# Critical Purpose

The design and implementation of *information systems,* used for supporting the business processes of the Electronics Department, are crucial for security. The objective of this policy is to ensure that security is integral part of *information systems*’ development lifecycle.

# Scope

This policy is applicable to all *information systems* in the Electronics Department.

# 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. Security requirements must be defined for all projects during the planning phase.
  2. System Development Policies
     1. Requirement specifications must include security requirements.
     2. Based on the requirements, redundancy and fault tolerance must be designed for the *critical information assets*.
     3. Input and output data must be validated to ensure that it is correct and appropriate.
     4. Validation checks must be implemented in applications to detect corruption of data, to guard against defects or malicious attacks.
     5. Communication among systems must be secured as per the requirements specified in R03 Access Control Matrix.
     6. Test data must be similar to operational data. However, personal data must not be used for testing. Sensitive test data must be protected, and removed from test environment.
     7. Migration of systems from development to operation must be controlled. It must be approved by all stakeholders. *Information systems* must not be deployed without prior authorization of the *area managers*.
     8. The system developer must not include special entry points into the system to gain access thus subverting the system security.
     9. Configurations of all systems must be managed. A configuration management or version control system must be used to manage the various configurations.
     10. Access to source code and system documentation must be controlled.
     11. Production environment must be isolated from development and test environments.
     12. Code reviews must be performed to check for vulnerabilities. Applications must be checked for covert functionalities (Trojan Horses, Backdoors etc). Sensitive information such as passwords must not be embedded in the source code. Applications must handle exceptions gracefully. Allocated of resources, such as memory and database connections, must be released properly. The code must conform to the set programming standards. Automated tools must be used to check for vulnerabilities such as a memory leaks, buffer overflows etc.
     13. All systems must log critical errors.
     14. All systems must maintain detailed documentation on their relationships and interfaces to other systems.
     15. The system owner must monitor and supervise outsourced system development for security requirements.
  3. System Operation Policies
     1. Once a system is in operation, it must be monitored for errors and failures. In cases of errors and failures, the application owner and system administrator must be notified.
     2. The data needed for the operation of the system, and the data generated by the system must be archived appropriately to recover from disasters.
     3. Whenever applicable, the data must be retained to conform to appropriate regulatory requirements.
     4. Upgrades to existing systems must be planned and approved. The impact of the upgrade must be analyzed. Systems must be evaluated for capacity for upgrades. Acceptance criteria for upgrades must be defined and tested.
     5. In case of unforeseen problems with upgrades, there must be provisions in place to revert to earlier versions of the system.
     6. Changes to a system must be reflected in its documentation. All the documentation must be upgraded to match the changes, before the system is deployed.

# Exceptions

# References

* 1. *M01 NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P0501 Information Security Policy,* NSCL Document Server, Electronics Folder
  3. *P1001 Change Management Policy,* NSCL Document Server, Electronics Folder
  4. *P1203 Vulnerability Management Policy,* NSCL Document Server, Electronics Folder
  5. *R03 Access Control Matrix,* 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**