REGENT MIDDLE EAST

Policy

IT Backup and Restoration Policy

1.0 Purpose

The objective of this policy is to define formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster and allow for an efficient recovery of IT services and data in a timely manner.

2.0 Scope

This policy applies to all IT systems or applications managed by Regent Institute Middle East (RIME) that store, process or transmit information, including network and computer hardware, software and applications.

This policy does not apply to information that is stored locally by users on desktops, laptops, tablets and mobile phones. Device owners are responsible for appropriate backup of the data stored locally on their mobile devices, apart from data synchronized with the device and stored on the institute's servers (such as Outlook emails and contacts).

3.0 Guiding Principles

- IT systems that are critical to institution activities must be clearly identified, as well as the potential risks of disruption that apply to them.
- IT continuity, backup and recovery must be managed in accordance with The Emergency Response and Business Resumption Policy.
- Recovery Time Objectives ("RTOs") of critical systems must be formally defined as per the business needs.
- Procedures and technology must be in place and tested regularly to ensure:
  - ✓ Prevention against IT system disruption.
  - ✓ Regular and comprehensive backup of critical systems, applications and data.
  - ✓ Timely recovery of critical systems, in line with the business expectation or RTO.

4.0 Responsibilities

- The IT Manager oversees developing and reviewing the institute's IT Backup and Recovery Policy. The IT Manager oversees ensuring that the institute's backup and restore objectives are met. RIME's CEO must approve the policy.
- Based on advice from the IT Manager, the institution is responsible for ensuring enough resourcing to maintain and develop this policy.
- RIME's Director of Studies is currently responsible for the administration of all institute department backup systems and related records.

- Data custodians are responsible for working with the institute's IT staff to set up acceptable backup schedules. Additionally, RIME workers responsible for data generation and management must ensure that essential institutional data under their control is included in the institute's disaster recovery strategy.
- Data backups are not meant to be used as archived copies of data or to meet record-keeping requirements for institutions.
- The backup and recovery method is implemented for all data held inside the institution.
- This policy applies to all workers within the institution and third parties who process or store institutional data. The owner / user of any computer or device that is not located in a recognized location, regardless of ownership, is solely responsible for data backup.

5.0 IT Backup Plan and Execution

5.1 Information owners shall store all data on the central repository.

5.2. The IT team shall develop and maintain a Backup Plan (BCKR_F01) for the data under their custody and IT infrastructure considering the information backup and business continuity requirements. This plan shall include the following:

a) Description of the data to be backed up (Backup group)

b) Schedule

c) Frequency (daily, weekly, monthly, etc.)

d) Media

e) Responsibility

5.3. Adequate copies of bought-out software packages shall be made and maintained. The terms of the software license agreements in respect of the number of copies of the software shall be considered in this regard.

5.4. Instructions for taking backup under special request received from departments are mentioned in the Backup Request Form (BCKR_F02) in the service desk tool. Backup jobs shall be executed as per the approved Backup Plan (BCKR_F01).

5.5 Data needs to be stored in the IT drive for backup to take place.

5.66. IT is responsible for the scheduling and execution of backup jobs as per the backup plan. Failure of backup jobs shall be monitored; failed backup jobs shall be restarted to ensure the successful completion of the job.

5.7. For PCs and mobile computing devices, the users are responsible for the execution of backup.

6.0 Restoration of Data

6.1 Backup restoration happens on a sample basis.

6.2 The restoration of data from the backup media shall be done upon request from the user through the Restoration Request Form (BCKR_F03).

6.3 Restoration shall be done at an alternate location.

6.4 On successful restoration, acknowledgement from the user shall be obtained.

7.0 Storing Backup in an offsite location

7.1 Offsite storage locations shall be identified such that the offsite location does not have the same risks as the primary site. The offsite location shall be approved by the IT Manager.

7.2 Data storage should be done only on consent from the client and as per the scope of work.

7.3 At least two backup copies shall be created for high critical data. One copy must be stored in the offsite location in accordance with the Backup Plan (BCKR_F01). This ensures that enough backup copies are always available for restoration following an emergency or a disaster.

7.4 The physical security and access control requirements for the storage location shall be determined and a protection similar to that of the original location shall be established.

7.5 The security requirements of the information are to be ensured during data replication.

8.0 Monitoring

Staff Members Involved
IT Manager
Other Staff Members

9.0 Review

This Policy will be reviewed annually by the Senior Management Team.

It may also be reviewed in the case of any substantial change, whichever is earlier.

For advice and support contact Operations / IT Manager.

REGENT MIDDLE EAST

Policy

Policy Information

PURPOSE	Policy Information
Title	IT Backup and Restoration Policy
Document number	0169/88
Purpose	The objective of this policy is to define formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster and allow for an efficient recovery of IT services and data in a timely manner.
Audience	Staff; Learners
Category	Compliance
Next review date	March, 2024

Version Control

Version	Author	Amended by	Date	Comments
1.01	DoS	DGS	26/9/2022	Policy approved by RIME Governance Committee
2.01	AH	QAC	20/3/2023	Policy approved by RIME Quality Assurance Committee