



UNIVERSITY OF YORK MUMBAI

Information Security Policy

1. Scope

- a. This Information Security Policy ("**Policy**") outlines the rules and guidelines for the proper usage, management, and maintenance of the University of York Mumbai's ("**University**") information technology resources and assets, in order to ensure their secure, ethical, and acceptable use.
- b. Overall ownership of this Policy rests with the University's IT Department. Legal or Compliance functions shall be consulted on updates that affect monitoring, access to personal data, or statutory reporting obligations.
- c. All staff, employees, students, and other authorised users are required to comply with this Policy while using any equipment, systems, or software provided or approved by the University.
- d. This Policy must be read together with the University's Privacy Policy, Privacy and Personal Data Protection SOP, and other applicable institutional policies. In the event of any inconsistency relating to the processing of personal data, the Privacy Policy shall prevail.

2. Purpose

- a. The purpose of this Policy is to protect the University's information and IT assets from security threats, misuse, damage, or theft, and to maintain data integrity, confidentiality, and operational continuity. This Policy establishes a University-wide approach to information security and

acceptable use, and compliance with applicable information technology, cybersecurity, and data protection laws in India.

- b. This Policy shall be reviewed annually to ensure its effectiveness and alignment with evolving legal, regulatory, and security requirements. Specific technical standards and operational controls set out in this Policy may be updated from time to time by the University's IT Department to address emerging risks and technologies, by circulating a memo of updates. Provided that where any policy updates have implications for personal data processing or user monitoring they shall be finalized in consultation with the University's legal or compliance function.

3. Account Creation and Management Policy

- a. All members of the University, including staff and students, shall be provided with an institutional user account with an initial password. Multi-factor authentication ("**MFA**") must be enabled for access to University systems and accounts, particularly where such access involves sensitive data, privileged functions, remote access, or elevated risk, as determined by the IT Department in accordance with the University's IT Security Standards. Users must log in using the assigned username and password and shall be required to change the initial password before accessing University resources and facilities. Privileged, administrative, and remote access accounts may be subject to enhanced authentication controls as determined by the IT Department.
- b. User accounts are subject to lifecycle management controls throughout their period of use. Where a user's role or responsibilities change, access rights must be reviewed and adjusted to reflect current operational requirements. Upon cessation of affiliation with the University (including employment termination, graduation, or completion of contractual engagement), user accounts must be promptly disabled or deactivated in accordance with the University's access management procedures. Detailed account provisioning, modification, and de-provisioning procedures are to be maintained by the IT Department as part of the aforesaid access management procedures.

4. Password Management Policy

- a. The objective of password management is to enhance information security by ensuring that passwords are strong, confidential, and properly used.
- b. Passwords must be changed at least once every year and shall satisfy the following minimum requirements:
 - (i) contain at least ten (10) and ideally twelve (12) characters;
 - (ii) include a mix of upper- and lower-case letters, with at least one capital letter and one special character.

Where supported by University systems, multi-factor authentication shall be enabled for access to University systems in accordance with the University's IT security standards, including through central authentication mechanisms where applicable.

- c. Passwords must not contain usernames, easily discoverable personal information, initial passwords, or previously used passwords.
- d. Users must not share their passwords with any other person and must take reasonable precautions to ensure that passwords are not observed or compromised.
- e. Users shall be required to change their password where their account is believed to have been compromised.

5. User Account Management

- a. University-issued email addresses are provided to students and staff with a valid affiliation with the University for academic and institutional communication purposes. Incidental personal use is permitted provided it does not interfere with academic or operational objectives.
- b. Email services are provided only for the duration of a user's affiliation with the University. Upon termination of such affiliation, access to the email service and mailbox contents may be withdrawn.
- c. The relevant department heads or supervisors are responsible for ensuring that email accounts no longer required are reported to the IT Department for de-provisioning. De-provisioning of user accounts shall be initiated by the relevant administrative function (Student Administration or Human Resources, as applicable) upon cessation of a user's affiliation with the University, and shall be implemented and

documented by the IT Department in accordance with institutional access-control procedures.

- d. The email service must be used responsibly and in a manner that does not violate University policies or applicable law. Prohibited uses include:
 - (i) sending messages that violate University policies;
 - (ii) sending spam or unauthorised communications;
 - (iii) impersonation or false representation of the University;
 - (iv) use for unauthorised commercial activities;
 - (v) unauthorised access to another person's account.
- e. Users are expected to follow reasonable security practices, including exercising caution with external links and attachments and using available security features such as multi-factor authentication where provided.
- f. The University email system and associated communications infrastructure are University property.
- g. Any monitoring, access, or review of University email systems shall be undertaken in accordance with applicable law and the University's Privacy Policy, with senior leadership or legal approval, and only to the extent necessary for legitimate security, operational, or legal purposes.
- h. Users must promptly report suspected compromise of their email accounts, including phishing, spoofing, or other social engineering attempts, via the IT helpdesk or designated security contact notified by the IT Department.
- i. Violations of this Policy may result in disciplinary action, depending on the nature and severity of the breach.

6. Bulk or Broadcast Emails

- a. Broadcast emails to students shall be limited to academic or institutional purposes and shall be sent only through approved systems.
- b. Personal email addresses of recipients must not be disclosed in such emails.
- c. Prior coordination with the IT Department may be required where a proposed broadcast involves system-wide distribution, unusual volume

- d. or urgency, or technical, security, or data-protection risk, in order to ensure appropriate safeguards are in place.

7. Shared Drive Policy

- a. All shared drives must have at least one designated manager with a University-issued email address.
- b. University data must not be transferred to personal accounts during or after affiliation with the University.
- c. Responsibility for continuity of access must be ensured before a user exits the University.
- d. Storage of excessive or unnecessary data on shared drives should be avoided.
- e. Data retention and deletion shall be carried out in accordance with applicable University policies and legal requirements.

8. Use of Computing Resources

- a. Users are responsible for the careful, secure, and appropriate use of all computing resources allocated to or accessed by them.
- b. Users must:
 - (i) comply with email and account usage rules;
 - (ii) protect account credentials from misuse;
 - (iii) promptly report loss or theft of devices containing University information or personal data, to the IT Department.
- c. Prohibited uses include unauthorised access, security circumvention, illegal activity, copyright infringement, and misuse of University systems.
- d. The University may impose reasonable limits on system usage to ensure equitable and secure access.
- e. Users must comply with all applicable laws and licence conditions.
- f. The IT Department may temporarily suspend or withdraw access to computer resources, without prior notice, where necessary to protect the security or integrity of University systems. Such actions shall be documented, and affected users shall be notified as soon as practicable

unless doing so would compromise security or an ongoing investigation. Significant access restrictions imposed under this clause shall be reported periodically to the appropriate institutional authority or committee.

9. Phone Usage and Printer Policy

- a. University communication systems are intended for official use.
- b. Users must follow appropriate communication etiquette.
- c. Mobile devices and laptops used for University purposes must be secured and encrypted where feasible.
- d. Access to printers, storage devices, and peripherals shall be restricted to authorised users.
- e. Confidential documents must be printed only when necessary and collected promptly.

10. Remote Control Facility Policy

- a. Remote access tools may be used by authorised personnel for support purposes with user consent.
- b. Explicit user permission must be obtained and recorded by IT support personnel prior to initiating any remote control session, in accordance with IT support procedures.
- c. Users must be informed when remote access is initiated and terminated.
- d. Misuse of remote access facilities constitutes a breach of this Policy.

11. Electronic Data and Privacy

- a. The University is committed to protecting personal data and information processed through its IT systems, in accordance with applicable law and the University's Privacy Policy. Loss or misuse of information may result in legal, financial, and reputational harm.
- b. Users must comply with University policies when creating, storing, transmitting, or destroying University information, including the University's Privacy Policy, Privacy and Personal Data Protection SOP, and any information security standards or technical guidance issued by the IT Department from time to time.

- c. Users must take reasonable measures to secure personal data, including locking devices, securing physical records, and preventing unauthorised access.
- d. Access to systems containing personal data shall be restricted and documented in accordance with the University's information classification and access control frameworks. Access rights shall be reviewed periodically and upon role changes or cessation of affiliation.
- e. Personal data accessed through the University must not be stored on personal devices unless expressly authorised and secured in accordance with University standards.
- f. The University may deny access to University systems from devices that do not meet security requirements. Any such measures shall be proportionate, risk-based, and carried out in accordance with applicable law and University policies. This may include controls relating to third-party platforms, cloud services, or externally hosted systems used for academic or administrative purposes.
- g. This Policy uses the following terms to describe information requiring security controls: (i) "confidential" information refers to non-public University information that requires protection from unauthorized disclosure; (ii) "sensitive" or "restricted" data or information refers to categories of personal data or University information requiring enhanced safeguards due to legal, regulatory, or contractual obligations. Detailed classification criteria and handling requirements for different categories of information are maintained by the IT Department in coordination with the Legal or Compliance function, and communicated to users via the University IT portal and onboarding materials.

12. IT Services Support and User Guidance

- a. IT support is provided in accordance with institutional priorities and capacity. Support may be provided through phone, email, or in person. Support for personal devices may be limited in scope and duration.
- b. The University shall ensure that users are provided with appropriate training, guidance, and awareness on the secure and acceptable use of IT resources, including through onboarding processes and periodic communications coordinated by designated IT Department personnel.

Completion of mandatory information security awareness activities may be required for certain user groups.

13. IT Incident Reporting and Response

- a. Users must promptly report suspected or actual IT incidents to the IT Department through channels communicated during onboarding and maintained on the University IT portal, which shall include anonymous reporting options.
- b. The IT Department is responsible for investigation, containment, and responding to IT security incidents in accordance with the University's Cyber Incident Response Plan.
- c. Where an incident involves or may involve personal data, the incident shall be escalated to the Legal or Compliance function for assessment of obligations under data protection and cybersecurity laws.
- d. The IT Department shall ensure timely technical reporting of cybersecurity incidents to appropriate external authorities in accordance with applicable law and regulations (including CERT-In requirements), in coordination with the Legal or Compliance function, which shall have oversight of regulatory assessment, documentation, and any notifications to authorities or affected individuals. Post-incident reviews may be conducted to identify corrective and preventive actions.
- e. Detailed incident response procedures, reporting channels, escalation criteria, and contact information are maintained in the IT Security Incident Response Plan to be maintained by the IT Department.

14. Governance and Enforcement

Compliance with this Policy is mandatory. Violations may result in disciplinary or corrective action in accordance with University policies and applicable law. The University may conduct periodic audits or assessments to evaluate compliance with this Policy and associated standards.

15. Review and Updates

- a. This Policy shall be reviewed periodically, and in any event not less than once each year. Updates may be issued to address changes in law, technology, or institutional practices.
- b. Reviews under this section shall take into account updates to the University's privacy and information security framework, including its Privacy Policy, Privacy and Personal Data Protection SOP, applicable IT

- c. Security standards and incident response procedures developed by the IT Department.