MISR UNIVERSITY FOR SCIENCE AND TECHNOLOGY

MUST

DATA BACKUP & DISASTER RECOVERY POLICY

Document Reference:	MUST-IT-POL-001
Version:	1.0
Effective Date:	2025
Review Date:	Annually
Classification:	Internal – Restricted
Issued By:	Information Technology Department
Approved By:	Chief of Information Technology

1. PURPOSE

This policy establishes the framework governing the backup of institutional data and the procedures for recovering systems and data following a disaster or significant disruption at Misr University for Science and Technology (MUST). The policy ensures business continuity, safeguards academic and administrative data, and defines roles and responsibilities for all stakeholders.

2. SCOPE

This policy applies to:

- All data systems, databases, servers, and applications operated by MUST
- All departments, faculties, and administrative units of the university
- Third-party vendors and cloud service providers handling MUST data
- Faculty, staff, students, and contractors who access or manage university information assets

3. DEFINITIONS

Term	Definition
Backup	A copy of data stored separately from the primary source to enable recovery in case of loss or corruption.
Disaster Recovery (DR)	The process of restoring IT systems and data to operational status following a disruptive event.
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss measured in time (e.g., 4 hours of data).
Recovery Time Objective (RTO)	The target time within which systems must be restored after a disruption.
Business Continuity Plan (BCP)	A strategic plan ensuring the university can continue critical operations during and after a disaster.
Incident	Any event that disrupts, or could disrupt, normal IT operations, including hardware failure, cyberattack, or natural disaster.
Hot Site	A fully operational off-site data center that can immediately take over operations.
Cold Site	A backup location with basic infrastructure but requiring setup time before operations can resume.

4. POLICY OBJECTIVES

MUST is committed to:

- Ensuring availability and integrity of all critical university data
- Minimizing downtime and data loss in the event of a system failure or disaster
- Meeting defined RPO of no more than 4 hours for critical systems

- Achieving RTO of no more than 24 hours for core academic and administrative systems
- Complying with applicable laws, regulations, and accreditation standards
- Providing a tested, documented, and regularly reviewed disaster recovery capability

5. DATA CLASSIFICATION & BACKUP PRIORITY

5.1 Critical Data (Tier 1)

- Student academic records, transcripts, and grades
- Financial and payroll data
- HR records and employee data
- Active research data and funded project files
- University ERP/LMS databases

Backup Frequency: Every 4 hours (continuous). Retention: 7 years minimum.

5.2 Operational Data (Tier 2)

- Email and communications systems
- Administrative documents and reports
- Faculty and departmental files

Backup Frequency: Daily. Retention: 3 years.

5.3 Standard Data (Tier 3)

- General user files and shared drives
- Non-critical system configurations
- Website content and digital assets

Backup Frequency: Weekly. Retention: 1 year.

6. BACKUP PROCEDURES

6.1 Backup Methods

- Full Backup: Complete copy of all selected data – performed weekly (every Sunday at 02:00 AM)
- Incremental Backup: Only data changed since the last backup – performed daily (Monday–Saturday at 02:00 AM)
- Differential Backup: Data changed since last full backup – used for critical systems as supplementary measure

6.2 Backup Storage

- On-site storage: Primary backup server located in the university data center
- Off-site storage: Encrypted backup replicated to a geographically separate facility
- Cloud backup: A cloud-based secondary copy maintained for Tier 1 and Tier 2 data
- Encrypted media: All physical backup media encrypted using AES-256 standard

6.3 Backup Verification

- Automated integrity checks run immediately after each backup cycle
- Monthly manual restore tests conducted by IT staff for each Tier
- Results logged and reviewed by the IT Director

7. DISASTER RECOVERY PLAN

7.1 Disaster Declaration

A disaster may be declared by the IT Director or University President when an incident disrupts critical operations for more than 2 consecutive hours, or when it is determined that recovery cannot be achieved through standard IT support procedures.

7.2 Disaster Recovery Team

Role	Responsibility	Contact Tier
DR Coordinator (IT Director)	Overall coordination of DR activities	Primary
Systems Administrator	Server and infrastructure recovery	Primary
Network Engineer	Network and connectivity restoration	Primary
Database Administrator	Database restoration and validation	Primary
IT Security Officer	Security assessment post-incident	Secondary
University President / VP	Executive decision-making & communication	Executive
Finance Director	Budget authorization for DR expenses	Executive
Communications Officer	Internal/external stakeholder updates	Support

7.3 Recovery Phases

Phase 1 – Detection & Notification (0–30 minutes)

- Incident identified and logged in the IT ticketing system
- DR Coordinator notified immediately
- Initial impact assessment performed

Phase 2 – Containment & Assessment (30–120 minutes)

- Affected systems isolated to prevent further damage
- Scope and severity of incident determined
- Disaster declaration issued if criteria are met

Phase 3 – Recovery Execution (2–24 hours)

- DR team activated; recovery procedures initiated
- Systems restored from most recent clean backups
- Data integrity verified before re-introducing systems to production

Phase 4 – Post-Recovery Review (24–72 hours post-incident)

- Full incident report prepared
- Root cause analysis conducted
- Lessons learned documented and policy updated as necessary

8. TESTING & MAINTENANCE

MUST shall conduct the following DR tests on a regular schedule:

Test Type	Frequency	Owner
Backup Restore Test	Monthly	Systems Admin
Tabletop Exercise	Quarterly	DR Coordinator
Full DR Simulation	Annually	IT Department
Business Continuity Review	Annually	IT Director + VP

9. SECURITY & COMPLIANCE

- All backup data must be encrypted at rest (AES-256) and in transit (TLS 1.2 or higher)
- Access to backup systems is restricted to authorized IT personnel only
- Backup logs are retained for a minimum of 12 months
- Compliance with Egyptian data protection regulations, ISO/IEC 27001, and applicable accreditation standards is mandatory
- Any breach of backup data must be reported to the IT Security Officer within 2 hours of discovery

10. ROLES & RESPONSIBILITIES

IT Director: Owns this policy; ensures adequate resources for backup and DR; reports to university leadership.

IT Staff: Executes backup procedures; monitors success/failure; escalates issues; performs restore tests.

Department Heads: Identify critical data within their units; cooperate in DR exercises; ensure staff compliance.

University President / VP: Approves DR declarations; allocates emergency resources; communicates with external stakeholders.

All Staff & Faculty: Comply with data handling requirements; report data loss incidents promptly.

11. POLICY REVIEW & VERSION CONTROL

This policy shall be reviewed annually by the IT Director and updated as required to reflect changes in technology, regulatory requirements, or university operations. All amendments require approval by the University President.

Official Endorsement

Chief of Information Technology Officer (CITO)

Name: _____

Signature: _____

Date: _____