INTERNATIONAL BUSINESS UNIVERSITY (IBU)

POLICY CONTROL

Policy Number	1027
Policy Title	IBU Policy on Institutional Data and Information Management
Policy Owner / Responsible Offices	Office of Information Technology
Approval Authority	Board of Directors
Applies To	Faculty, staff, students, contractors, consultants, and third-party service providers acting on behalf of IBU
Approval Date	November 28, 2025
Effective Date	November 28, 2025
Review Date/s	Every three years from the approval date
Revision Date/s	–
Revision Implementation Date/s	–

1. INTRODUCTION AND BACKGROUND

International Business University ("IBU") is committed to the systematic governance, management, and protection of its institutional data and information assets. In accordance with this Policy, IBU implements technology-enhanced methodologies and comprehensive administrative, technical, and physical security measures to ensure the confidentiality, integrity, and availability of data.

2. PURPOSE

This Policy establishes a comprehensive institutional framework for the governance, classification, security, quality, retention, sharing, and lifecycle management of institutional data and information assets at IBU.

Institutional data is recognized as a strategic, business-critical, and shared University asset that supports academic quality assurance, institutional planning, operational effectiveness, regulatory compliance, accreditation, and evidence-based decision-making. This policy promotes a culture of responsible, ethical, transparent, and skillful data use across IBU.

This Policy also establishes the framework for the lawful collection, processing, storage, use, retention, and disposal of institutional data, including personal information, in compliance with applicable data protection, privacy, and cybersecurity laws and regulations, and in support of IBU's academic, administrative, and operational functions.

In furtherance of this purpose, the policy is intended to ensure consistent institutional practices, strengthen accountability for data stewardship, mitigate legal and operational risk, and enable the effective and secure use of data to support IBU's mission, governance, and continuous improvement.

3. POLICY STATEMENT

This Policy applies to all institutional data regardless of format or medium (electronic or physical), system or platform (on-premise or cloud-based), location of access (on-campus or remote), or level of transformation (raw, revised, aggregated, or derived), and shall be interpreted broadly to ensure comprehensive data governance and protection.

It applies to all faculty, staff, students, contractors, consultants, and third-party service providers acting on behalf of IBU, and governs their access to, use of, and responsibility for institutional data. Research data generated through scholarly activity is governed separately under applicable research policies, except where such data intersects with institutional administrative systems, in which case the relevant provisions of this Policy shall apply.

4. APPLICABILITY

The responsibility and authority for adherence to and review of this Policy resides with the Office of Information Technology, which must report data matters under this Policy to the Dean/Vice-President (or designate), the Registrar, department chairs, and faculty, as appropriate.

5. DEFINITIONS

Institutional Data
All data created, collected, received, maintained, or processed by the University in the course of its academic, administrative, financial, research, or operational activities. Institutional data includes student records, personnel records, financial data, academic program information, research data, operational logs, and any other information governed by University policy or regulatory requirements.

Data Classification
A structured categorization of institutional data based on sensitivity, confidentiality, and required safeguards. Classifications typically include (a) Public Data, (b) Internal Data, (c) Confidential Data, and (d) Restricted or Highly Sensitive Data. Each classification level will determine appropriate access controls, handling procedures, retention requirements, and protection measures.

Regulatory Compliance Terms
References to laws, regulations, and external standards—including but not limited to privacy legislation, accreditation standards, quality assurance frameworks, records-retention statutes, and cybersecurity requirements—that govern how institutional data must be collected, stored, used, shared, and protected. Regulatory terms apply according to jurisdiction and the scope of institutional operations.

6. POLICY

6.1 GUIDING PRINCIPLES

- **Data Integrity and Quality** – Institutional data must be accurate, complete, timely, and reliable in order to support effective decision-making, regulatory compliance, and

institutional reporting. Appropriate controls shall be implemented to ensure data consistency and to prevent unauthorized alteration or degradation of data quality.

- **Collect Once, Use Many Times** – Data should be collected at the authoritative source and reused where appropriate to minimize duplication, inefficiency, and inconsistency across systems and processes. This principle supports standardized data definitions and promotes interoperability among institutional systems.
- **Accountability and Stewardship** – Clear ownership and stewardship must be assigned for all institutional data to ensure responsibility for data accuracy, protection, and appropriate use. Data owners and stewards are accountable for defining access rules, maintaining data quality, and ensuring compliance with applicable policies and regulations.
- **Role-Based and Purpose-Limited Access** – Access is granted only to authorized individuals for legitimate institutional purposes. Such access shall be limited to the minimum level necessary to perform assigned duties and shall be regularly reviewed to prevent unauthorized or excessive access.
- **Privacy and Security by Design** – Privacy and security safeguards are embedded throughout the data lifecycle, from initial collection through processing, storage, transmission, and disposal. This includes the implementation of technical, administrative, and physical measures to protect data from unauthorized access, disclosure, or loss.
- **Lifecycle Management** – Data is managed from creation through secure archival and irreversible disposal in accordance with institutional retention schedules and legal requirements. This ensures that data is retained only for as long as necessary and disposed of in a manner that mitigates legal, operational, and security risks.
- **Transparency and Auditability** – Data processes must be documented, traceable, and auditable to support accountability, oversight, and continuous improvement. Adequate records shall be maintained to demonstrate compliance with institutional policies and applicable laws and regulations.
- **Institutional Stewardship** – Data is managed for long-term institutional value rather than individual or system ownership, recognizing data as a strategic institutional asset. Decisions regarding data use, integration, and governance shall prioritize the overall interests and sustainability of the institution.

6.2 Mandated Institutional Data Types

- **Student Data** – This includes admissions, enrolment, academic records, progression, graduation, and related demographic, contact, or personal information, as well as information pertaining to student support services, disciplinary records, and engagement in co-curricular activities.
- **Academic Data** – This encompasses programs, courses, curriculum, faculty records, learning outcomes, assessment results, instructional materials, and other academic or assessment-related information that supports the delivery, quality, and evaluation of educational programs.
- **Operational and Administrative Data** – This includes finance, HR, procurement, facilities, operational documentation, workflow data, institutional policies,

administrative correspondence, and other records necessary to support the efficient functioning of the University's administrative and operational processes.

- **Quality Assurance and Performance Data** – This includes KPIs, surveys, evaluations, accreditation evidence, and other metrics or reports used to monitor and improve institutional effectiveness.
- **Research Administration and Capstone Project Data** – This includes research proposals, funding records, ethical approvals, project deliverables, and associated documentation that supports scholarly and applied research activities.
- **IT, Cybersecurity, System, and Audit Log Data** – This includes system configurations, access logs, security events, incident reports, and other technical or operational information necessary to ensure the secure and reliable operation of institutional technology environments.

IBU shall maintain an institutional data inventory that identifies authoritative systems and the mandated data types, ensuring comprehensive governance, accountability, and compliance across all institutional information assets.

6.3 Data Collection and Quality Management

Institutional data shall be collected lawfully, fairly, and transparently for defined institutional purposes, ensuring that all data handling aligns with applicable legal, regulatory, and institutional requirements.

Data Stewards are responsible for establishing and maintaining:

Data standards, definitions, and metadata; implementing and overseeing validation and quality controls; defining and enforcing synchronization and integration across systems; monitoring data governance policies; and supporting data users in the correct interpretation, usage, and protection of institutional data.

All data users share responsibility for promptly reporting inaccuracies, inconsistencies, or quality concerns in a timely manner and cooperating with Data Stewards to ensure the ongoing reliability, integrity, and usability of institutional data.

6.4 Data Classification

Institutional data is classified according to sensitivity and institutional impact.

- Restricted Data includes highly sensitive data with the potential for severe legal, financial, regulatory, or reputational impact if compromised, such as personally identifiable information, financial records, or confidential research data.
- Confidential Data refers to sensitive internal data with significant privacy, operational, or strategic implications that require controlled access, including internal reports, personnel records, and administrative plans.

- Protected Data consists of internal data with moderate sensitivity that necessitates role-based access controls, such as departmental documentation, operational schedules, and non-public communications.
- Public Data encompasses information approved for public release, including press releases, published reports, and publicly available institutional statistics.
- Data Stewards assign these classifications and are responsible for ensuring appropriate handling, access controls, and security measures in accordance with institutional policies, standards, and regulatory requirements.

  Classifications are assigned by Data Stewards with corresponding handling and security controls.

6.5 Data Access and Acceptable Use

Access to institutional data is granted based on legitimate institutional need and is not transferable.

Institutional data must not be accessed out of personal curiosity; accessed, copied, or manipulated for personal gain or advantage; altered, falsified, or deleted in an unauthorized manner; or disclosed, shared, or transmitted outside of approved institutional processes, systems, or channels.

Such actions are strictly prohibited and may result in disciplinary, legal, or regulatory consequences, in accordance with institutional policies and applicable laws.

Authorization decisions for data access must be properly documented, reviewed periodically, and maintained in accordance with institutional policies and regulatory requirements.

All data users shall adhere to these requirements to ensure that access and use of institutional data remain lawful, ethical, and aligned with IBU's governance and security standards.

6.6 Information Security

IBU implements layered security controls to ensure the confidentiality, integrity, and availability of institutional data, aligning with institutional policies, standards, and regulatory requirements.

- **Identity and Access Management** - Identity and Access Management ensures that all users are uniquely identified, authenticated, and authorized to access only the data necessary for their institutional roles. This includes the management of credentials,

authentication protocols, and periodic review of user accounts to prevent unauthorized access.

- **Role - Based Access Control** - Role - Based Access Control limits access to institutional data according to defined roles, responsibilities, and institutional needs. It ensures that sensitive and restricted information is only accessible to authorized personnel and that access permissions are regularly reviewed and updated.
- **Audit Logging and Monitoring** - Audit Logging and Monitoring tracks system activity, user access, and changes to data, providing a verifiable record for accountability, compliance, and forensic investigations. Continuous monitoring helps detect irregularities, potential breaches, or policy violations in a timely manner.
- **Incident Detection and Response** - Incident Detection and Response establishes processes and tools to promptly identify, report, and mitigate security incidents or breaches. This also ensures that potential threats are addressed quickly, minimizing risk to institutional operations, data integrity, and compliance obligations.
- **Backup and Disaster Recovery Mechanisms** - Backup and Disaster Recovery Mechanisms ensure that institutional data is regularly backed up, securely stored, and can be restored in the event of system failure, data corruption, or other operational disruptions. These mechanisms are tested periodically to confirm data recoverability and operational resilience.

6.7 Data Retention, Archival, and Disposal

Institutional data is retained in accordance with legal, regulatory, academic, and operational requirements ensuring compliance and supporting institutional accountability.

- **Retention Periods** - Retention periods define the minimum and maximum duration for which each category of institutional data must be maintained. These periods are determined based on legal, regulatory, academic, and operational obligations, and are designed to ensure that data remains available for required purposes such as reporting, auditing, research, or institutional decision-making.
- **Archival Requirements** - Archival requirements specify the methods and standards for securely storing institutional data that is no longer actively used but must be preserved for future reference, compliance, or historical purposes. This includes the format, location, protection measures, and accessibility protocols for archived data. All archival activities shall ensure data integrity, prevent unauthorized access, and comply with institutional policies and applicable regulations.
- **Approved Disposal Methods** - Approved disposal methods define the authorized processes for permanently destroying institutional data once it is no longer required, ensuring irreversibility and preventing any possibility of reconstruction or unauthorized recovery. When data is no longer required, it must be securely destroyed to ensure irreversibility and prevent reconstruction. Disposal methods may include secure digital deletion, physical destruction of media, or other verifiable techniques that comply with institutional and regulatory standards. All data disposal actions shall be

documented and overseen by authorized personnel to ensure accountability and compliance.

6.8 Data Sharing and Disclosure

Internal sharing of institutional data requires prior authorization from the appropriate Data Owner or Data Steward to ensure that access is consistent with institutional policies, role responsibilities, and data classification.

External sharing of institutional data requires documented agreements, including data sharing or processing contracts, and strict compliance with applicable privacy, security, and contractual obligations.

All data sharing and disclosure activities shall be conducted in a manner that safeguards the confidentiality, integrity, and lawful use of institutional data, with appropriate oversight and recordkeeping to demonstrate compliance.

7. ROLES AND RESPONSIBILITIES

7.1 Data Owner

Data Owners are senior institutional leaders accountable for specific data domains, and they hold overall responsibility for ensuring the quality, integrity, and proper management of the data within their domains.

Their responsibilities include overall accountability for data quality and integrity; approving access and usage permissions; ensuring compliance with institutional policies, standards, and applicable regulatory obligations; and authorizing the restriction or revocation of access where risk, non-compliance, or potential misuse is identified.

Data Owners shall provide guidance and oversight to Data Stewards and other personnel to ensure that institutional data is managed in accordance with governance requirements and best practices.

7.2 Data Steward

Data Stewards are operational managers responsible for day-to-day data governance within their domains, ensuring that institutional data is accurate, consistent, and properly managed.

Their responsibilities include assigning and maintaining data classification; defining data standards, definitions, and quality rules; documenting processes, metadata, and usage guidelines; monitoring data quality and resolving data issues; and ensuring alignment with institutional policies, regulatory requirements, and best practices.

Data Stewards shall provide guidance and support to data users, facilitate compliance with governance procedures, and collaborate with Data Owners to maintain the integrity, usability, and security of institutional data across all systems.

7.3 IT Data Administrators

IT Data Administrators are responsible for the technical management of institutional data, ensuring its secure, reliable, and compliant handling within institutional systems.

Their responsibilities include secure storage, access controls, and authentication mechanisms; backups, disaster recovery, and system resilience; system integrity, configuration, and audit logging; and collaboration with Data Stewards on system changes, integrations, and technical implementations.

IT Data Administrators shall work closely with Data Owners and Data Stewards to maintain the integrity, availability, and confidentiality of institutional data, and to ensure that all technical operations align with institutional policies, security standards, and regulatory requirements.

7.4 Data Users

Data Users are authorized individuals who access institutional data as part of their assigned duties and responsibilities.

They are responsible for using data ethically, accurately, and in compliance with this policy; protecting data from unauthorized access, disclosure, or misuse; and promptly reporting any data quality, integrity, or security issues.

Data Users shall adhere to all applicable institutional policies, standards, and procedures, and cooperate with Data Stewards, Data Owners, and IT Data Administrators to ensure the proper management, confidentiality, and reliability of institutional data.

8. REVIEW

This Policy is reviewed annually, or earlier if required due to regulatory changes, audit findings, system changes, or evolving institutional priorities.

Recommendations for updates or enhancements are documented and submitted to the appropriate authorities for approval, ensuring that the Policy remains current, effective, and supportive of continuous improvement in the management, governance, and protection of institutional data

9. COMPLIANCE PROCEDURES

IBU complies with all applicable privacy and data protection legislation, ensuring that institutional data is collected, processed, stored, and shared in a lawful, ethical, and transparent manner.

IBU implements measures to protect personal information and to meet its regulatory obligations.

9.1.1 Personal Information Protection and Electronic Documents Act (PIPEDA)

IBU adheres to the requirements of PIPEDA, including the collection, use, disclosure, and safeguarding of personal information. Policies and procedures are in place to ensure that personal data is handled responsibly, individuals' rights are respected, and breaches or incidents are managed appropriately.

9.1.2 General Data Protection Regulation (GDPR)

Where applicable, IBU ensures compliance with the GDPR, including the lawful processing of personal data implementation of privacy by design and by default principles, and protection of data subjects 'rights. This includes conducting data protection impact assessments and appointing data protection officers where required.

9.1.3 Provincial and Sector-Specific Requirements

IBU complies with relevant provincial legislation and sector-specific regulatory obligations, ensuring that institutional data management aligns with local legal frameworks and industry standards. This includes adherence to any additional requirements for data security, retention, and privacy specific to higher education or research activities.

9.1.4 Compliance Documentation and Evidence

IBU maintains evidence of compliance with privacy and regulatory requirements, including records of data processing activities, risk assessments, audits, and staff training. Documentation is retained to demonstrate adherence to all applicable laws, regulations, and institutional policies, and to support accountability and continuous improvement in data protection practices.

10. EVALUATION AND QUALITY ASSURANCE

10.1 MONITORING, AUDIT, AND ENFORCEMENT

Compliance with this policy is monitored through internal reviews, audits, and incident reporting, including periodic assessments of access controls, data handling practices, and adherence to defined data governance standards.

Monitoring activities also involve verifying that data classification, retention, sharing, and security requirements are consistently applied across institutional systems and processes.

Where risk or non-compliance is identified, access privileges may be restricted or revoked immediately to prevent further exposure or misuse, and disciplinary, contractual, or legal actions may be taken in accordance with IBU's policies, agreements, and applicable laws.

All monitoring, audit, and enforcement activities shall be documented, reported to appropriate institutional authorities, and used to inform improvements in data governance, accountability, and overall institutional compliance.

11. RELATED DOCUMENTS

None