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

Argus – Business Continuity Plan

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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 5](#_Toc290295767)

[1.1 Why do we need this? 5](#_Toc290295768)

[1.2 Principles 6](#_Toc290295769)

[1.3 Overview 7](#_Toc290295770)

[2 Terms and Definitions 7](#_Toc290295771)

[3 Structure of this Document 7](#_Toc290295772)

[4 Organization 7](#_Toc290295773)

[4.1 Internal Organization 7](#_Toc290295774)

[4.2 Procedures 9](#_Toc290295775)

[5 Security Policy 9](#_Toc290295776)

[5.1 Information Security Policy 9](#_Toc290295777)

[5.1.1 Review of Information Security Policy 10](#_Toc290295778)

[6 Asset Management 10](#_Toc290295779)

[6.1 EE Asset Classification 10](#_Toc290295780)

[6.2 Asset Tracking 10](#_Toc290295781)

[6.3 Asset Allocation/ Release/Reallocation 11](#_Toc290295782)

[7 Policies 11](#_Toc290295783)

[7.1 Change Management 11](#_Toc290295784)

[7.2 Development and Testing 11](#_Toc290295785)

[7.3 System Planning 12](#_Toc290295786)

[7.4 System Acceptance 12](#_Toc290295787)

[7.5 Malicious Code Protection 12](#_Toc290295788)

[7.6 Backup 12](#_Toc290295789)

[7.7 Information Access Control 13](#_Toc290295790)

[7.8 Acceptable Software Usage 14](#_Toc290295791)

[7.9 Removable Media 14](#_Toc290295792)

[7.10 Cryptography 14](#_Toc290295793)

[7.11 Password 15](#_Toc290295794)

[7.12 User Account Management 15](#_Toc290295795)

[7.13 Information Classification 15](#_Toc290295796)

[7.14 Remote Access 15](#_Toc290295797)

[7.15 Vulnerability Management 16](#_Toc290295798)

[7.16 Human Resources 16](#_Toc290295799)

[7.17 Physical Security 16](#_Toc290295800)

[7.18 System Development 17](#_Toc290295801)

[7.19 Legal Compliance 17](#_Toc290295802)

[7.20 Email Usage 17](#_Toc290295803)

[7.21 Internet Usage 17](#_Toc290295804)

[8 Standards and Procedures 17](#_Toc290295805)

[8.1 Risk Assessment and Treatment 17](#_Toc290295806)

[9 References 18](#_Toc290295807)

[10 Glossary 18](#_Toc290295808)

# Introduction

This document describes the business continuity plan to address information security requirements of the Electronics Department (EE). It is part of EE’s Information Security Management System, Argus.

## What is Business Continuity?

Continue critical business processes. Disasters. Differences with DR. Limited to Info Sec.

## Scope

Part of Argus.

## Overview

The structure of this document.

# References

1. Argus -Electronics Department ISMS- Manual, NSCL Document Server, Electronics Folder
2. Terms and Definitions, EE-ISMS-S001, NSCL Document Server, Electronics Folder
3. Argus Business Continuity Policy, EE-ISMS-P1401, NSCL Document Server, Electronics Folder
4. Argus Risk Assessment Procedure, EE-ISMS-W00401, NSCL Document Server, Electronics Folder

# Terms and Definitions

Information security related terms are marked in *underlined italics*. Please check [2] for their definitions.

# Business Continuity Plan

.

## Preparation

### Risk Management

Business Continuity related risks are managed in the same way as other information security risks, as described in *Argus Manual* []. The risks are identified, analyzed, and evaluated based on the methodology described in Argus Risk Assessment Procedure [].

### Backup Strategy

### Documentation Storage

Electronic copies of all the Argus documentation, including this plan, are stored at the offsite location (see Backup Strategy). Electronic and hard copies of the documentation are also issued to each member of the Emergency Response Team (see ) to be kept at home.

## Activation

An event causes

## Emergency Response

|  |  |  |
| --- | --- | --- |
| **Step** | **Role** | **Action** |
| 1 | EEDH | Alert the Emergency Response Team (ERT), and activate emergency response. |
| 2 | ERT | **Emergency Response**. Perform the following tasks:   * Call emergency services * Assess the extent of disaster and its impact on the department * Based on the assessment, plan the recovery actions * Establish and manage the Business Recovery Team (BRT) to maintain critical services and resume normal operation * Notify users * Allocate responsibilities and activities as required * Alert Media Team to handle the media * Report the plan and progress to Senior Management |
| 3 | BRT | **Business Recovery.** Perform the following:   * Execute the recovery plan as established by ERT * Coordinate activities with vendors, first responders, and others * Report progress to ERT   . |

### Media

Only the designated Media Team (see ) is permitted direct contact with the media. All inquiries from media must be redirected to the Media Team.

## BCP Maintenance

Simulation. Reviews. Audits. Updates.

# Appendix A: Key Personnel Contact Information

# Appendix B: Notification Tree