuration data shall be secured.
     2. **Computers & Consoles**
        1. *Field Consoles must automatically logout following a period of inactivity as specified by the CSSM.*
        2. *Generic accounts are exclusively owned and controlled by the CSSM and shall only be used for login to 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. *The CSSM shall maintain a formal risk registry.*

1. **Definitions & Requirements** 
   1. **Laboratory Control System (LCS)**

*The system that supervises and controls the laboratory research equipment not specifically designated as controlled by an alternate system. This includes the IOC’s, PLCs, embedded controllers, networks, etc.*

* 1. **Control Network**

*The network interconnections and associated hardware exclusively used to interconnect all devices of the LCS and to connect the LCS to other networks.*

* 1. ***Control Console***

*Dedicated LCS computers located in designated access controlled control rooms.*

* 1. ***Field Console***

*Dedicated LCS computers located in open restricted areas of the laboratory.*

* 1. ***User Component***

*Devices or computers not controlled by the LCS used for LCS access.*

* 1. ***Process Variable (PV)***

*An analog or digital variable defined in the LCS used to monitor or control an individual device or process state.*

* 1. ***Process***

*A computer program that accesses the LCS.*

* 1. ***Owner***

*Owner of a User Component.*

* 1. ***User***

*An individual with authorized access to the LCS.*

* 1. ***Machine***

*The set of all devices controlled by the LCS.*

* 1. ***Machine State***

*The combined values of all the machine PV’s at any defined instant.*

* 1. ***Access Control List (ACL)***

*A list of Users and their associated access privileges used by a computer system to control access to resources. As many ACL’s exist as unique access privilege sets are required and a user may be listed in more than one ACL.*

* 1. ***Need To Access (NTA)***
     1. *Need for access to the control system for a recognized laboratory business purpose as determined by the CSSM.*
  2. ***Control System Security Manager (CSSM)***
     1. *A role assigned to a single individual selected by the laboratory director.*
     2. *Authorizes all access to the control system based on NTA for Users and Processes.*
     3. *Enforces this policy*
     4. *Maintains the ACL’s identifying the control system authorized Users and associated access to control system resources.*
     5. *Works with recognized experts as appropriate to ensure control system security.*

1. **Policy History**

|  |  |  |
| --- | --- | --- |
|  | | |
| **Revision**  **Level:** | **Date:** | **Revision Changes:** |
|  |  |  |
|  |  |  |

**Associate Directors’ input:** Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Technical Group input:** Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Approved**

**Laboratory Director:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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