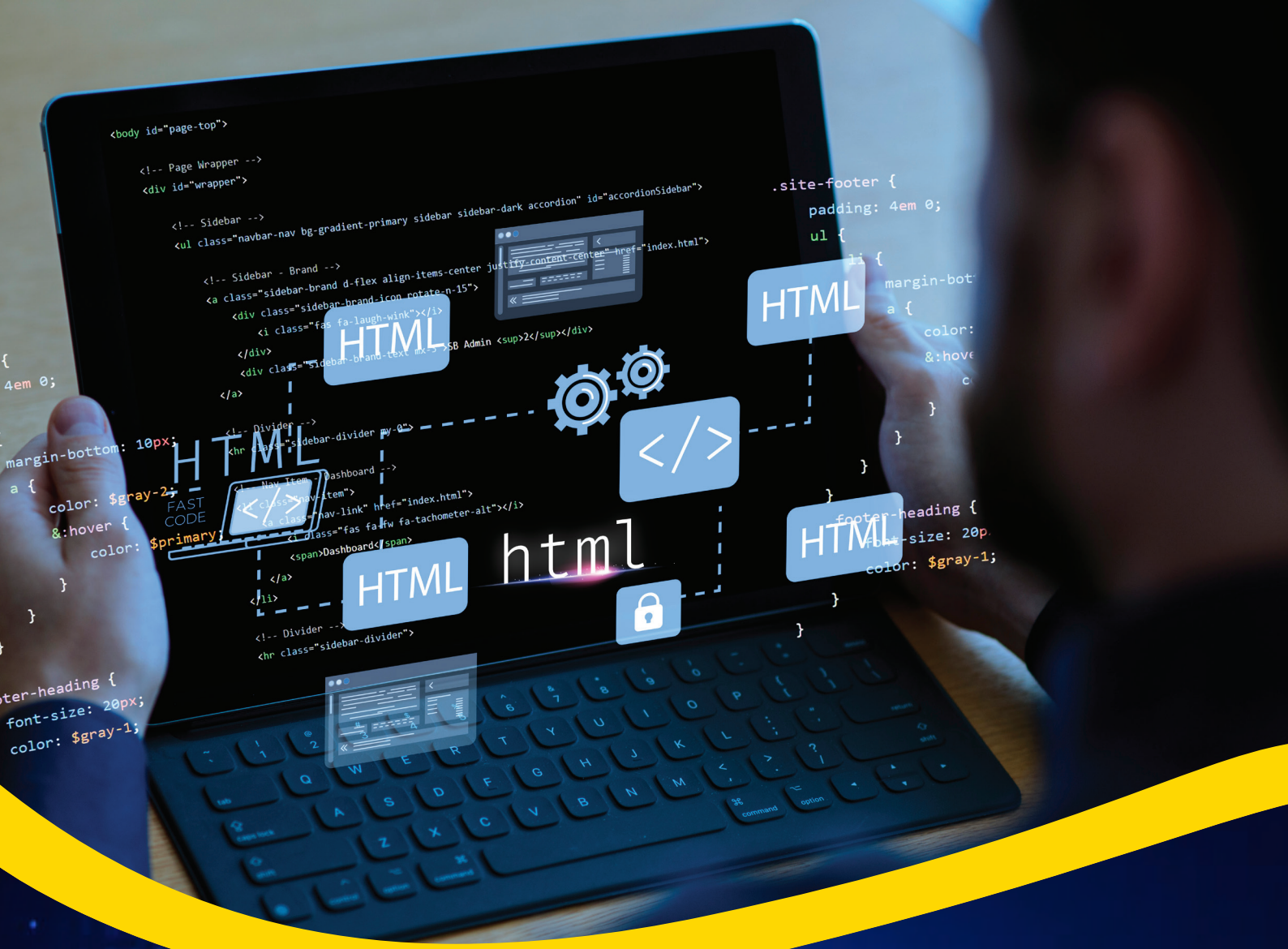


# IT POLICY

ITM UNIVERSITY
GWALIOR • MP • INDIA
"CELEBRATING DREAMS"

## Message from Vice Chancellor

**Dear Students, Faculty, and Staff,**

At ITM University, Gwalior, we recognize the transformative power of technology in education. To fully leverage this potential and ensure a secure and productive learning environment, I am pleased to announce the implementation of a new IT policy. This policy serves as a roadmap for responsible and effective technology use within our university community.

The new IT policy outlines clear guidelines for accessing and utilizing university IT resources. It emphasizes secure practices like strong password management and responsible data handling. The policy also addresses responsible use of university-provided email and internet access, ensuring a professional and productive online environment for everyone. Additionally, the policy recognizes the growing importance of personal devices in education and establishes protocols for their safe and secure integration within the university network.

By fostering responsible and ethical technology use, this new IT policy empowers our students, faculty, and staff to leverage technology for academic success. We believe this policy will create a secure and productive learning environment where technology facilitates collaboration, knowledge sharing, and innovative learning experiences. Together, let's embrace the power of technology to propel ITM University towards a future of academic excellence and boundless learning possibilities.

**Vice Chancellor**

ITM University Gwalior

# IT POLICY

# TABLE OF CONTENTS

## 1. ABBREVIATION

| Sl. No. | Abbreviation | Description |
|---|---|---|
| 1. | ITMU | ITM University |
| 2. | CA | Competent Authority |
| 3. | IA | Implementing Agency |
| 4. | LAN | Local Area Network |
| 5. | GoI | Government of India |
| 6. | IT | Information Technology |
| 7. | ICT | Information and Communication Technology |
| 8. | IP | Internet Protocol |
| 9. | DHCP | Dynamic Host Configuration Protocol |
| 10. | IR | Institutional Repository |
| 11. | EULA | End User License Agreement |
| 12. | CAPEX | Capital Expenditure |
| 13. | OPEX | Operational Expenditure |

## 2. INTRODUCTION

ITM University (ITMU) furnishes IT resources to support the educational, instructional, research, and administrative endeavors of the institution, aiming to bolster the efficiency and productivity of its personnel. These resources serve as aids for accessing and processing information pertinent to their respective domains of operation, enabling them to stay abreast of developments and execute their duties proficiently.

This policy delineates specific requisites governing the utilization of all IT resources within ITMU. Applicable to all individuals utilizing computing assets owned or overseen by ITMU, this policy encompasses ITMU faculty, visiting faculty, staff, students, alumni, guests, external entities, organizations, departments, offices, affiliated colleges, and any other entities under ITM University's purview accessing network services via ITMU's computing infrastructure.

For the purposes of this policy, the term 'IT Resources' encompasses all hardware and software owned, licensed, or managed by the university, as well as the utilization of the university network via wired or wireless connections, irrespective of the ownership of the connected computer or device.

The improper use of these resources may expose the university to unwarranted risks and liabilities. Consequently, it is imperative that these resources be primarily employed for university-related endeavors and in a manner consistent with legal and ethical standards.

## 3. SCOPE

This policy regulates the utilization of IT Resources from the viewpoint of end users. It applies to all individuals, users, or entities accessing the IT Resources provided by ITMU.

## 4. OBJECTIVE

The aim of this policy is to guarantee the proper access to and utilization of ITMU's IT resources while preventing their misuse by users. By utilizing resources provided by ITMU, users implicitly agree to abide by this policy.

- The University IT policy is in place to uphold, secure, and ensure the lawful and suitable utilization of the Information Technology infrastructure established by the University on its premises.
- This policy outlines University-wide strategies and responsibilities for safeguarding the Confidentiality, Integrity, and Availability of the information assets managed, accessed, created, and/or controlled by the University.
- Information assets covered by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

## 5. ROLES AND RESPONSIBILITIES

The following roles and responsibilities are delineated for each respective entity:

1) ITMU is tasked with implementing suitable controls to ensure adherence to this policy by its users. The Computer Centre serves as the primary Implementing Agency and will offer necessary support in this capacity.
2) The Computer Centre is responsible for resolving all incidents related to the security aspects outlined in this policy by its users. The Implementing Agency will extend the required support in this regard.
3) Users are expected to utilize ITMU's IT resources for activities aligned with the academic, research, and public service mission of the University and refrain from engaging in "Prohibited Activities."
4) All users must adhere to existing national, state, and other relevant laws.
5) Users are required to abide by existing telecommunications and networking laws and regulations.
6) Users must adhere to copyright laws pertaining to protected commercial software or intellectual property.
7) As members of the University community, ITMU provides access to scholarly and/or work-related tools, including the library, specific computer systems, servers, software, databases, and the Internet. The University community expects reasonable access to these tools, a certain level of privacy, and protection from abuse and intrusion. Authorized users can expect their right to access information and express their opinions to be safeguarded, similar to non-electronic communication forms.
8) Users of ITMU are prohibited from installing any network/security device on the network without consulting the Implementing Agency.
9) It is the responsibility of the University Community to familiarize themselves with the regulations and policies governing the appropriate use of the University's technologies and resources. The University Community is accountable for exercising discretion in the use of these resources. Just because an action is technically feasible does not necessarily mean it is appropriate.

10) As representatives of the ITMU community, individuals are expected to uphold and respect the University's reputation in any ICT communications-related activities, both within and outside the university.

11) The Competent Authority of ITMU is tasked with ensuring the proper dissemination of this policy.

## 6. ACCEPTABLE USE

- Authorized users are permitted to utilize only the IT resources for which they have been granted permission. It is strictly prohibited for any user to utilize another individual's account or attempt to gain unauthorized access by capturing or guessing passwords.
- Users are personally accountable for the appropriate utilization of all resources allocated to them, encompassing computers, network addresses or ports, software, and hardware. Consequently, users bear responsibility to the University for all activities involving such resources. As authorized ITMU users, they must refrain from engaging in or facilitating unauthorized access to the network, whether through ITMU's resources or personal computers connected to ITMU's campus-wide Local Area Network (LAN).
- The University is obligated by its End User License Agreement (EULA) regarding specific third-party resources, and users are expected to adhere to all such agreements when utilizing said resources.
- Users are encouraged to take reasonable measures to safeguard their passwords and ensure resources are protected against unauthorized use or access.
- Users must not attempt to access restricted sections of the network, operating systems, security software, or other administrative applications without appropriate authorization from the system owner or administrator.
- Users must adhere to the policies and guidelines governing any specific set of resources to which they have been granted access.
- In cases where other policies impose more stringent restrictions than this policy, the more restrictive policy shall take precedence.

## 7. PRIVACY AND PERSONAL RIGHTS

1) Users of the university's IT resources are required to uphold the privacy and personal rights of others.

2) Unauthorized access or duplication of another user's email, data, programs, or files is strictly prohibited without approval from the Competent Authority (CA).

3) Although the University typically refrains from monitoring or restricting the content of information transmitted on the campus-wide LAN, it retains the right to access and review such information under specific conditions, with prior approval from the competent authority.

## 8. PRIVACY IN EMAIL

Although extensive measures are taken to safeguard the privacy of ITMU email users,

complete privacy cannot always be guaranteed. As employees are provided access to electronic information systems and network services for conducting University-related tasks, there may arise situations where, with approval from the competent authority, the University reserves the right to access and review stored information, provided the user consents to such inspection.

## 9. USER COMPLIANCE

When utilizing ITMU's IT resources and accepting any computing accounts issued by the University, individuals implicitly consent to adhere to this policy and all other relevant computing policies. It is the individual's responsibility to remain informed about updates to ITMU's IT policy and adjust accordingly as needed.

## 10. ACCESS TO THE NETWORK

### 10.1. Access to Internet and Intranet

1) Before connecting a client system to the University's Campus-wide LAN, a user must register the system and secure one-time approval from the competent authority.
2) ITMU will uphold two distinct networks, namely Internet and Intranet, with no physical connection or devices linking them. End-point compliance measures will be enforced on both networks to thwart unauthorized data access.
3) Users are prohibited from engaging in activities via websites or applications aimed at bypassing network filtering or conducting any unlawful actions that may compromise the network's performance or security.

### 10.2. Access to ITMU's Wireless Networks

To connect to ITMU's wireless network, users must adhere to the following guidelines:

1) Before connecting their access device to ITMU's wireless network, users must register the device and secure one-time approval from the competent authority.
2) Wireless client systems and devices are strictly prohibited from connecting to ITMU's wireless access points without proper authentication.
3) To safeguard information security, it is advisable for users to refrain from connecting their devices to unsecured wireless networks.

### 10.3. Filtering and blocking of sites:

1) The Computer Centre or any designated Implementing Agency (IA) reserves the authority to restrict internet content that violates provisions outlined in the IT Act 2000 and other relevant laws, or presents a potential security risk to the network.
2) Additionally, the Computer Centre or any designated Implementing Agency (IA) retains the right to block content deemed inappropriate by the university or that may hinder user productivity.

## 11. MONITORING AND PRIVACY

1) The Computer Centre or any designated Implementing Agency (IA) is authorized to conduct regular network and system audits to ensure compliance with this policy.

2) For security purposes or to comply with relevant laws, the IA/Nodal Agency reserves the right to access, review, copy, or delete any electronic communications or files stored on university-provided devices, with notification to the user. This encompasses files, emails, posts on electronic platforms, internet history, and similar items.

3) The IA may monitor users' online activities on the University network in accordance with established Standard Operating Procedures and Government of India norms.

## 12. E-MAIL ACCESS FROM THE UNIVERSITY NETWORK

1) The email service sanctioned by ITMU and managed by the Computer Centre is designated solely for official correspondence purposes.

2) Further information on this matter can be found in the "E-mail Usage Policy of ITMU."

## 13. SECURITY INCIDENT MANAGEMENT PROCESS

1.1. A security incident encompasses any adverse event capable of affecting the availability, integrity, confidentiality, and authority of the University's data.

1.2. The IA retains the authority to deactivate or remove any device from the network if it poses a threat and could potentially compromise a system, with notification to the competent authority of the university.

1.3. Any observed security incident must be promptly reported to the Computer Centre of the University.

1.4. Notwithstanding the aforementioned clause, the disclosure of logs pertaining to or contained within any IT Resource to Law Enforcement agencies and other organizations by the IA shall adhere to the provisions outlined in the IT Act 2000 and other applicable laws.

1.5. The IA shall decline any request from other organizations for the examination or release of logs, except as specified within this clause.

## 14. INTELLECTUAL PROPERTY

Content available via ITMU's network and resources may be legally protected under various rights, including privacy, publicity, and intellectual property laws such as copyrights, patents, trademarks, and trade secrets. Users are strictly prohibited from utilizing ITMU's network and resources in any way that violates or infringes upon these rights, including but not limited to infringement, dilution, or misappropriation.

## 15. ENFORCEMENT

1.1. This policy applies to all ITMU users, as outlined in Section 2 of this document. Adherence to the provisions of this policy is mandatory for all users.

1.2. Each division of ITMU is accountable for ensuring compliance with this policy. The Implementing Agency will offer the required technical support to user entities for this purpose.

## 16. DEACTIVATION

1.1. If a user's resources pose a security threat to ITMU's systems or network, the Implementing Agency (IA) may deactivate the resources immediately.

1.2. Following the deactivation, both the user in question and the competent authority of the university will be notified.

## 17. AUDIT OF ITMU NETWORK INFRASTRUCTURE

The Computer Centre of the University, along with an organization sanctioned by the university, will conduct regular security audits of the NIC network infrastructure.

## 18. IT HARDWARE INSTALLATION POLICY

The University network user community must take certain precautions when installing computers or peripherals to minimize service interruptions due to hardware failures.

### A. Primary User:

An individual whose room houses the computer primarily used by them is considered the "primary" user. If a computer has multiple users without a designated primary user, the department head should appoint a responsible person for compliance.

### B. End User Computer Systems:

In addition to client PCs, servers not directly managed by the Computer Centre are considered end-user computers. If no primary user is identified, the department assumes responsibilities designated for end-users. Servers providing services to users on the Intranet/Internet, although registered with the Computer Centre, are still considered "end-user" computers under this policy.

### C. Warranty & Annual Maintenance Contract:

Computers procured by any section/department/project should ideally come with a 3-year onsite comprehensive warranty. Post-warranty, computers should be covered by an annual maintenance contract, including standard repair and maintenance procedures defined by the Computer Centre.

### D. Power Connection to Computers and Peripherals:

All computers and peripherals should be connected to electrical points via UPS. The power supply to the UPS should remain uninterrupted for battery recharging, except when the UPS is left unattended. Additionally, UPS systems should be connected to properly earthed electrical points with well-laid wiring.

### E. Network Connection:

When connecting computers to the network, ensure that network cables are kept away from electrical/electronic equipment to prevent interference. Furthermore, avoid sharing power supplies with other electrical/electronic equipment connected to the computer and its peripherals.

### F. File and Print Sharing Facilities:

File and print sharing over the network should only be installed when absolutely necessary. When sharing files, ensure they are protected with passwords and read-only access rules.

### G. Maintenance of University-provided Computer Systems:

The University Computer Maintenance Cell, attached to the Computer Centre, will handle complaints related to maintenance problems for centrally purchased computers distributed by the Estate Branch.

## 19. SOFTWARE INSTALLATION AND LICENSING POLICY

All computer acquisitions by individual departments/projects must ensure that the systems are equipped with licensed software, including the operating system, antivirus software, and required applications.

In adherence to anti-piracy laws, the University IT policy prohibits the installation of pirated or unauthorized software on university-owned computers and those connected to the campus network. Any instances of such installations will result in the department/individual being held personally accountable by the university for any pirated software found on computers within their department or personal spaces.

### A. Operating System and Updates:

Individual users must ensure that their computer systems have their operating systems updated with the latest service packs and patches via the internet. Checking for updates and updating the OS should be conducted at least once a week. As a policy, the University encourages the user community to utilize open-source software like Linux and OpenOffice whenever feasible.

### B. Software Usage on Desktop Systems:

a. Users are prohibited from copying or installing any software on their desktop systems, including privately-owned shareware and freeware, without approval from the competent authority.

b. Any software installed must be utilized solely for university-related activities.

### C. Antivirus Software and Updates:

Computer systems within the university premises should have antivirus software installed and active at all times. The primary user of a computer system is responsible for ensuring compliance with this virus protection policy. Individual users should ensure that their computer systems have current antivirus software installed and regularly updated.

### D. Data Backups:

Individual users are responsible for regularly backing up their essential data. They should store their backups on external storage devices such as pen drives or external hard drives.

## 20. USE OF IT DEVICES ON ITMU NETWORK

This section outlines the best practices for utilizing desktop devices, portable devices, external storage media, and peripheral devices such as printers and scanners on ITMU's network.

### 20.1. Desktop Devices

**1. Use and Ownership:**

Desktops should primarily be utilized for conducting university-related tasks. Users are advised to limit personal use of desktop devices to the minimum extent possible, exercising

good judgment and discretion.

**2. Security and Protection of Proprietary Information:**

a. Users must obtain prior approval from the IA before connecting any access device to ITMU's network.

b. Users are responsible for maintaining the security of their passwords and must not share their account details. Passwords should adhere to the password policy of the application, ensuring they are strong and secure.

c. All active desktop computers must be secured with a password-protected screensaver set to activate automatically after 10 minutes of inactivity or less, or to log off when the system is unattended.

d. Users should ensure that updated virus-scanning software is active on all systems. Caution must be exercised when opening email attachments from unknown senders, as they may contain viruses, email bombs, or Trojan horse code.

e. Users must promptly report any loss of data or accessories to the IA and the competent authority of ITMU.

f. Authorization must be obtained from the competent authority before removing any ITMU-issued desktop from the university premises.

g. Users are required to properly shut down systems before leaving the office or department.

h. Users must comply with instructions or procedures issued by the Computer Centre as necessary.

i. If users suspect that their computer has been infected with a virus (e.g., it exhibits erratic behavior or slows down), they should report it to the IA (Computer Centre) for corrective action.

## 20.2. Sharing of data

Users are prohibited from sharing their account(s), passwords, Personal Identification Numbers (PINs), digital signatures certificates, or any similar information or devices used for identification and authorization purposes.

## 20.3. Use of Portable devices

Devices covered under this section include ITMU-issued laptops, mobiles, iPads, tablets, PDAs, etc. The use of these devices is governed by the following:

a. Users are responsible for any unauthorized usage of their ITMU-issued access device by a third party.

b. Users must keep ITMU-issued devices with them at all times or store them in a secured location when not in use. Devices should not be left unattended in public locations (e.g., classrooms, meeting rooms, restaurants, etc.).

c. Users must ensure that portable devices are password-protected and have auto-lockout enabled. Passwords should be as strong as the device supports and comply with the password policy of the application.

d. The Computer Centre will ensure that the latest operating system, antivirus, and application patches are available on all devices, in coordination with the user. Firewalls should be enabled whenever possible.

e. Users must wipe or securely delete data from the device before returning or disposing of it.

f. Lost, stolen, or misplaced devices must be reported immediately to the IA and the competent authority.

g. When installing software, users should review the application permissions to prevent unwanted sharing of user information with the application provider.

## 21. NETWORK (INTRANET & INTERNET) USE POLICY

The network connectivity provided by the University, hereafter referred to as "the Network," whether through an authenticated network access connection or a Virtual Private Network (VPN) connection, is regulated by the University IT Policy. The Computer Centre is responsible for the continuous maintenance and support of the Network, excluding local applications. Any issues encountered within the University's network should be promptly reported to the Computer Centre.

### A. IP Address Allocation:

Any computer (PC/Server) connecting to the university network must be assigned an IP address by the Computer Centre. IP address allocation follows a systematic approach, with addresses assigned based on Virtual LAN (VLAN) configurations specific to each entity or objective. Each network port in a room is internally bound to an IP address to prevent unauthorized usage elsewhere. New computer installations are allocated IP addresses according to DHCP pool policies, with each computer obtaining a unique address through a requisition process.

### B. DHCP and Proxy Configuration by Individual Departments/Sections/Users:

End users are prohibited from setting up any computer as a DHCP server to distribute IP addresses through individual switches/hubs, or configuring proxy servers, as it violates university IP address allocation policies. This includes configuring additional network interface cards for proxy/DHCP purposes. Non-compliance will result in port disconnection, restored only upon written assurance of compliance from the department/user.

### C. Running Network Services on Servers:

a. Departments/individuals connecting to the university network may run server software (e.g., HTTP/Web server, SMTP server, FTP server) after notifying the Computer Centre in writing and meeting university IT policy requirements. Non-compliance results in termination of network connection.

b. The Computer Centre bears no responsibility for the content of machines connected to the Network, regardless of ownership.

c. Client machines may be disconnected if potentially damaging software is found or if their activity affects network performance adversely.

d. Access to remote networks via the university network must comply with those networks' policies and rules, with university resources not used for personal commercial purposes.

e. Network traffic is monitored for security and performance reasons by the Computer Centre.

f. Impersonating an authorized user to connect to the Network violates this policy and results in connection termination.

### D. Internet Bandwidth obtained by Other Departments:

a. Internet bandwidth obtained by university departments under research programs/ projects should ideally be pooled with university bandwidth and treated as a common resource.

b. If pooling is not feasible, the network should be entirely separate from the university's campus network, with separate VLANs for all computer systems. Network security measures must align with university IT policy, with network diagrams submitted to the Computer Centre.

c. Non-compliance constitutes a direct violation of the university's IT security policy.

## 22. EMAIL ACCOUNT USAGE POLICY

ITMU offers official email access to its users to facilitate efficient information dissemination among administration, faculty, staff, and students. To enhance the distribution of critical information, it is advised to utilize the university's email services for formal communication and official purposes.

Email communication enables the delivery of messages and documents to campus and extended communities or specific user groups. Formal university communications include official notices, administrative content, policy messages, general announcements, etc.

To receive these notices, maintaining an active email address is crucial. Staff and faculty can access the email facility by logging on to http://gmail.com with their User ID and password. To obtain the university's email account, users can contact the Computer Centre for an email account and default password by submitting an application.

By using the email facility, users agree to abide by the following policies:

1.1 The facility should primarily be used for academic and official purposes, with limited personal use.

1.2 Using the facility for illegal/commercial purposes violates the university's IT policy and may result in withdrawal of the facility. This includes unlicensed software copying, sending unsolicited bulk emails, and generating threatening, harassing, abusive, obscene, or fraudulent messages/images.

1.3 When sending large attachments, users should ensure the recipient's email facility can receive such attachments.

1.4 Users should keep mailbox usage within 80% threshold to avoid mail bouncing, especially for incoming mail with large attachments.

1.5 Users should avoid opening emails or attachments from unknown and suspicious sources. Even if from a known source, confirmation about authenticity should be sought before opening suspicious attachments to prevent potential damage from viruses.

1.6 Users should not share their email account credentials as they are personally accountable for any misuse.

1.7 Intercepting or attempting to break into others' email accounts infringes on users' privacy.

1.8 Users should promptly close accidentally open email accounts on shared computers without accessing their contents.

1.9 Impersonating others' email accounts is a serious offense under the IT security policy.

1.10 Each individual is responsible for ensuring their email account complies with the university's email usage policy.

1.11 Users should periodically check their SPAM_MAIL folder for important emails wrongly marked as spam and empty it frequently.

The above policies apply broadly, even to email services provided by other providers like Gmail, Hotmail, Yahoo, Rediff Mail, when used from the university's campus network or resources provided by the university for official use, even outside the campus.

## 23. INSTITUTIONAL REPOSITORY (IR)

Services related to the Institutional Repository (IR) at ITM University will be facilitated through the Central Library, adhering to the following policies:

### 23.1 What is IR (Institutional Repository)?

An institutional repository (IR) based at a university entails a range of services provided by the university library to its community members. These services facilitate the management and distribution of digital materials generated by the university or institution and its members. Essentially, it signifies the organization's dedication to preserving, accessing, and disseminating digital resources over the long term for the benefit of its users.

### 23.2 What Does IR contain?

The institutional repository (IR) of the institution encompasses a diverse array of documents, subject to the institution's policies. Among the most common are research outputs such as journal articles (pre-print and post-print), conference papers, technical reports, computer programs, presentations, technical manuals, video and audio recordings, e-books, seminar and webinar lectures, theses and dissertations, and rare books. Grey literature holds equal importance to published outputs within the IR. Additionally, the IR may include convocation addresses, student handbooks, and teaching materials. While some sources suggest integration with the university's course management system and incorporation of e-learning features, in practice, the ITM University's institutional repository (IR) primarily serves as a basic repository for online access to research and academic publications.

### 23.3 Who will be entitled to access ITM University IR?

Access to the ITM University's Institutional Repository (IR) is primarily granted to authorized members, including faculty members, research scholars, students, and staff members, who possess institutional email IDs (i.e., ending with "@itmuniversity.ac.in").

### 23.4 How will you access the IR?

Registered members can access the ITMU Institutional Repository (IR) by logging in with their institutional email address. They can browse the IR and download digital materials in PDF format strictly for academic purposes. However, they are required to provide general information about themselves as per the provisions outlined in the ITM University IR portal.

### 23.5 Validity Period of Accessibility of IR

Faculty, researchers, and students have access to the ITMU Institutional Repository (IR) during their tenure at the university. However, once they complete their course or leave the university and receive no-dues certificates from the University Library authority, their access to the ITMU IR will be revoked.

### 23.6 Copyright Violation on IR Use

The digital materials available in the ITM University Institutional Repository (IR) primarily consist of grey literature. Any digital materials downloaded from the IR are subject to copyright laws. It is prohibited to reproduce or sell downloaded materials for commercial purposes. Violation of copyright laws will be dealt with in accordance with the Copyright Act of 1957. User IDs and passwords are assigned to individual users and cannot be transferred to others. Violation of this policy will be subject to the standard operating procedures (SOPs) of the ITM University IR.

## 24. DISPOSAL OF ICT EQUIPMENT

ICT hardware equipment disposal must adhere to the Standard Operating Procedures outlined in the university's E-Waste Management guidelines.

### 24 Smart Classrooms

- Each department will have at least one digitized/smart classroom equipped with teaching aids such as projectors and speaker-enabled audio/video systems to enhance learning and facilitate the implementation of diverse teaching methodologies.
- These smart classrooms will be furnished with essential instruments and software required to facilitate hybrid learning approaches.

## 25. BREACH OF THIS POLICY

Users are strongly encouraged to remain vigilant and promptly report any suspected violations of this Policy to the Computer Centre. Upon receiving notice or becoming aware of any suspected breach of this Policy, the University retains the authority to suspend a user's access to university data.

In cases of observed breaches of this Policy, disciplinary action may be taken, including but not limited to dismissal for staff, expulsion for students, or contract termination for third parties, following the University's disciplinary procedures.

## 26. REVISIONS TO POLICY

The University retains the right to amend the terms of this Policy at its discretion. Any such changes will be documented in the policy's revision history, accessible on the ITMU website. By continuing to utilize the University's IT Resources after any modifications, users are deemed to accept the revised terms of this Policy.

UNIVERSITY

GWALIOR • MP • INDIA

"CELEBRATING DREAMS"