Prestige Institute of Management and Research, Gwalior

Information Technology Policy of PIMRG

Prestige Institute of Management and Research maintains Information policies that will enhance the Institute's academic excellence and other related activities. It includes gadgets, systems, tools, databases, logs, webspace, and networking. Any user, i.e. student, faculty, staff, non-teaching staff, management body, technical personnel, and developers, are expected to abide by these regulations.

1. Objectives:

1.1 To uphold the integrity, reliability, accessibility, and optimal performance of the IT Infrastructure at Prestige Institute of Management and Research, Gwalior.

1.2 To safeguard the official e-identities (as designated by the Institute) of all individuals utilizing IT resources.

1.3 To enforce accountability among all Institute users in complying with the protocols outlined in this Policy document and any associated regulations.

2. Applicability:

The institute's IT/ICT resources are designated solely for teaching, learning, and research purposes by users. It is the users' responsibility to utilize and safeguard institutional IT resources appropriately while respecting the rights of others. This policy serves as a guideline for promoting safer and legitimate usage of available IT resources and infrastructure.

3. Policy Statement:

The institute's IT/ICT resources are exclusively intended for users to engage in teaching, learning, and research activities. Users are responsible for the proper utilization and protection of institutional IT resources while honoring the rights of others. This policy serves as a framework for ensuring the safe and ethical use of available IT resources and infrastructure.

4. IT Policy – Vision and Mission

- **Vision:**

  The vision of the Information Technology (IT) Policy at our Institute is to establish a digitally- driven, cutting-edge, and technologically advanced environment that empowers students, faculty, and staff to excel in the rapidly evolving business landscape. We aspire to berecognized as a pioneering business school that leverages IT to deliver innovative and immersive learning experiences, fosters research and entrepreneurship, and ensures efficient administrative processes.

- **Mission:**

  The mission of our IT Policy is to create a seamless integration of technology across all facetsof our Institute's operations. We are committed to providing state-of-the-art IT infrastructure, tools, and support that enable our students to develop essential digital skills, our faculty to deliver transformative education, and our administrative staff to streamline processes for enhanced efficiency. Upholding the highest standards of data security, privacy, and ethical IT practices is fundamental to our mission.

5. Areas:

- **IT Usage and Prohibitions**

  - Users of the institute are expected to utilize campus collaboration systems, internet services, wireless resources, official websites (such as the institute website, conference websites, journal portals, online admission systems, and course websites), as well as Management Information Systems (MIS) and ERP solutions, Learning Management System, Remote Login based facilities, and e-Library resources.

  - Emphasis shall be placed on ensuring that users adhere to institute policies and legal obligations, including licenses and contracts.

- **Prohibited Use:**

  Users are strictly prohibited from sending, viewing, or downloading fraudulent, harassing, obscene, threatening, or any other messages or materials that contravene applicable laws or institute policies. Contributing to the creation of a hostile academic or work environment is strictly forbidden.

- **Copyrights and Licenses**:

  Users are obligated to respect copyright laws and adhere to licenses pertaining to copyrighted materials. Engaging in unlawful file sharing utilizing the institute's information resources is a violation of this policy.

- **Social Media:**

  Users are expected to adhere to the institute's regulations concerning the use of social networking sites, mailing lists, news rooms, chat rooms, and blogs.

- **Commercial Use:**

  The institute's IT resources are not to be utilized for commercial or promotional purposes, including advertisements, solicitations, or any other forms of message dissemination, unless permitted under institute regulations.

6. Security and Integrity:

- **Personal Use:**

  Institute IT resources should not be utilized for activities that undermine the fundamental functionality and mission of the institute, except incidentally.

- **Unauthorized Access**:

  Users must abstain from unauthorized access to information to ensure secure access to the network and computers.

- **System Administrator Access:**

  Competent system administrators may access information resources for legitimate purposes.

- **Firewall:**

  Additional measures to maintain secure internet and intranet traffic flow within the campus shall be implemented through the utilization of Unified Threat Management (firewall).

- **Anti-virus and Security Updates:**

  Regular updates to the anti-virus policy and security measures must be conducted to safeguard computing resources.

7. Operating Aspects:

- The institute will strive to ensure the fair implementation of this policy to align with the objectives of its establishment. The management of operational aspects of IT resources will be handled in accordance with the hierarchical flow of the institute governance structure.

- The respective Heads of the Institutions hold responsibility for ensuring compliance with all institute policies concerning the use and ownership of information resources, while considering the Vision and Mission of the Institute.

- At the institute level, the Website & Technical Committee will oversee various activities related to adherence to the IT Policy in collaboration with the IT

Administrator of the respective institute.

- Individual Users are solely accountable for the activities they undertake on Institute/Institute servers using their "User Name/Password" pairs and assigned IP (Internet Protocol) addresses.

8. IT Asset Management:

8.1 Asset Management: The Institute shall establish business processes for the management of hardware and software assets to facilitate the usage of IT resources effectively. This includes procedures for procurement, deployment, maintenance, utilization, energy audit, and disposal of software and hardware applications.

8.2 Copying and Distribution: The Institute will ensure compliance with copyright laws and licensing agreements to prevent unauthorized copying and distribution of proprietary and licensed software.

8.3 Risk Management: Emphasis will be placed on managing risks associated with IT resource usage. This involves standard procedures for identifying, minimizing, and monitoring risk impact through protective and corrective measures. Additionally, procedures for timely data backup, replication, and restoration policies, power backups, audit policies, and alternate internet connectivity will be implemented for fail-safe operations.

8.4 Open Source Asset: The Institute will promote and encourage the effective usage of open-source software solutions.

9. IT Hardware Installation Policy:

The institute network user community is advised to observe precautions during computer or peripheral installations to minimize service interruptions due to hardware failures.

A. Primary User Definition: An individual primarily using the computer in their room is considered the "primary" user. In cases of multiple users, the department head will designate a responsible person for compliance.

B. End User Computer Systems: Besides client PCs, servers not directly administered by the internet unit are considered end-user computers. Responsibility for end-user compliance falls on the department if no primary user is identified.

C. Warranty & Maintenance: Computers should preferably come with a 3-year comprehensive warranty and be under an annual maintenance contract after the warranty period. Maintenance should include OS reinstallation and virus checks.

D. Network Cable Connection: When connecting computers to the network, ensure network cables are kept away from electrical/electronic equipment to avoid interference. Computers and peripherals should not share power supplies with other electrical/electronic equipment.

E. Noncompliance: Non-compliance with this policy may lead to network-related problems and productivity loss. Individuals failing to comply may face disciplinary action.

10. Software Installation and Licensing Policy:

All computer systems purchased by departments/projects should have licensed software installed, including operating systems, antivirus software, and necessary applications.

Unauthorized software installation is prohibited, and individuals/departments will be held responsible for any pirated software installed on computers connected to the institute network.

A. Operating System Updates: Users are responsible for keeping their OS updated with service packs/patches. Open-source software adoption is encouraged whenever possible.

B. Data Backups: Regular data backups are essential to protect against data loss from virus infections or other issues. Users are encouraged to partition hard drives for data protection and utilize external storage devices for backups.

C. Noncompliance: Failure to comply with this policy may result in virus infections, data loss, and other adverse effects on individuals and the institute. Non-compliant computers must be brought into compliance promptly.

11. Violation of Policy:

Any violation of the IT Policy shall be considered misconduct or gross misconduct under Institute Rules and may result in penalties or punitive actions if necessary.

12.Implementation of Policy:

The Institute will establish necessary rules for the implementation of the IT policy as required.