



UoM- Data Security Policy



Document Control

Document Creation

Date	Version	Description	Author
15 May 2025	1.0		Dr. Satish Zende (DICT)

Review Details

Review Date	Reviewed By
23 June 2025	BOIT Members

Approval Details/

Approval Date	Approved By
25 June 2025	BOIT



1. Purpose

To establish a framework for protecting the confidentiality, integrity, and availability of student, employee, faculty, research, and assessment data—including intellectual property and sensitive personal information—in compliance with the Digital Personal Data Protection Act, 2023, CERT-In Guidelines, and MeitY Security Practices

2. Scope

This policy applies to all individuals and entities handling University data, including internal staff, students, contractors, and third-party service providers. It also extends to the students and staff (teaching and non-teaching) of colleges / institutes affiliated to the University of Mumbai (UoM). It covers both digital and physical records across all platforms, devices, and storage environments.

3. Institutional Ownership & Personnel Obligations

All data, systems, and digital assets created, processed, stored, or transmitted within the University's infrastructure are the exclusive property of the University. Unauthorized retention, replication, or use of such assets is strictly prohibited and shall be treated as a violation of institutional policy and applicable law.

All personnel entrusted with access to university systems, credentials, or sensitive data are obligated to cooperate fully with authorized audits, investigations, and operational requests. Withholding passwords, access tokens, or system-level information shall be treated as a violation of institutional policy and may result in disciplinary action or legal proceedings under applicable law.

4. Data Classification

Classification	Examples	Handling Requirements
Public	Announcements, brochures	No restrictions
Internal	Course materials, internal notices	Access limited to authorized university members
Confidential	Student records, employee files, assessments	Encryption, access logging, retention control
Highly Confidential	IP, financial data, examination records	MFA, strict access control, breach notification
Sensitive Personal	Aadhaar, biometric, health data	DPDP-compliant consent, encryption, data subject rights enforcement



5. Data Protection Principles

All data processing shall adhere to:

1. **Lawfulness & Consent:** Data to be collected with valid explicit consent or lawful basis
2. **Purpose Limitation:** To be used only for specified academic, administrative, regulatory or compliance purposes
3. **Minimization:** Only necessary data as required to be retained as per law
4. **Accuracy:** Maintained and updated regularly
5. **Storage Limitation:** Retention aligned with legal and operational needs
6. **Integrity & Confidentiality:** Protected against unauthorized access or loss
7. **Attribution:** Proper citation of intellectual contributions and sources

6. Access Control

- Only the personnel duly authorised by the competent authority shall be given access to confidential and highly confidential data.
- Access permissions shall be granted based on role and necessity (least privilege principle).
- Multi-factor authentication (MFA) shall be implemented for access to sensitive systems.
- Role-based access shall be enforced using identity and access management systems
- MFA mandatory shall be used for systems handling Highly Confidential or Sensitive Personal Data
- Access logs shall be retained for 180 days (CERT-In mandate)
- Unauthorized device connections (USB, mobile) prohibited unless explicitly approved by competent authority

7. Data Security Measures

- **Encryption:** All confidential and highly confidential data shall be encrypted in transit and at rest.
- **Secure Storage:** Data shall be stored on secure servers with appropriate backup mechanisms.
- **Data Transfer:** Secure channels (e.g., VPN, encrypted emails) shall be used for data transmission.
- **Endpoint Control:** DLP tools and device restrictions enforced.
- **Third-Party Compliance:** Vendors handling university data must comply with security requirements and should have provisions to manage information and data security and shall be



liable for penalty as decided by the competent authority of the University for any lapse in security of data while in transit or at rest.

- **Incident Response:** A security incident response plan shall be in place to handle breaches and shall be disseminated to the concerned employees / users .
- **USB/Hard Drive:** Unless authorised, copying data onto USB/Hard Drive/Mobile and other similar devices is strictly prohibited.
- **Backup & Recovery:** Daily backups, tested restoration, and documented RTO/RPO targets shall be in place.

8. Incident Response

- Incidents must be reported within **6 hours** of detection (CERT-In mandate)
- Response workflow: Detection → Containment → Notification → Recovery → Review
- Breach notifications to be issued to affected data subjects and authorities as required
- Forensic readiness shall be maintained for critical systems

9. Data Retention Periods

Data shall be retained based on the following guidelines:

- **Student Records:** Retained for lifetime after graduation or separation.
- **Employee Records:** Retained for lifetime after graduation or separation.
- **Assessment and Examination Data:** Retained for 5 years post-publication of results.
- **Financial and Transactional Data:** Retained for 7 years in compliance with financial regulations.
- **Research Data and Intellectual Property:** Retention period depends on contractual or legal requirements.
- **Backup Data:** Retained for a maximum of 1 year unless required for investigations.

10. Data Disposal

- **Digital Data:** On need basis, digital data shall be securely erased.
- **Physical Records:** On need basis, physical records shall be shredded or destroyed as per approved policy.
- **IT Equipment:** On need basis, IT equipment shall be decommissioned securely, ensuring no recoverable data remains in the equipment.
 - Disposal logs retained for 1 year for audit purposes



11. Training & Awareness

- Mandatory annual training for all users
- Specialized modules for privileged users and vendors
- Completion tracked via LMS/ERP; non-compliance escalated

12. Compliance and Monitoring

- Quarterly internal audits; annual external audits; external audit as may be required by law.
- Violations categorized as Minor, Major, or Critical
- Disciplinary actions range from warnings to termination
- Audit logs maintained for all access, changes, and disposal events

13. Policy Governance

- i. Version control and changelog maintained by Policy Owner
- ii. Exceptions require formal request and written approval
- iii. Archived versions to be retained for 5 years

14. Policy Review and Updates

This policy shall be reviewed annually or as required due to regulatory changes, emerging threats, or operational needs.

15. Appendix: Legal References

- Digital Personal Data Protection Act, 2023
- Information Technology Act, 2000 (Amended 2008)
- CERT-In Guidelines (2022)
- MeitY Security Practices for Government Entities
- UGC/AICTE IT Governance Guidelines