



UoM- Information Security Policy



Document Control

Document Creation

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

Review Details

Review Date	Reviewed By
23 June 2025	BOIT

Approval Details

Approval Date	Approved By
25 June 2025	BOIT



1. Purpose

To safeguard the confidentiality, integrity, and availability of University data and IT assets, in compliance with Indian laws and sectoral guidelines. This policy ensures responsible use, secure processing, and lawful handling of digital and physical information

2. Scope

Applies to all employees irrespective of the nature of their appointment (Permanent, Ad-Hoc, Contractual, Third Party Rolls), faculty (of University Departments, Conducted Colleges, University Institutes and Affiliated Colleges), students (of University Departments, Conducted Colleges, University Institutes and Affiliated Colleges), contractors, vendors, and third parties who access or manage University data across all digital platforms, physical records, cloud services, mobile devices and any other touchpoint / IOT Devices.

Exceptions to the policy must be formally requested, reviewed, advised and approved by Director, IT through the appropriate / relevant University authority.

This policy, its associated requirements and standards will be revised regularly to ensure continued effectiveness over technology and operations.

3. Information Security Policy Statements

Listed below are statements that shall form a broad level Information Security Policy for the University.

- a) All users would be responsible for protecting University of Mumbai's (UoM) confidential information.
- b) Unauthorised access and use of UoM confidential information is strictly prohibited.
- c) UoM information systems and information must not be used in any manner that violates University policy / policies and for unlawful purposes or for any other purpose not authorised by the relevant University Authorities.
- d) All users are responsible for protecting their UoM system passwords and access credentials from unauthorised use. Passwords must not be shared or written on any information assets.
- e) All users of UoM having access to confidential information must be accurately and individually identified. A record of these uses must be maintained with the relevant University Authorities



with the power to cease the access in case of any violation of the policies and/or service conditions laid down by the University.

- f) UoM confidential information must be protected on computer or any other computer supported device against improper access and use. System logs for each access must be maintained.
- g) Electronic and physical records containing UoM confidential information must be protected when transported or transmitted or at rest. No such record, either Physical or electronic, must be transported or transmitted or shared unless authorised by the relevant University Authority.
- h) Software assets must be kept up to date on all UoM information systems.
- i) Electronic and Physical records containing UoM confidential information/data must be properly disposed when not needed so that the information cannot be retrieved or reassembled.
- j) UoM and its Departments / Conducted Colleges / Constituent Colleges / Constituent Institutes / Affiliated Colleges must conduct due diligence on third parties that will store or may have access to UoM information or sensitive information.
- k) Any actual or suspected loss, theft or improper use or access to UoM confidential information or systems must be reported to the relevant University authorities.
- l) Users must obtain authorisation / written permission before using / connecting personal devices to the UoM information systems.
- m) The risks associated with the use of information and networking systems must be reported / communicated to the authorities.
- n) All digital information created, processed, or stored in any application, software, firmware, or website—whether developed internally or externally and stored on University or external servers or databases—is the sole intellectual property of the University of Mumbai. Any attempt to use this information for personal gain or unauthorized purposes shall be treated as cybercrime and will be prosecuted under the IT Act, 2000.
- o) No employee, external vendor, or any other user of the University's software or hardware or any other allied connected system is permitted to withhold or retain exclusive access to the credentials of university-owned assets, including but not limited to desktops, servers, hand held devices, IoT devices and web applications. All credentials are institutional property, and their unauthorized retention or misuse will be treated as a violation of this policy

4. Responsibilities of Community members



Role	Responsibility
All Users	Follow security protocols, report incidents, protect credentials and devices
IT Security Team	Monitor compliance, manage incidents, enforce controls
Department Heads	Ensure team-level adherence and training completion
Third Parties	Comply with contractual security obligations and undergo due diligence
Policy Owner	Maintain version control, review updates, and approve exceptions

5. Access Control & Credential Management

- Role-based access must be enforced using identity management systems.
- Passwords must comply with MeitY-recommended complexity and rotation standards.
- Multi-factor authentication (MFA) is mandatory for privileged accounts.
- Credentials must not be retained or shared outside authorized systems.
- All access logs must be retained for a minimum of 180 days as per CERT-In directive. Access and/or transaction logs related to Financial transactions, Purchases, Human Resource (HR), Examination, Admission & Eligibility or any other area of importance, must be stored for a longer duration as per the statutory/working requirement decided by the relevant University Authorities.

6. Data Classification & Handling

Classification	Examples	Handling Requirements
Public	Website content, brochures	No restrictions
Internal	Meeting notes, internal memos	Access limited to employees; no external sharing; access logged
Confidential	Student records, HR files	Encrypted at rest and in transit; access logged
Sensitive	Aadhaar, financial data, health info	DPDP-compliant consent, encryption, breach notification

7. Asset Management

- Maintain an inventory of all IT assets (Software / Hardware) with ownership and lifecycle tracking.
- Disposal must follow secure wipe/shred protocols with audit logs.
- All endpoints must be protected with anti virus/malware/spyware and endpoint detection tools

8. Incident Response



- All incidents must be reported within 6 hours of detection, as per CERT-In mandate.
- Response workflow: Detection → Containment → Investigation → Recovery → Reporting.
- Maintain forensic readiness for critical systems and preserve evidence trails.

9. Training & Awareness

- Mandatory annual training for all users would be provided for sensitising and training them in the latest trends, regulations and approaches for protecting the digital infrastructure of the University.
- Specialized training modules for privileged users and vendors would be provided.
- Training completion to be tracked via internal LMS; non-compliance escalated and reported for necessary action.

10. Data Disposal

- Digital data: Secure erase using tools compliant with MeitY standards.
- Physical records: Cross-cut shredding or certified destruction.
- Disposal logs retained for 1 year or more depending on the sensitivity of the information / data to be disposed.

11. Policy Governance

- All changes must be versioned and approved by the Policy Owner through the relevant University Authority.
- Maintain a change-log with stakeholder sign-offs.
- Exceptions require formal request and written approval from the relevant University Authorities.

12. Third-Party Risk Management

- Authorised Vendors must undergo security vetting and sign DPDP-compliant data processing agreements.
- Contracts must include breach notification & penalty clauses and SLA-based security controls.
- Offboarding of vendors or third-party associates/affiliates/firms must include credential revocation and data handover.

13. Mobile & BYOD Policy

- Personal devices must be registered, encrypted, and monitored for accessing any University system that comes in the definition of an IT asset.
- Remote wipe capability required for access to sensitive systems.



- Unauthorized device connections are prohibited.

14. Cloud Usage

- Only MeitY-approved cloud providers may be used for storing / processing sensitive data.
- Data residency must comply with Indian jurisdictional / techno-legal requirements.
- Encryption in transit and at rest is mandatory.

15. Review & Updates

- This policy must be reviewed annually or upon regulatory/operational change.
- All Stakeholders be notified of updates via internal communication channels.
- Archived versions be retained for 5 years.

16. Compliance and Monitoring

- Regular internal / external audits of departments (teaching & administrative), conducted & constituent colleges/institutes and information systems must be conducted to ensure compliance with this policy.
- Any violation of this policy shall be subject to disciplinary actions suggested by the disciplinary committee.
- Users shall undergo periodic training on data protection and retention requirements as suggested or recommended from time to time.
- Internal audits be conducted quarterly and external audits be conducted annually through a competent / qualified authority or agency.
- Violations be categorized as Minor, Major, or Critical and actions be taken as per the policy.
- Disciplinary actions against any violation range from warnings to termination, based on the severity of the violation.

17. Appendix: Legal References

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