Documentation Retention and Secure Storage Policy

Policy Owner	Compliance Manager
Approved By	Registrar
Policy Date	27/07/2026
Review Date	2 Years

B-TIC
PROFESSIONALISM SIMPLIFIED

Table of Contents

1.Introduction

This policy establishes the requirements for the retention, secure storage, protection, retrieval, archiving and disposal of B-TIC records. It ensures that institutional documentation is maintained in accordance with legal, regulatory, accreditation and operational requirements while safeguarding confidentiality, integrity and availability of information.

2. Scope

This policy applies to:

- All academic and administrative departments.
- All B-TIC employees, contractors, consultants, and temporary staff.
- All records maintained in physical or electronic format.
- Records held by third-party service providers on behalf of the B-TIC.

3. Policy Statement

B-TIC is committed to maintaining accurate, complete and secure records throughout their lifecycle. Documentation shall be retained for the minimum retention periods specified by applicable legislation, regulatory authorities, accreditation bodies and institutional requirements.

Records shall be securely stored to prevent unauthorized access, alteration, loss, destruction or disclosure while ensuring timely retrieval when required.

4. Types of Records

This policy applies to, but is not limited to:

Academic Records

- Student applications and admissions
- Enrolment records
- Attendance records
- Assessment submissions
- Examination scripts
- Marks and grade records
- Academic transcripts
- Graduation records
- Academic misconduct investigations

Quality Assurance Records
- Programme approvals
- Curriculum reviews
- Validation reports
- External examiner reports
- Internal audits
- Accreditation documentation
- Continuous improvement plans

Staff Records
- Recruitment documentation
- Employment contracts
- Performance reviews
- Training records
- Professional qualifications

Financial Records
- Budgets
- Invoices
- Purchase orders
- Financial statements
- Payroll records
- Tax documentation

Governance Records
- Board minutes
- Committee minutes
- Strategic plans
- Policies and procedures
- Risk registers

Research Records
- Ethics approvals
- Research data
- Grant documentation
- Publications
- Intellectual property records

5.Documentation Retention Requirement

The B-TIC shall maintain records for the following minimum periods unless longer retention is required by law or regulatory bodies.

Record Type	Minimum Retention Period
Student academic records and transcripts	Permanent
Graduation records	Permanent
Student assessment evidence	5 years after certification or graduation
Examination scripts	1 year after publication of results
Admissions documentation	3 years after decision
Attendance records	5 years
Programme validation documents	10 years
Accreditation records	10 years after expiry
Staff personnel files	7 years after employment ends
Recruitment records (unsuccessful applicants)	1 year
Financial records	7 years
Contracts and legal agreements	7 years after expiry

6. Secure Storage

Physical Records

Physical documentation shall:

- Be stored in secure filing cabinets or archive rooms.
- Be protected against fire, flooding, theft, pests, and environmental damage.
- Have controlled physical access.
- Be clearly indexed for retrieval.
- Be accessible only to authorized personnel.

Electronic Records

Electronic records shall:

- Be stored on secure servers or approved cloud platforms.
- Be protected through encryption where appropriate.
- Be subject to regular system backups.
- Have disaster recovery arrangements.
- Include audit logs where appropriate.
- Be protected using antivirus and cybersecurity controls.

7. Access Control

Access to records shall be based upon legitimate business need.

The B-TIC shall:

- Implement role-based access permissions.
- Maintain user authentication controls.
- Review access permissions periodically.
- Remove access immediately when employment or authorized access ends.
- Record access to sensitive information where appropriate.

Confidential records shall only be accessed by authorized personnel.

8. Confidentiality

Staff must protect confidential information relating to:

- Students
- Employees
- Examination materials
- Financial information

Confidential records shall not be shared unless authorized by law or institutional policy.

9. Backup and Disaster Recovery

Electronic records shall be:

- Backed up regularly according to the B-TIC's IT Backup Policy.
- Stored in geographically separate or secure cloud locations where appropriate.
- Periodically tested to ensure successful restoration.
- Included within the B-TIC's disaster recovery and business continuity arrangements.

10. Record Retrieval

Departments shall ensure that:

- Records can be located promptly.
- Archived records remain searchable.
- Requests for records are handled within reasonable timescales.
- Retrieval activities maintain confidentiality and integrity.

11. Archiving

Records that are no longer actively used but remain within their retention period shall be archived. Archived records shall:

- Remain protected.
- Be indexed.
- Be retrievable.
- Continue to meet confidentiality requirements.

12. Disposal of Records

At the end of the retention period, records shall be securely destroyed unless subject to legal hold or ongoing investigation. approved disposal methods include:

Physical Records

- Cross-cut shredding
- Confidential waste destruction
- Certified document destruction services

Electronic Records

- Secure deletion
- Data wiping
- Cryptographic erasure
- Secure destruction of storage media

Disposal shall be documented where appropriate.

13. Legal Hold

Where litigation, investigations, audits, regulatory reviews, or complaints are anticipated or ongoing, relevant records shall not be destroyed until authorization is provided by the B-TIC's Legal Office or senior management.

14. Responsibilities

B-TIC Management

- Approve this policy.
- Allocate appropriate resources.
- Monitor institutional compliance.

Information Technology Services

- Maintain secure electronic storage.
- Manage backups.
- Maintain cybersecurity controls.
- Support disaster recovery.

Registrar / Quality Assurance Office

- Monitor compliance.
- Maintain retention schedules.
- Coordinate record management activities.

Department Heads

- Ensure departmental compliance.
- Maintain accurate records.
- Authorize access where appropriate.

Employees

- Create accurate records.
- Store records securely.
- Protect confidential information.
- Dispose of records in accordance with this policy.

15. Monitoring and Compliance

The B-TIC shall periodically audit compliance with this policy. non-compliance may result in:

- Corrective actions
- Additional staff training
- Disciplinary action where appropriate

Regulatory reporting where legally required

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

www.b-tic.org

B-TIC

PROFESSIONALISM SIMPLIFIED