# Purpose

Failures of hardware or software systems can result in loss or corruption of critical data. The purpose of this policy is to ensure integrity and availability of business critical data to support business continuity by conducting periodic backups and restoration tests.

# Scope

This policy applies to all systems that contain *information assets*. This includes but is not limited to file-systems, databases, source code, operating systems, and configuration information.

# 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. Users must not store critical information on their workstation’s local storage devices. Data storage locations that are backed up must be identified, and communicated to the users.
  2. Information owners must identify the data to be backed up, and the periodicity of the backup.
  3. Data must be backed up on appropriate media based on the criticality of the data and its retention.
  4. Backup media must be labeled appropriately. It must be classified based on classification policy, and handled accordingly.
  5. Backups of critical information must be stored at one or more off-site locations. The off-site locations must be identified and approved by the Information Security Board. The integrity and confidentiality of data must be preserved during transportation to off-site locations.
  6. Logs of backups must be maintained.
  7. Backups must be periodically verified through restoration tests. The restoration tests and results must be logged.
  8. Information managed by an application must be backed up using application specific methods. For example, data in a database must be backed up using the method specified by the database management system.

# Exceptions

* 1. Only data stored on identified data storage locations are backed up. The data stored on the local storage devices of a workstation may not be backed up. It is the responsibility of the user to backup such data.

# References

* 1. *NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P0501 Information Security Policy,* 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**