# Information Security

## MEIL Business Continuity Planning Policy

## DOCUMENT CONTROL

| | |
|---|---|
| **DOCUMENT NAME** | MEIL Business Continuity Planning Policy |
| **DOCUMENT NO.** | MEIL- POL/BCP/02/V1 |

## AUTHORISATION

| | **Prepared By** | **Reviewed By** | **Approved By** |
|---|---|---|---|
| **Name** | Priyanka Haldankar | Anil Khedulkar | Giriraj Mohta |
| **Designation** | GRC Consultant | Manager - IT | Chief Finance Officer |
| **Date** | 4-July-2025 | 24-Feb-2026 | 24-Feb-2026 |

## SECURITY CLASSIFICATION: Internal

## VERSION HISTORY

| VERSION | DATE | PREPARED BY | CHANGES & REASONS FOR CHANGE |
|---|---|---|---|
| 1.0 | 4-July-2025 | Priyanka Haldankar | Initial Release |

## DISTRIBUTION LIST

| Sr. # | Location | Department |
|---|---|---|
| 1 | All MEIL Locations | All Departments |
| | | |

# Table of Contents

## 1. Purpose

The purpose of this policy is to establish a structured approach for MEIL's Business Continuity and Disaster Recovery efforts, ensuring the resilience and integrity of critical ICT services and the continuity of information security management in the face of disruptions.

## 2. Scope

The scope of this policy encompasses all activities, processes, personnel, and technologies involved in maintaining the continuity of MEIL's critical ICT services and safeguarding information assets against disruptions, as well as the coordination and implementation of the Disaster Recovery Plan (DRP) across all business units and locations.

## 3. Applicability

This policy is applicable to all the locations of Mahindra EPC Irrigation Limited.

## 4. Terms and Definitions

| Terms | Definitions |
|---|---|
| Access Controls | Security features that control how users and systems communicate and interact with other systems and resources. |
| Business Continuity Planning (BCP) | The process of creating systems of prevention and recovery to deal with potential threats to a company, ensuring that personnel and assets are protected and able to function quickly in the event of a disaster. |
| Business Impact Analysis (BIA) | An exploratory and planning component of an organization's business continuity plan that reveals vulnerabilities and develops strategies for minimizing risk. |
| Disaster Recovery Planning (DRP) | A documented, structured approach with instructions for responding to unplanned incidents, including safeguarding data and assets and ensuring the quick resumption of system functions. |
| Encryption | The method by which information is converted into secret code that hides the information's true meaning. |
| Recovery Point Objectives (RPOs) | The maximum tolerable period in which data might be lost from an IT service due to a major incident. |
| Recovery Time Objectives (RTOs) | The targeted duration of time and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity. |

# 5. Roles and Responsibility

| Roles | Responsibilities |
|---|---|
| Information Technology | • Develop and maintain the backup strategy. Ensure alignment with DRP and BCP objectives.<br>• Implement and oversee automated backup processes. Manage offsite storage and data redundancy.<br>• Conduct routine tests of backup restoration. Document and report on test results.<br>• Facilitate regular training and awareness programs for all employees to reinforce the importance of their roles in BCP and DRP. |
| CIO | • Approves the formal DRP document and ensures it aligns with the organization's strategic objectives.<br>• Provides executive support and resources for the BCP/DRP initiatives.<br>• Reviews and endorses changes to the DRP following major updates or reviews. |
| Business Heads | • Conducts the Business Impact Analysis (BIA) in consultation with Sector IT to identify critical business functions and ICT dependencies.<br>• Ensures the BIA is updated regularly and following significant changes to ICT systems or the introduction of new systems.<br>• Collaborates with business units to understand their operational needs and the impact of potential disruptions. |

# 6. Business Continuity Planning Policy

## 6.1 Development and Approval of the DRP

- The DRP shall encompass strategies for maintaining the continuity of critical ICT services and recovering from disruptions in a timely manner.
- The DRP shall encompass strategies for the continuity and recovery of critical ICT services and information assets.
- The DRP shall also clearly define roles and responsibilities for initiating the plan, including those of MEIL IT/Sector IT personnel and outsourced vendors, to ensure a coordinated and swift response to incidents.

## 6.2 Business Impact Analysis (BIA)

- The BIA shall identify critical business functions and the impact of their disruption.
- The BIA shall be conducted periodically and whenever there is a significant change in the ICT environment or introduction of new systems.

## 6.3 Communication of the DRP

- The DRP shall be communicated to all relevant stakeholders within the organization, including MEIL IT/Sector IT, key functional managers, and officials of MEIL.

- Communication plans shall ensure coordination and cooperation during DRP activation.

### 6.4 Testing and Drills

- Disaster recovery drills shall be conducted regularly to test the DRP's effectiveness.
- Outsourced vendors involved in DRP execution shall participate in testing and drills.
- Disaster recovery drills shall encompass both technical recovery and organizational response, including employee evacuation drills and communication tests.

### 6.5 Coordination of Business Continuity and Disaster Recovery Efforts

- Location-specific documentation shall be maintained, based on critical IT applications and services.
- Coordination efforts should follow the DRP Guidelines to ensure consistency and effectiveness.

### 6.6 Information Security Continuity

- The BCP/DRP shall include specific measures to ensure the continuity of information security management.
- Information security controls shall be designed to remain effective during and after a disruption.

### 6.7 Review and Update of the DRP

- The DRP shall be reviewed and updated periodically to ensure it remains current and effective.
- Reviews shall consider changes in the business environment, technology, and organizational structure.
- Updates shall be documented and communicated to all relevant stakeholders.
- Ensure integration with the organization's Incident Response Plan for a cohesive approach to managing and recovering from incidents.
- Incorporate a change management process to assess the impact of any changes to ICT systems or the business environment on the BCP and DRP.

### 6.8 Backup Strategy

- The DC team shall establish a comprehensive backup strategy to ensure regular and reliable backups of all critical data and systems, consistent with the defined recovery time objectives (RTOs) and recovery point objectives (RPOs).
- Backup copies shall be stored in a secure offsite location to safeguard against local disasters, and data redundancy measures shall be implemented to provide immediate failover capabilities.
- The DC team shall conduct routine tests to verify the effectiveness of the backup restoration process and shall enforce stringent security measures, including encryption and access controls, to protect backup data.
- Backup procedures shall be reviewed and updated on a regular basis to ensure ongoing effectiveness and alignment with current technological standards and organizational requirements.

## 7. Exception

- Exceptions to this policy must be formally documented, reviewed, and approved by the IT Head, ensuring compliance with security policies while addressing specific operational or business requirements.

## 8. Disclaimer

- This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of is document is strictly prohibited and may be unlawful.