|  |  |  |
| --- | --- | --- |
| nscl.PNG | National Superconducting Cyclotron Laboratory | msu.png |

Electronics Department ISMS Manual

|  |  |  |  |
| --- | --- | --- | --- |
|  | Name | Signature | Date |
| Prepared By | Vasu V |  |  |
| Reviewed By | Jay Kusler, Kelly Davidson |  |  |
| Approved By | John V |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | 7/15/10 | Vasu V | Initial |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 4](#_Toc314532762)

[1.1 What is an ISMS? 4](#_Toc314532763)

[1.1.1 What is Information? 4](#_Toc314532764)

[1.1.2 Information Security 5](#_Toc314532765)

[1.1.3 Management 5](#_Toc314532766)

[1.1.4 Management System 5](#_Toc314532767)

[1.1.5 Importance of ISMS 6](#_Toc314532768)

[1.1.6 Establishing an ISMS 6](#_Toc314532769)

[1.2 Scope 6](#_Toc314532770)

[1.3 Overview 6](#_Toc314532771)

[2 References 7](#_Toc314532772)

[3 Terms and Definitions 7](#_Toc314532773)

[4 Argus, the ISMS 7](#_Toc314532774)

[4.1 Argus Lifecycle 7](#_Toc314532775)

[4.2 Documentation 8](#_Toc314532776)

[4.3 Management Responsibilities 9](#_Toc314532777)

[4.4 Internal Audits 9](#_Toc314532778)

[4.5 Management review of Argus 9](#_Toc314532779)

[4.6 Argus Improvement 9](#_Toc314532780)

[5 Argus Controls 9](#_Toc314532781)

[5.1 Business Continuity 11](#_Toc314532782)

# Introduction

National Superconducting Cyclotron Laboratory (NSCL) is a world leader in rare isotope research and nuclear science education. NSCL scientists and researchers conduct advanced research in fundamental nuclear science, nuclear astrophysics, and accelerator physics. To facilitate the research, NSCL operates two superconducting cyclotrons. The Electronics Department (EE) at NSCL designs, develops, and manages the control systems, the power supplies, and the Radio Frequency (RF) systems used in the cyclotrons.

Just like any organization, the Electronics Department collects, processes, stores, and transmits large amounts of information. The information, and related processes, systems, networks and people are important assets of the department. These assets face a range of risks that may affect their functioning. They are subject to threats of attack, error, nature (flood, fire, etc), and are subject to vulnerabilities inherent in their use. The products and services provided by the Electronics Department are critical to the operation and growth of NSCL. Any vulnerability in Electronics Department’s systems has a direct impact on the services rendered by NSCL to its users. Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential for the department to achieve its objectives.

The Electronics Department must treat unacceptable information security risks and implements suitable controls. It must monitor and evaluate the effectiveness of implemented controls and procedures, identify emerging risks, and implement appropriate controls. To coordinate such information security activities, the Electronics Department has implemented a management system that is compliant with international information security standards.

## What is an ISMS?[[1]](#footnote-1)

An ISMS provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve organizational objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

### What is Information?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.

An organization's information is dependent upon information and communications technology. This technology is an essential element in any organization and assists in facilitating the creation, processing, storing, transmitting, protection and destruction of information. Where the extent of the interconnected global business environment expands so does the requirement to protect information as this information is now exposed to a wider variety of threats and vulnerabilities.

### Information Security

Information security includes three main dimensions: confidentiality, availability and integrity. With the aim of ensuring sustained business success and continuity, and in minimizing impacts, information security involves the application and management of appropriate security measures that involves consideration of a wide range of threats.

Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific security and business objectives of the organization are met. Relevant information security controls are expected to be seamlessly integrated with an organization's business processes.

### Management

Management involves activities to direct, control and continually improve the organization within appropriate structures. Management activities include the act, manner, or practice of organizing, handling, directing, supervising, and controlling resources. Management structures extend from one person in a small organization to management hierarchies consisting of many individuals in large organizations. In terms of an ISMS, management involves the supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, standards, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

### Management System

A management system uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

* satisfy the security requirements of customers and other stakeholders
* improve an organization's plans and activities
* meet the organization's information security objectives
* comply with regulations, legislation and industry mandates
* manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals and to the environment

### Importance of ISMS

The successful adoption of an ISMS is important to protect information assets allowing an organization to:

* achieve greater assurance that its information assets are adequately protected against information security risks on a continual basis
* maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness
* continually improve its control environment
* effectively achieve legal and regulatory compliance

### Establishing an ISMS

To ensure that the ISMS is effectively protecting the information assets on an ongoing basis, it is necessary for the following steps to be continuously repeated to identify changes in risks or in the organization's objectives:

* identify information assets and their associated security requirements
* assess information security risks
* select and implement relevant controls to manage unacceptable risks and
* monitor, maintain and improve the effectiveness of security controls associated with the organization's information assets

## Scope

The ISMS at the Electronics Department is named Argus. This document informally describes the constitution of Argus. It ties together the myriad documents and processes that form Argus. This document serves as the introduction for the users, auditors, and all those who want to understand the ISMS at the Electronics Department.

## Overview

The structure of this document follows that of ISO/IEC 27001 standard [2]. ISO/IEC 27001 provides a lucid and concise model for an ISMS, hence adopting its structure makes compliance and audits much easier. The *References* section lists the sources for the material in this document. The *Terms and Definitions* section lists and defines the terms used in this and other documents of Argus. The section *Argus, the ISMS* describes the components of the ISMS established at the Electronics Department. The section *Management Responsibilities* describes the responsibilities of the management in regards to Argus. The *Internal Audits* section describes the processes established to audit Argus. The *Management Review* section describes the processes to review Argus. The *ISMS Improvement* section describes established methods for improving Argus.

# References

1. ISO/IEC 27000 International Standard, Information Technology – Security Techniques –Information security management systems – Overview and vocabulary
2. ISO/IEC 27001 International Standard, Information Technology – Security Techniques –Information security management systems – Requirements
3. ISO/IEC 27002/17799 International Standard, Information Technology – Security Techniques – Code of practice for information security management
4. The OCTAVE Allegro Guidebook V1.0, Computer Emergency Response Team (CERT) Program, Software Engineering Institute, Carnegie Mellon University
5. Terms and Definitions, EE-ISMS-S001, NSCL Document Server, Electronics Folder
6. Argus Statement of Applicability, EE-ISMS-D00x, NSCL Document Server, Electronics Folder

# Terms and Definitions

Terms having special meaning, with respect to information security, are marked in *italics*. They are defined in [5].

# Argus, the ISMS

This section describes the workings of Argus without going into too many details. The details are formalized in the policies and procedures of Argus.

## Argus Lifecycle

Argus’ lifecycle follows the standard PDCA (Plan-Do-Check-Act) iterative model defined in [1] and shown in Figure 1; it has the following phases:

1. Plan: *Establish the ISMS*. Establish the policies, objectives, processes, and procedures relevant to managing risks and improving information security. It all starts with defining the scope of Argus, and the policy which establishes an overall sense of direction with regard to information security. The next step is to develop an approach to identify, evaluate, and treat risks faced by the Electronics Department. Afterwards, risks are identified and analyzed, and their treatment options evaluated. The controls needed for risk treatment are selected. At the end of this phase, the Statement of Applicability is developed; it contains a list of selected and excluded controls.
2. Do: *Implement and Operate the ISMS*. Implement and operate the ISMS policies, controls, processes, and procedures. The first step in this phase is to develop a Risk Treatment Plan (RTP) that identifies the management actions, resources, responsibilities, and priorities for managing information security risks. Then implement the RTP to achieve the control objectives selected in the previous phase. The effectiveness of the implemented controls is measured. Simultaneously, security events and incidents are detected and dealt with. This phase also implements the training and awareness programs.
3. Check: *Monitor and review the ISMS*. This phase monitors and reviews Argus’ processes. Assess, and where applicable, measure process performance against ISMS policy, objectives; and report the results to the management for review. The effectiveness of the ISMS is measured taking into account results of security audits, incidents, results from effectiveness measurements, suggestions, and feedback from all interested parties. At planned intervals, the risk assessment is reviewed, and the internal audits of Argus are conducted.
4. Act: *Maintain and improve the ISMS*. Based on the reviews and audits done in the previous phase, the identified improvements are implemented. At the same time, appropriate corrective and preventive actions are taken based on the result of the internal ISMS audit and management review, to achieve continual improvement of Argus.

Figure 1 PDCA Model

## Documentation

Like any management system, Argus incorporates a set of documents and records[[2]](#footnote-2). They are necessary to record management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible. Some of the Argus’ documents are the Argus ISMS policy, the Argus scope, risk assessment procedure, and risk assessment report. Argus’ documents must be controlled and protected. The documentation requirements of Argus and their control are formally defined in “EE-ISMS-P003: Argus Documentation Requirements”.

## Management Responsibilities

Management’s commitment is crucial for Argus’ establishment, implementation, operation, monitoring, review, maintenance, and improvement. The management communicates the importance of meeting information security objectives and conforming to information security policy to the organization (Electronics Department). It provides sufficient resources to establish and manage Argus. It decides on the criteria for accepting risks. It ensures that the training and awareness programs, internal audits, and management reviews are conducted effectively. The management’s responsibilities, as related to Argus, are defined in “EE-ISMS-P004: Argus Management Responsibilities”.

## Internal Audits

As part of Argus’ processes, internal audits are conducted at planned intervals to determine whether its control objectives, controls, processes and procedures conform to the international standards such as [2], meet the information security requirements, and are effectively implemented. The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records are defined in “EE-ISMS-P005: Argus Internal Audits Policy” and “EE-ISMS-R005: Argus Internal Audit Procedure”.

## Management review of Argus

Management reviews Argus at planned intervals to ensure its suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to Argus, including the information security policy and objectives. The requirements, inputs, and outputs of the review are defined in “EE-ISMS-P006: Argus Management Review Policy”.

## Argus Improvement

The effectiveness of Argus is continually improved through the use of the information security policy, information security objectives, audits results, analysis of monitored events, corrective and preventive actions, and management reviews. Argus’ corrective and preventive actions are defined in “EE-ISMS-P007: Argus Corrective and Preventive Action Policy”.

# Argus Controls

Based on risk assessment, Argus (its policies and procedures) implements controls to treat the risks to be mitigated. This is done during the *Plan* and *Do* phases of Argus’ lifecycle (see Section 4.1). The control objectives and controls are based on ISO/IEC 27002, the international standard for information security best-practices [3]. This section describes an overview of the controls. The controls implemented by Argus are listed in the Statement of Applicability [6]. The main categories for the controls are:

1. Security Policy: The objective of having a security policy is to provide direction and support for management for information security in accordance with department’s requirements and relevant laws and regulations. The controls in this category define the security policy and its review.
2. Information Security Organization: A management framework has to be established to initiate and control the implementation of information security in the department. The objectives of the controls in this category are to manage information security within the department, and to safeguard department’s information that are processed or managed by external parties.
3. Asset Management: All information assets in the department should be accounted for and have a nominated owner. The controls in this category achieve and maintain appropriate protection of departmental assets. The controls in this category identify assets, assign ownership, mandate their acceptable use, classify them, and set the procedures for labeling and handling them.
4. Human Resources Security: The controls in this category ensure that the employees[[3]](#footnote-3) understand their responsibilities and are suitable for the roles they are considered for to reduce the risk information security breaches. They also ensure that the employees exit the department or change roles in a manner such that the information security risks are minimized.
5. Physical and Environmental Security: These controls prevent unauthorized physical access, damage, and interference to the department’s premises and information. They protect equipment from physical and environmental threats. They include security perimeters, physical entry controls, protection from utility failures, securing cables, and secure disposal of information.
6. Communication and Operations: information processing facilities, such as servers, workstations, laptops etc, should be operated and managed appropriately. The controls in this category ensure correct and secure operation of information processing facilities by controlled change management, documented operating procedures, segregation of duties, capacity planning, and protection against malicious code. They ensure integrity and availability of information through data backup and restoration procedures. They also ensure the protection of information on networks and supporting infrastructure, prevent unauthorized disclosure, modification, removal or destruction of assets, and detect unauthorized information processing activities.
7. Access Control: The controls in this category control access to information. They prevent unauthorized access, and ensure authorized access through authentication, passwords, and privilege management. They prevent unauthorized access to network services, operating systems, and applications,.
8. Information Systems: The controls in this category ensure that security is integral part of information systems. They prevent unauthorized access, modification, or loss of information in applications through input and output data validation, and internal data corruption detection. The controls protect the confidentiality and integrity of information through cryptography and other means. They maintain the security of application system software through change control, review of applications after changes, and supervising outsourced development.
9. Information Security Incident Management: The weaknesses in information systems and breaches to information security should be communicated in a manner so as to ensure timely corrective action. Information security incidents should be managed effectively, once they are reported. The controls in this category ensure that the above objectives are met.
10. Business Continuity: The objective of this category is to counteract interruptions to the activities of the department, and to protect crucial processes from the effects of major failures in information systems or disasters, and to ensure their timely resumption.
11. Compliance: The operation, use, and management of the department’s information systems is subject to statutory, regulatory, and sometimes contractual security requirements. The objective of controls in this category is to avoid breaches of any such legal, statutory, regulatory or contractual obligations.

## Security Organization

The Electronics Department has myriad hierarchies: Human Resource based reporting hierarchy, project based hierarchy, EE Groups based hierarchy, and so on. The following chart shows the organizational structure related to the management of information security. Each node in the chart depicts a role, not a person or a position. It is possible for one person to assume multiple roles, or to have multiple people representing one role.

* EE Department Head (EEDH)
  + Information Security Board (ISB)
  + Information Security Manager (ISM)
  + Physical Security Manager (PSM)
  + Human Resource Security Manager (HRSM)
  + Internal Audit Team (IAT)
  + IT Management Group (ITG)

The following table describes the responsibilities of the above roles.

|  |  |
| --- | --- |
| Role | Responsibilities |
| EE Department Head | * Sponsor and champion the ISMS * Provide management support and direction for implementation of the ISMS * Establish the Information Security Policy |
| Information Security Board | * Review, approve, and recommend ISMS policies and procedures * Monitor changes to the ISMS * Review roles and responsibilities * Review security incidents, and recommend corrective and preventive actions |
| Information Security Manager | * Implement the ISMS * Periodically perform risk assessment and risk treatment * Inform ISB about updates to ISMS * Implement recommendations of internal and external audits * Close non-conformances in a timely fashion * Provide training for staff and users * Communicate the ISMS policies to all users * Review and approve ISMS releases |
| Physical Security Manager | * Responsible for managing all the physical security of the information assets |
| HR Security Manager | * Responsible for managing personnel security |
| Internal Audit Team | * Perform Internal Audits * Report non-conformances * Report security incidents |
| IT Management Group | * Responsible for managing IT security * Implement ISMS over IT infrastructure * Ensuring Disaster Recovery plans are implemented for IT Infrastructure effectively and tested periodically. * Providing constructive feedback on improvement of Security Infrastructure. * Ensuring implementation of information Security policies and Procedures in location. * Provide user awareness to IT staff members on information Security periodically. * Minimize virus security incidents in location by taking preventive and corrective actions. * Approve access rights for physical & information security as defined in procedures. * Implementation of Security Policies as per Client specific requirements. * Maintain records for procedures stated in Information Security Management System. * Providing guidance to users on Network Security policies. * Provide security training for IT staff |
|  |  |
|  |  |

## Business Continuity

No organization is an island. The business activities of the Electronics Department depend on employees, students, utilities, vendors, state and federal funding, communication links, and the weather. A long-term disruption to any of these resources can severely affect the products and services provided by the department. For example, a tornado can damage the offices and the file servers, preventing employees from performing their day=to-day activities, It may take several days or weeks to recover from the damage. The department cannot provide its design and support services to NSCL until it recovers from the disasters. The longer it takes to recover from the disaster, the worse it is for the department, in terms of reputation and finances. With the right preparation, it is possible to prevent or mitigate some of such risks.

It is not possible to prevent or even prepare for every possibility. However, it is prudent to plan for dealing with such events in general. In absence of such preparations, it can take an inordinate amount of time to recover, and sometimes it may be even impossible to resume operations from a catastrophe. A Business Continuity Management (BCM) system manages such risks, and helps with recovery and restoration of an organization’s activities in an optimal way. BCM deals with all business processes of an organization including HR, Finance, IT, etc. However, for Argus, we are interested only in those processes that depend on information assets. Argus is limited to business continuity related to information systems. This portion of Argus should form a part of the overall BCM of the department or the lab or MSU.

The Argus team developed the business continuity sub-system in the following manner:

1. Business Continuity Policy: Based on the information security, regulatory, and legal requirements, the department setup a business continuity policy (ISMSxxx-). It defines the scope and the goals of the system. The department head approved the policy.
2. Impact Analysis: The Argus team identified the critical business processes of the department, and identified the resources (information assets only) that the processes depend on. For each resource, the Argus team calculated the Maximum Tolerable Downtime (MTD), the outage time that is acceptable to the department. The Argus team identified the threats to the resources, calculated the impact and risks. The Argus team devised the backup system based on the impact analysis. ISMS-EE-xxx records the results of the impact analysis.
3. Preventive Controls: The Argus team identified and implemented preventive controls based on the impact analysis.
4. Recovery Strategy: The Argus team developed strategies for recovering the subsystems and resources needed to resume the critical activities of the department. As mentioned earlier, the recovery is limited to information security requirements.
5. Business Continuity Plan (BCP-IS): The Argus team documented the recovery strategies, procedures, responsible teams, their roles, activation criteria in the BCP. The BCP-IS is the document that will guide the resumption of services during a disaster.
6. Test BCP: The Argus team periodically tests the BCP, trains the employees in their roles, and improves the plan.
7. Maintain BCP: The Argus team periodically reviews the BCP, and updates it; this is generally done alongside the periodic review of Argus.

1. Most of the content for this section is based on the ISO/IEC 27000:2009 standard [↑](#footnote-ref-1)
2. Records are artifacts stating results achieved or providing evidence of activities performed. They are historical in nature and are not to be altered. Examples: access log, [↑](#footnote-ref-2)
3. This includes permanent and temporary employees, student employees, contractors, visiting scholars etc [↑](#footnote-ref-3)