



IT BACKUP POLICY

Policy Owner	Compliance Manager
Approved By	Registrar
Version Date	08/10/2026
Version Number	2
Review Date	2 Years

Table of Contents

1.Introduction	3
2.Scope	3
3.Audience	3
4.Policy Statement	4
5.Objectives	4
6. Roles and Responsibilities	4
7. Backup Strategy	5
8. Backup Schedule	5
9. Backup Storage	6
10. Backup Security	6
10. Recovery Objectives	6
11. Backup Verification	7
12. Backup Testing	7
13. Retention and Disposal	7
14. Cloud Backup Requirements	7
15. Incident Response	8
16. Policy Violations	8

1.Introduction

The purpose of this policy is to ensure the confidentiality, integrity and availability of B-TIC information assets through a structured backup and recovery process. This policy establishes minimum requirements for backing up institutional data to minimize data loss resulting from hardware failures, software failures, cyberattacks, accidental deletion, natural disasters or other unexpected incidents.

2. Scope

This policy applies to:

- All B-TIC departments.
- All employees, academic staff, administrative staff, contractors, consultants and authorized third parties.
- All B-TIC-owned servers, desktop computers, laptops, virtual machines, cloud services, databases, applications and storage devices.

All institutional information classified as confidential, sensitive, internal, or public.

3. Audience

- B-TIC Management
- IT personnel
- Department Heads
- All B-TIC users/employees
- Academic and administrative staff

Relevant Policies/Others to be used in conjunction with,

- Data Protection Policy
- Documentation Retention and Secure Storage Policy
- Contingency and Adverse Effect Policy
- Compliance Policy
- Notification of Adverse Effects to Ofqual Policy

4. Policy Statement

B-TIC shall maintain secure, reliable and regularly tested backups of critical information systems to support business continuity, disaster recovery, teaching, learning, research and administrative operations.

5. Objectives

The objectives of this policy are to:

- Protect B-TIC information against accidental or intentional loss.
- Ensure rapid restoration of critical services.
- Meet business continuity requirements.
- Support legal, regulatory and accreditation requirements.
- Reduce operational risks associated with data loss.

6. Roles and Responsibilities

B-TIC shall

- Protect the confidentiality, integrity and availability of all institutional information assets through structured backup, storage and recovery frameworks.
- Maintain secure, encrypted and regularly tested backups to ensure continuous operations, disaster recovery and compliance with legal, regulatory and accreditation requirements.
- Establish clear system recovery metrics to minimize operational disruptions and prevent data loss.
- Ensure all institutional data is stored in approved, monitored storage environments.
- Implement physical, technical and administrative safeguards to protect backup infrastructure against unauthorized access, malware, environmental hazards and cyber threats.
- Conduct routine backup verification, logging and restoration testing to validate data integrity and system readiness.
- Manage third-party and cloud backup service providers to ensure full adherence to data protection standards, encryption protocols and operational security requirements.

7. Backup Strategy

B-TIC adopts the 3-2-1 Backup Principle:

- Maintain 3 copies of data.
- Store copies on 2 different media types.
- Keep 1 copy off-site or in secure cloud storage.

Backups shall include:

- Student Information System
- Learning Management System (LMS)
- Finance System
- Email Systems
- File Servers
- Research Data
- Website
- Database Servers
- Configuration Files

8. Backup Schedule

Data Type	Backup Frequency	Retention
Data Bases	Daily	90 Days
File Servers	Weekly	90 Days
Email System	Weekly	1 Year
Cloud Services	Weekly	1 Year
Critical Documents	Daily	5 Years

9. Backup Storage

Backups shall be stored:

- On secure backup servers.
- In encrypted cloud storage.
- At an approved off-site disaster recovery location.
- On immutable or offline storage where feasible to protect against ransomware.

Backup media shall be protected from:

- Fire
- Flood
- Theft
- Unauthorized access
- Malware
- Environmental damage

10. Backup Security

All backup data shall:

- Be encrypted during transmission.
- Be encrypted at rest using approved encryption standards.
- Be accessible only to authorized IT personnel.
- Be protected using multi-factor authentication where supported.
- Be logged and monitored.

11. Recovery Objectives

The B-TIC shall maintain the following targets:

Recovery Point Objective (RPO)

Maximum acceptable data loss:

- Critical systems: 1 hour
- Business systems: 24 hours
- Non-critical systems: 48 hours

Recovery Time Objective (RTO)

Maximum acceptable restoration time:

- Critical systems: 4 hours
- Business systems: 24 hours
- Non-critical systems: 72 hours

12. Backup Verification

The IT Department shall:

- Verify backup completion every day.
- Review backup logs daily.
- Investigate failed backups immediately.
- Maintain records of backup success and failures.

13. Backup Testing

Backup restoration testing shall be conducted:

- Monthly for critical systems.
- Quarterly for all production systems.
- After major infrastructure changes.
- Following disaster recovery exercises.
- Test results shall be documented and retained.

14. Retention and Disposal

Expired backups shall be securely deleted using approved data destruction methods. backup media shall be disposed of according to the B-TIC applicable legal requirements.

15. Cloud Backup Requirements

Where cloud services are used:

- Data must be encrypted.
- Providers shall comply with applicable data protection regulations.
- Backup copies shall be maintained independently of production cloud environments where practical.

16. Incident Response

Where backup failures occur:

1. Notify the IT Service Desk immediately.
2. Investigate the cause.
3. Restore backup operations within 24 hours.
4. Document corrective actions.
5. Report significant incidents to the Director of Information Technology.

17. Policy Violation

Failure to comply with this policy may result in:

- Removal of system access.
- Disciplinary action.
- Financial liability where negligence results in significant data loss.
- Legal action where applicable.

B-TIC has taken all effort to ensure that the Policy and information contained in this version of publication are true and accurate to the best of knowledge when published.

Disclaimer: However, Policies, Products and Services of B-TIC are subject to continuous learning and improvement frequently. Thus we reserve the right to improve the Policies, Products and Services accordingly. We cannot accept any responsibility for loss or damage of any nature upon the usage of this document.



business@b-tic.org



w w w .b-tic.org

B-TIC
PROFESSIONALISM SIMPLIFIED