

IT POLICY



MOUNT ZION COLLEGE OF ENGINEERING AND TECHNOLOGY

Lena Vilakku, Pudukkottai Dt. - 622507, Tamil Nadu.

Ph.: 96591 73000, 73733 44444

Website: www.mzcet.in, Email: info@mzcet.in

Vision & Mission

Vision

- To be the preferred choice of students who aspire to become Engineers of the highest calibre.

Mission

- Provide world-class physical and digital infrastructure and learning environment.
- Develop the competencies of students to make them job-ready and entrepreneurs.
- Facilitate mental, physical, emotional and spiritual development of students and ensure their holistic development.
- Preserve the environment through the implementation of eco-friendly and sustainable practices.
- Serve the community through skill development and other need-based services.
- Establish sustainable partnerships with industries and R&D laboratories for mutual benefit.

1.INTRODUCTION

Access to Institution IT facilities is a privilege that everyone should be an authorized member to act reasonably and protect users from abuse and exploitation. Therefore, the community and each user have a role in adhering to acceptable usage standards.

2.OBJECTIVES

The objectives of the IT policy are as follows:

- To provide all necessary computer facilities as per the academic program established by AICTE. Also, introduce new computer technology that will benefit students and staff.
- To have an effective annual plan for introducing new technologies.
- To make arrangements for early product development.
- To plan for annual maintenance expenses to ensure maximum utility of the product.
- To plan and budget for redundancy at all levels.
- To ensure that products are updated and provided 24/7 on campus or based on policies established by institution management.

3.DESCRPTION OF POLICY

As IT users know, all educational institutions worldwide, have implemented IT standards in their institutions. Without solid management policies, IT security systems will not be effective and will not necessarily align with management goals and aspirations. Due to the changing nature of information technology, information security in general and policies that govern the information security process are also dynamic. They should be constantly reviewed and modified to reflect the ever-changing technology, the changing needs of computer operators, and the operating system. A written computing policy for educational purposes that is accurate and clear for using various computing facilities is in practice for students, Faculty, staff, management, visitors, and members.

A Systems Administrator manages the Institution's intranet and internet services. The system runs security, DHCP, DNS, mail, web servers and applications and manages the corporate network. The IT policy applies to the use of equipments from central administrative services such as libraries, computer laboratories, hostels, guest houses wherever the network facilities are provided.

3.1 IT Hardware Installation Policy

Users of the institute network must exercise caution when accessing the computers or peripherals are installed so that they can face minimal inconvenience due to service interruption when there is hardware failure. A comprehensive three-year on-site warranty should cover computers of every department/cell purchased. When the warranty expires, the computer should be maintained by the system admin or external service. Maintenance should also include reinstalling the operating system and checking for virus-related issues.

3.2 Software Installation and Licensing Policy

The Members of the concerned authority will verify the computer system and all licenced software (operating system, anti-virus software) are installed properly whenever any computer purchase is made by respective departments/cells. In compliance with the country's anti-piracy laws, the IT policy of the Institute does not allow any pirated/unauthorized software installation on institute computers connected to the Institution's campus network. In such cases, the Institution will hold the department/individual responsible for any pirated software installed on computers in their departments/rooms.

Computers used in the Institute should have anti-virus software installed and be always active. The primary computer user is responsible for keeping the computer system compliant with this virus protection policy.

The Institute's IT standards govern network connections provided through network access connections or Wi-Fi. It is managed by the system admin's ongoing maintenance and support of the network, excluding local applications. Problems within the Institute's network must be reported to the system admin through <http://mzcet.in/helpdesk>.

The Institution's network and computer facilities should not be used for personal or commercial purposes. The system admin will monitor network traffic for security and performance purposes.

In wireless area networks, the rule applies, in general, to the local wireless network of the department or hostel. In addition to the requirements of this law, the department or hostel must register each wireless access point with a computer centre, including a contact point departments or hostels should not operate with unrestricted access to wireless LANs. Access to the network will be limited by inspection or MAC/IP address restrictions. Passwords and data should be encrypted.

3.3 Email Account Use Policy

Increasing the circulation is essential to all departments, users and students, and administrators of the Institute. It is recommended to use email service for the Institute's communication, academics, and other staff. All the official announcements from the Institute are communicated to Faculty, staff and students through e-mail.

3.4 Web Site Hosting Policy

Official Pages of the Departments, Cells, and central facilities may have pages on the mzcet official Web Site. As on date, the system admin is responsible for maintaining the official website of the Institute, viz., <https://www.mzcet.in/default.php>.

Departments, cells, and individuals are responsible for sending updated information from time to time about their events organized to the system admin.

3.5 Institute's Database Use Policy

The Institution has its policy on creating databases and accessing information and a policy to get more quantitative data. Taken together, these policies define the way the students, staff and others operate and access and use the Institute's facilities in a fitting manner.

The requirements of this institution management information (IMS) system are as follows:

- Employee information management system through e-campus.
- Student information management system through e-campus.
- Financial information management systems.
- Library management system through e-campus.
- Document management and information retrieval process through the file server.

3.6 Security

By connecting to the network's backbone, the department is giving much importance to follow the network usage policy within the Institute's IT security policy. Any network security issues are resolved in the organization by the System Admin.

3.7 Video Surveillance Policy

The system comprises fixed-position cameras, monitors, digital video recorders, storage and public information signs.

Cameras are installed at various vital (strategic) points on the campus, especially at the entrance and exit points of our College buildings. No camera is hidden from view and is prevented from focusing on private accommodation's front or rear areas.

Sign boards are prominently placed at conspicuous places(points),viz. campus entrance, exit points etc., to inform staff, students, visitors and public mentioning that a CCTV camera is installed and all are under surveillance.

3.8 Responsibilities for Institution Infrastructure

- Responsible for the maintenance, configuration and reliable operation of computer systems, network servers, and security issue resolution.
- Administrate infrastructure, including firewalls, databases, malware protection software and other processes.
- Installing and upgrading computer components and software as and when required for enhanced functionality and integrating automation process.
- To establish and optimize wireless network infrastructure with radius server authentication and make recommendations on systems enhancements for optimizations.
- A Google workspace account has been created for all students and faculty members with the help of Google Cloud directory sync in the active directory server.
- Creating, modifying and deleting active directory user accounts, groups, computer accounts, organizational units (OUs) and other objects in the directory service database.

-
- Helping end users with issues related to their accounts or computers, such as resetting passwords or troubleshooting technical problems.
 - Maintaining the database of all users on the college campus and their respective rights and privileges within the network.
 - We are framing and implementing security policies that conform to industry best practices and align with organizational risk management objectives.
 - Creating, configuring and administering active directory domains and adding new users to existing domains.
 - Troubleshoot hardware and software errors by running diagnostics (reviewing application logs), documenting problems and resolutions, prioritizing problems, and assessing the impact of issues.
 - Provide documentation and technical specifications to IT staff for planning and implementing new or upgrades of IT infrastructures.
 - Perform or delegate regular backup operations and implement appropriate processes for data production, disaster recovery and failover procedures
 - Resolving desktop and helpdesk support efforts, ensuring all desktop applications, workstations and related equipment promptly with limited disruptions.
 - Responsible for capacity, storage plan, and database performance.

4.PERSON RESPONSIBLE

System Administrator

Mount Zion College of Engineering and Technology



MOUNT ZION COLLEGE OF ENGINEERING AND TECHNOLOGY

Lena Vilakku, Pudukkottai Dt. - 622507, Tamil Nadu.

Ph.: 96591 73000, 73733 44444

Website: www.mzcet.in, Email: info@mzcet.in