# Purpose

Many information systems, especially operating systems, publish their technical vulnerabilities, and provide fixes for them in the form of patches. The purpose of this policy is to manage the published technical vulnerabilities so as to reduce risks resulting from them.

# Scope

This policy is applicable to all business critical applications of the 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. Information about technical vulnerabilities must be obtained from genuine sources, which include vendor mailing list, security alert announcements, and virus bulletins,
  2. Patches must be evaluated for applicability, and then applied as soon as possible.
  3. Information regarding patch applications must be announced to the appropriate users, before the patches are applied.
  4. Patch applications must adhere to the Change Management policy.
  5. Suitable tools and technologies must be used for patch management. Status of patch application must be reported periodically.

# Exceptions

# References

* 1. *M01 NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P501 Information Security Policy,* NSCL Document Server, Electronics Folder
  3. *P1001 Change Management 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**