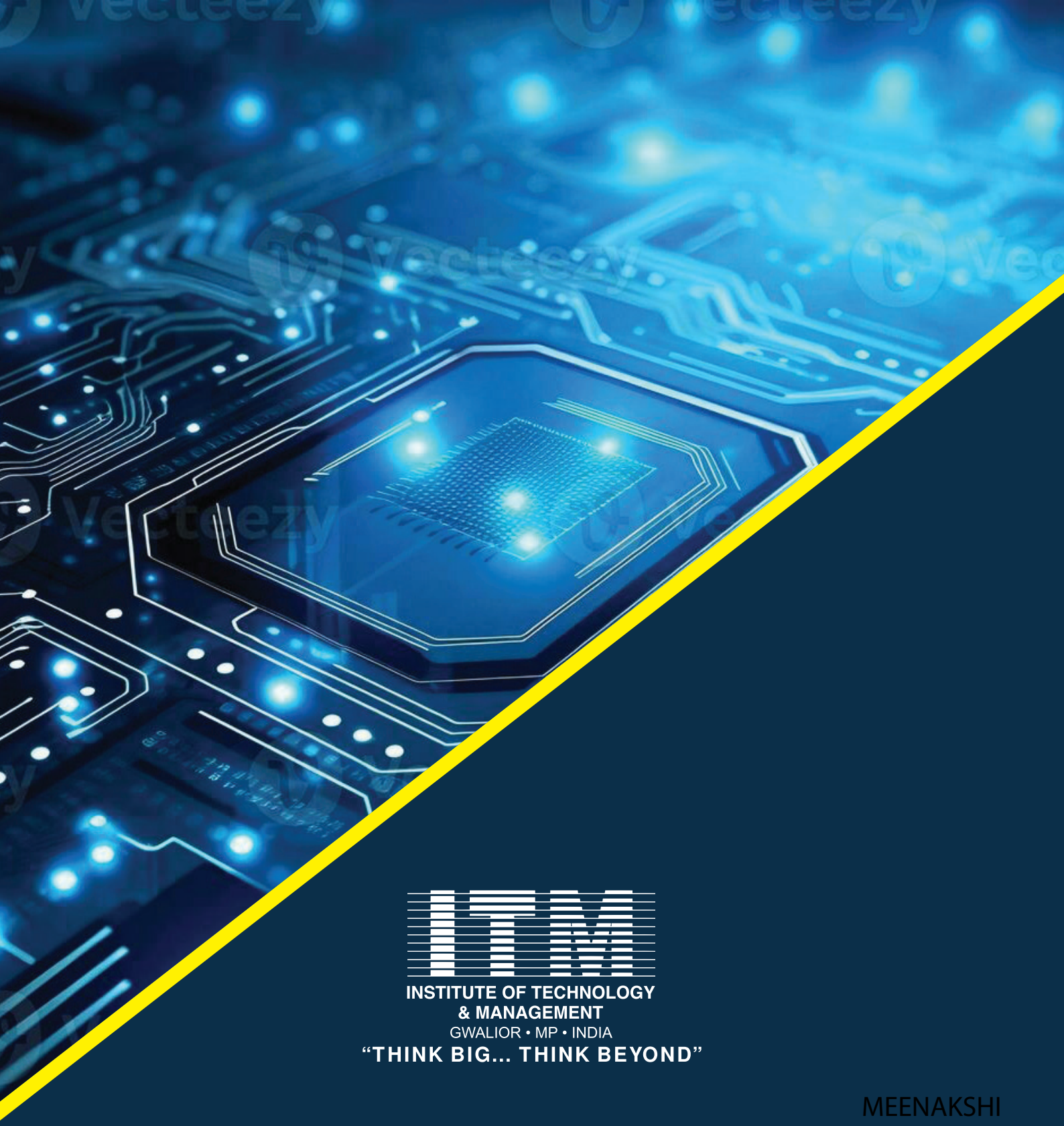

INSTITUTE OF TECHNOLOGY
& MANAGEMENT
GWALIOR • MP • INDIA
"THINK BIG... THINK BEYOND"

IT POLICY

MEENAKSHI MAZUMDAR

Digitally signed by MEENAKSHI MAZUMDAR
Date: 2024.09.14 11:08:55 +05'30'

INSTITUTE OF TECHNOLOGY & MANAGEMENT, GWALIOR
(AFFILIATED TO RGPV, BHOPAL)

Dr. Meenakshi Mazumdar
DIRECTOR
Institute of Technology & Management
Gwalior (M.P.)

INSTITUTE OF TECHNOLOGY
& MANAGEMENT
GWALIOR • MP • INDIA
"THINK BIG... THINK BEYOND"

Message from **Director**

Dear Students, Faculty, and Staff,

In the rapidly evolving world of education, technology stands at the forefront of our journey toward excellence. At ITM, Gwalior, we recognize the critical role that technology plays in enhancing our learning and teaching experiences. With this in mind, I am pleased to introduce a new IT policy that will serve as a blueprint for responsible and secure technology use within our community.

This policy is designed to provide clear, actionable guidelines for accessing and utilizing the IT resources of our institute. It emphasizes the importance of maintaining secure practices, such as creating strong passwords and handling data with care. These measures are essential not only for protecting our personal information but also for safeguarding the integrity of our academic work.

In addition to ensuring security, the policy also outlines expectations for the use of institute-provided email and internet services. By promoting a professional and productive online environment, we aim to support the academic and professional goals of every member of our community. Furthermore, recognizing the increasing reliance on personal devices in education, the policy includes specific protocols for their safe integration into our institute's network. This ensures that students, faculty, and staff can make the most of these tools without compromising the security of our systems.

The new IT policy is more than just a set of rules—it is a commitment to fostering an environment where technology is used thoughtfully and ethically. By adhering to these guidelines, we empower ourselves to leverage technology as a tool for growth, innovation, and success. This policy will help us create a secure, supportive, and forward-thinking educational environment where everyone can thrive.

As we move forward, I encourage each of you to embrace this policy and the opportunities it brings. Together, we can ensure that technology continues to drive ITM Gwalior toward new heights of academic achievement and success.

Director
ITM, Gwalior

1. Objectives:

1.1 To ensure the integrity, reliability, accessibility, and superior performance of the Institute's IT infrastructure.
1.2 To protect the official digital identity (email, login credentials) of each user.
1.3 To establish clear guidelines and responsibilities for the appropriate use of the Institute's IT resources by all users.

Applicability: This policy applies to all students, faculty, staff, and any other individuals (referred to as 'users') who utilize the Institute's Information Technology (IT) infrastructure, including but not limited to lab components, desktops/laptops, communication nodes, IT/ICT facilities, within the Institute's network or to access, transmit, or store Institutional and/or personal information.

Policy Statement: The IT/ICT resources provided by the Institute are to be used solely for teaching, learning, research, and administrative functions by the users. Users are responsible for the proper use, protection, and preservation of the Institute's IT resources, as well as respecting the rights and privacy of others. This policy serves as a comprehensive guideline for the safe, responsible, and legitimate use of the available IT resources and infrastructure.

2. IT Usage and Prohibitions:

2.1 **Authorized Use:** Users shall make effective, authorized, and ethical use of the internet, wireless resources, official websites, Learning Management Systems (LMS), Management Information Systems (MIS), online learning platforms, e-library resources, and other IT services.

2.2 **Compliance:** The Institute shall ensure that users comply with all applicable policies, laws, and legal obligations (including licenses and contracts).

2.3 **Awareness Programs:** The Institute shall organize regular awareness programs and training sessions to educate users on the effective and responsible usage of IT resources.

2.4 **Prohibited Use:** Users shall not engage in activities such as sending, viewing, or downloading fraudulent, harassing, obscene, threatening, or other materials that violate applicable laws or Institute policies. Behaviors that contribute to a hostile academic or work environment are strictly prohibited.

2.5 **Commercial Use:** The Institute's IT resources shall not be used for any commercial or promotional purposes, except as permitted under Institute rules or with the approval of the competent authority.

2.6 **Copyrights and Licenses:** Users must respect copyright laws and adhere to the terms of licensed materials. Unlawful file-sharing using the Institute's resources is a violation of this policy.

3. SECURITY AND INTEGRITY:

3.1 **Personal Use:** The Institute's IT resources should not be used for activities that violate the basic functionality and mission of the Institute, except in a purely incidental manner.
3.2 **Access Control:** Users must refrain from any unauthorized access or tampering of information to maintain the security of the network and computers.

3.3 **Authorized Access:** The competent system administrator may access the information resources for legitimate administrative and security purposes.

3.4 **Network Security:** The Institute shall manage a secured flow of internet and intranet-based traffic through the use of Unified Threat Management (firewall) solutions and other appropriate security measures.

3.5 **Anti-virus and Security Updates:** The Institute shall regularly update the anti-virus policy and security measures to protect computing resources from malware and other threats.

4. IT Asset and Hardware Management:

4.1 **Asset Management:** The Institute shall establish comprehensive processes for the management of hardware and software assets, including procedures for purchasing, deployment, maintenance, utilization, energy audits, and disposal.

4.2 **Licensing and Compliance:** The Institute shall ensure compliance with licensing requirements and prevent unauthorized copying and distribution of proprietary software.

4.3 **Risk Management:** The Institute shall manage the risks involved in the usage of IT resources, including data backup, replication, restoration, power backups, audit policies, and alternate internet connectivity.

4.4 **Open Source Promotion:** The Institute shall promote and encourage the effective use of open-source software and technologies.

4.5 **Primary User Responsibility:** The individual in whose room/workspace the computer is installed and primarily used is considered the "primary" user. The department head shall assign responsibility if a computer has multiple users without a defined primary user.

4.6 **End-User Computer Systems:** Apart from client PCs, the Institute shall consider servers not directly administered by the IT department as end-user computers. The department must assume the responsibilities if no primary user can be identified.

4.7 **Hardware Warranty and Maintenance:** Computers and peripherals should have a minimum 1-year / 3-yearon-site warranty, based on terms and conditions at purchase. After the warranty, they should be the under-maintenance cell of the institute for OS re-installation, virus checking and hardware failure detection and recovery (where possible). If required, services from the local vendors for maintenance may also be sought.

4.8 **Network Infrastructure:** The network cable should be installed following best practices to avoid interference from electrical/electronic equipment, and no other equipment should share the power supply. Further, the institute should have at least two dedicated internet connectivity services (leased lines) catering to the needs of the user effectively and also supporting during the failure of one connectivity.

4.9 **Noncompliance:** Non-compliance with the policy may result in punitive action, if needed.

5. Email Usage and Communication

5.1 Official Communication

a. Institutional email accounts should be used for all official communication.

b. Users are responsible for regularly checking their institutional email accounts.
c. Sensitive or confidential information should not be sent via email unless encrypted.

5.2 Email Security

a. Exercise caution when opening email attachments or clicking links, especially from unknown sources.
b. Report suspicious emails, including potential phishing attempts, to the IT department.
c. Institutional email should not be used for personal business or commercial activities.

5.3 Email Etiquette

a. Maintain professionalism in all email communications.
b. Be mindful of tone and content, as emails may be forwarded or become public.
c. Use appropriate distribution lists and avoid unnecessary "reply all" responses.

6. Software Installation and Licensing Policy:

6.1 Operating System and Updating:

a. Users should ensure their computers have the latest OS service packs/patches.
b. The Institute encourages the use of open-source software like Linux, Open Office and others.
c. Windows-based computers should access the Windows Update website for free updates.

6.2 Data Backups: Users should perform regular backups of their vital data, preferably by partitioning the hard disk and storing data on a separate volume.

6.3 Noncompliance: Non-compliance may result in virus infections, data loss, and other adverse effects on individuals and the Institute. Prompt compliance is critical. The users may use the malicious software removal utility provided by Windows OS.

7. Classroom Technology and Learning Management Systems

7.1 Smart Classrooms:

a. Users should be trained in the proper use of smart classroom equipment.
b. Any issues with classroom technology should be reported promptly to the IT department.
c. Faculty members are encouraged to incorporate technology into their teaching methods.

7.2 Learning Management Systems (LMS)

a. All courses should maintain a presence on the institutional LMS.
b. Faculty members are responsible for managing their course content on the LMS.
c. Students should regularly access the LMS for course materials and updates.

7.3 Online and Hybrid Learning

a. The institution will support online and hybrid learning technologies.
b. Users must adhere to academic integrity policies in online learning environments.
c. The IT department will ensure the security and reliability of online learning platforms.

8. Social Media and Online Presence

8.1 Institutional Social Media Accounts

a. Official institutional social media accounts must be approved and managed according to guidelines.
b. Users managing institutional accounts must receive training on best practices and policies.
c. The institution reserves the right to remove inappropriate content from official accounts.

8.2 Personal Use of Social Media

a. Users should exercise caution when posting about the institution on personal social media accounts.
b. Confidential or sensitive institutional information must not be shared on social media.
c. Users should be aware that their online activities may reflect on the institution.

8.3 Online Reputation Management

a. The institution will monitor its online reputation and address concerns as needed.
b. Users are encouraged to report any negative or false information about the institution found online.
c. The IT department will guide managing personal online reputations.

9. Violation of Policy:

Any violation of the IT Policy objectives and areas shall be considered misconduct and may attract a penalty/punitive action.

10. Implementation and Review of Policy:

The Institute shall regularly review and update the IT Policy as and when necessary, and decide on the necessary rules and procedures for its effective implementation.

Conclusion

This comprehensive IT policy aims to establish a secure, efficient, and innovative technology environment that supports the institution's mission. By adhering to these guidelines, all members contribute to the responsible use of IT resources and the protection of digital assets. The policy will be regularly reviewed and updated to address new challenges and opportunities. Users are encouraged to stay informed about policy updates and actively participate in maintaining a safe and productive IT ecosystem.

MEENAKSHI MAZUMDAR
Digitally signed by MEENAKSHI MAZUMDAR
Date: 2024.09.14 11:08:38 +05'30'

Dr. Meenakshi Mazumdar
DIRECTOR
Institute of Technology & Management
Gwalior (M.P.)