# Purpose

A common cause of system and security failures is ad-hoc changes to information processing facilities and systems. Changes to operational systems must be made only when there is a business need to do so. Upgrading to the latest version of operating system or application software may not be in an organization’s best interest as the upgrades may introduce new vulnerabilities or instabilities. The purpose of this policy is to ensure that the changes to operational systems are controlled.

# Scope

This policy applies to all change activities to the information systems of 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. Changes to *critical information assets* and systems must be planned.
  2. Potential impact of all changes must be assessed. They must be authorized and documented.
  3. Changes in any information processing facility or system must be carried out in a manner that does not compromise the security of existing systems or cause any security failure.
  4. Impacted users must be informed before the implementation of a change.
  5. There must be a plan to recover from unsuccessful changes.
  6. During the executing of a change, access must be granted only to the relevant application and systems.
  7. The implementation, approval, and requisition of a change must not be done by the same person. These duties must be segregated among multiple people to provide for checks and balances.
  8. A changed system must be first tested fully for its functionality. Changes must be tested on a test system before they are implemented on the production system. The test environment must be separated from the production environment.

# Exceptions

* 1. Emergency changes may be implemented without a plan. However, they must be analyzed for impact and authorized by the asset owner. The impacted users must be informed of the change in a timely manner. The changes must be documented promptly following the change.

# References

* 1. *Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *EE-ISMS-S001 Terms and Definitions,* 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**