# Purpose

Disasters, natural or deliberate, can result in loss of information assets or a prolonged disruption to their access. This in turn can cause severe interruption to the business activities of the Electronics Department. The objective of this policy is to minimize the impact of major failures of information systems on the critical business processes of the Electronics Department and to ensure their timely resumption.

# Scope

This policy is applicable to all units within the Electronics Department. The Electronics Department Head is responsible for the implementation of this policy.

# 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. The department must assess the risks of disasters on its critical information assets. The department must identify the events that can cause severe disruption to the department’s activities due to loss of access to information assets; it must evaluate their probability of occurrence and their impact.
  2. Based on the risk assessment, the department must develop a *Business Continuity Plan* (BCP-IS) that addresses the information security requirements needed for the department’s business continuity. The plan must include:
     + Preventive and mitigating controls for the identified risks
     + Criteria for qualifying an event as a disaster
     + Procedure(s) to recover the department’s critical processes
  3. The department must implement the BCP-IS. The department must inform each employee of the BCP-IS and his or her role, if any, in the plan.
  4. The BCP-IS and related documents must be stored such that they are easily accessible during disasters.
  5. The department must keep the BCP-IS up to date. Changes in the security requirements, risk assessment, and organization structure must be reflected in the BCP immediately. The department must review the BCP-IS at least once every year.
  6. To ensure the effectiveness of the BCP-IS, the department must test it at least once every year.
  7. During recovery, all users must comply with the established management systems, such as quality and environmental safety, unless exceptions are granted by the Electronics Department Head,

# Exceptions

* 1. The policy is limited to the information security requirements of the department:

# References

* 1. *M01 NSCL Electronics Department ISMS Manual*, NSCL Document Server, Electronics Folder
  2. *P501 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**