Model Institute of Engineering & Technology (Autonomous)

IT POLICY

2021-26

INTRODUCTION

MIET has network connections to every computer system covering more than Six buildings across the campus.

IT Operations (IT OP's) MIET is the department that has been given the responsibility of running the institute's intranet and Internet services.

IT OP's is running the Firewall security, DHCP, DNS, email, web and application servers and managing the network of the institute.

MIET is getting its Internet bandwidth from Reliance JIO and BSNL. Total bandwidth availability 200 Mbps (leased line 1:1).

With the extensive use of the Internet, network performance outreach in three ways:

- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.
- When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users, who are on the high-speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service and Quality of Experience. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe download, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network.

They can slow down or even bring the network to a halt. Containing a virus once it spreads through the network is not an easy job. Plenty of man- hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, IT OP's has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires.

Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

It may be noted that institute IT Policy applies to technology administered by the institute centrally or by the individual departments, to information services provided by the institute administration, or by the individual departments, or by individuals of the institute community, or by authorized resident or non-resident visitors on their own hardware connected to the institute network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the institute, wherever the network facility was provided by the institute.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the Institute's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by the institute by any institute member may even result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

- Students: UG, PG, Research
- Employees (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

Vision, Mission and Objectives

- VISION: To be globally competitive Engineering Institute destination that will strive to provide the latest Information Technological resources to all the students as a form of providing quality engineering education.

- MISSION: To place MIET amongst the most preferred Engineering Institutes when it comes to IT investment & Implementations through strategic planning combined with developing a globally competitive and sustainable IT Resource Campus environment, thereby making MIET as one of the most favored IT enabled Institutions.

- OBJECTIVES:

    - To provide all required IT resources as per the academic programs laid down by AICTE. Also, introduce new IT technologies which will benefit the students and research staff.
    - To effectively have an annual plan of introducing new technologies in-line with the Academia.
    - Create provision for priority up-gradation of the products

- Create Provision for Annual Maintenance expenses to ensure maximum uptime of the products.
- Plan and invest for redundancy at all levels.
- To ensure that the products are updated and catered 24x7 in the campus or as per the policies lay down by the College Management.
- Leveraging information technology as a tool for the socio-economic development of the Institute.

IT Hardware Installation Policy

Institute network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

- Primary User

An individual in whose room the computer is installed and is primarily used by him/her is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should arrange and make a person responsible for compliance.

- End User Computer Systems

Apart from the client PCs used by the users, the institute will consider servers not directly administered by Computer Center, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the Computer Center, are still considered under this policy as "end- users" computers.

- Warranty & Annual Maintenance Contract

Computers purchased by any Department/Cells should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by Computer Center or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

- Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

- Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

- File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

- Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the institute centrally and distributed by the Computer Center will attend the complaints related to any maintenance related problems.

- Noncompliance

MIET faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non- compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/cells should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, Institute IT policy does not allow any pirated/unauthorized software installation on the institute owned computers and the computers connected to the institute campus network. In case of any such instances, institute will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

- Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them.

- Antivirus Software and its updating

Computer systems used in the institute should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from Computer Center.

- Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned into many volumes typically C, D and so on. OS and other software should be on C drive and user’s data files on the other drives (e.g. D, E). In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data on CD / DVD or other storage devices such as pen drives, external hard drives.

- Noncompliance

MIET faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons.

An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

- IT OP’s Interface

IT Operations team upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The Computer Center will provide guidance as needed for the individual to gain compliance.

Network (Intranet & Internet) Use Policy

Network connectivity provided through an authenticated network access connection or Wi- Fi is governed under the Institute IT Policy. The IT Operations Team (IT OP's) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to IT OP's.

- IP Address Allocation

Any computer (PC/Server/Lapto/mobile) that will be connected to the institute network will have an IP address assigned by the MIET DHCP Servers. The range of IP addresses that will be allocated to each user is mapped to their VLAN Id's.
So, any user connected to the network from a specific VLAN will be allocated IP address only from that Address pool.

As and when a new computer is installed in any location, the concerned user has to take IP address allocation from Computer Center.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports.

- DHCP and Proxy Configuration by Individual Departments /Cells/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the institute. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by Computer Center.

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

- Running Network Services on the Servers

Individual departments/individuals connecting to the institute network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Center in writing and after meeting the requirements of the institute IT policy for running such services. Non- compliance with this policy is a direct violation of the institute IT policy, and will result in termination of their connection to the Network.

IT Operations team takes no responsibility for the content of machines connected to the Network, regardless of those machines being Institute or personal property.

IT Operations team will be constrained to disconnect client machines where potentially damaging software is found to exist.

A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Institute network and computer resources are not to be used for personal /commercial purposes.

Network traffic will be monitored for security and for performance reasons at Computer Center.

Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

- Dial-up/Broadband Connections

Computer systems that are part of the Institute’s campus-wide network, whether institute’s property or personal property, should not be used for dial-up/broadband connections, as it violates the institute’s security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

- Wireless Local Area Networks

This policy applies, in its entirety, department, or campus wireless local area networks. In addition to the requirements of this policy, faculty and students must get themselves registered in order to receive Wi-Fi login credentials (user id and passwords). Each user Wi-Fi internet is monitored and secured with well-defined policies and rules for safe and secure internet access.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and other stake holders, it is recommended to utilize the institute's e-mail services, for formal Institute communication and for academic & other official purposes.

Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://gmail.com with their User ID and password. Email id's and passwords will be created for the faculty and students by the IT Cell and delivered through well-defined interface.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender

about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have potential to damage the valuable information on your computer.

- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.

The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the institute's campus network, or by using the resources provided by the institute to the individual for official use even from outside.

Institute Database Use Policy

This Policy relates to the databases maintained by the institute.

Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential.

MIET has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the institute's approach to both the access and use of this institute resource.

- Database Ownership:

  MIET is the data owner of the entire Institute's institutional data generated in the institute.

- Data Administrators:

  Data administration activities outlined may be delegated to some of the officers in that department.

- MIS Components:

  For the purpose of Management Information System requirements of the institute these are:

  - Employee Information Management System.
  - Students Information Management System.
  - Financial Information Management System.
  - Library Management System.
  - Document Management & Information Retrieval System.

Here are some general policy guidelines and parameters for departments, cells and administrative department data users:

1. The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.
2. Data from the Institute’s Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.
3. One’s role and function define the data resources that will be needed to carry out one’s official responsibilities/rights. Through its data access policies, the institute makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be

distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.

5. Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.
6. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:
   - Modifying/deleting the data items or software components by using illegal access methods.
   - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
   - Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
   - Trying to break security of the Database servers.

Such data tampering actions by institute member or outside members will result in disciplinary action against the offender by the institute authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

Wi-Fi Use Policy

- Usage of Wireless infrastructure in the MIET classrooms, library and campus is to enhance the accessibility of internet for academic purposes and to browse exclusive online resource (licensed online journals) of MIET for student's/faculty members and staffs.

- Availability of the signal will vary from place to place. The signal strength also may vary from location to location. It is not mandatory that each and every area in each floor of every block will have the same kind of signal strength, coverage and throughput.

- Access to Wireless internet is only an extended service. Availability of wireless services solely depends on the discretion of the MIET and it has rights to stop/interrupt the services at any given point of time, if required for any technical purpose.

- The access points provided in the classrooms, library and the campus are the property of MIET and any damage or loss of the equipment will be considered as a serious breach of MIET's code of conduct and disciplinary action will be initiated on the student/s who are found guilty for the loss or damage of the Wireless Infrastructure or the corresponding equipment in the campus.

Video Surveillance Policy

The system comprises: Fixed position cameras; Monitors; digital video recorders; Storage; Public information signs.

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

The system has been installed by institute with the primary purpose of reducing the threat of crime generally, protecting institutes premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

It is recognized that members of institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Computer Center.

CCTV footage provided by the institute (Computer Center) upon receiving the requests from the individuals on prescribed proforma.

Responsibilities of IT Operations Team

- Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by IT OP's.
2. IT OP's operates the campus network backbone such that service levels are maintained as required by the Institute Departments, and labs served by the campus network backbone within the constraints of operational best practices.

   - Maintenance of Computer Hardware & Peripherals

     IT OP's is responsible for maintenance of the institute owned computer systems and peripherals that are under warranty or out of the warranty.

   - Receiving Complaints

     IT Cell MIET may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them is having any problems.

     The designated person in IT Cell receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems (which are in warranty) to resolve the problem within a reasonable time limit. For out of warranty computer systems, problems resolved at computer center.

     IT Cell may receive complaints from department/users, if any of the networks related problems are noticed by them such complaints should be made by email/phone.

     IT Cell may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call.

     The designated person in IT Cell receives complaints from the users and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

   - Scope of Service

     IT Cell will be responsible for solving the hardware related problems or OS or any other application software that were legally purchased by the institute and was loaded by the company as well as network related problems or services related to the network.

- Installation of Un-authorized Software

  IT Cell or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

- Physical Demarcation of Campus Buildings' Network

  1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of IT Cell MIET.
  2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of IT Cell team. It essentially means exactly at which location the fiber optic-based backbone terminates in the buildings will be decided by the IT team. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of IT team.
  3. IT Cell team will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
  4. It is not the policy of the Institute to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the Institute's Internet links.

- Network Expansion

  Major network expansion is also the responsibility of IT Cell team. Every 3 to 5 years, Computer Center reviews the existing networking facilities, and need for possible expansion.

- Wireless Local Area Networks

  1. Where access through Fiber Optic/UTP cables is not feasible, in such locations IT Cell team considers providing network connection through wireless connectivity.
  2. IT Cell team is authorized to consider the applications of Departments, or divisions for the use of radio spectrum from Computer Center prior to implementation of wireless local area networks.
  3. IT Cell team is authorized to restrict network access to the Cells, departments, or hostels through wireless local area networks either via authentication or MAC/IP address restrictions.

- Electronic logs

  Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

- Global Naming & IP Addressing

  IT Cell team is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. IT OP's team monitors the network to ensure that such services are used properly.

- Providing Net Access IDs and email Accounts

  IT Cell team provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the institute upon receiving the requests from the individuals on prescribed proforma.

- Disconnect Authorization

  IT Cell team will be constrained to disconnect any Department, or cell, hostel from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Department, or cell, hostel machine or network, Computer Center endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Department or division is disconnected, Computer Center provides the conditions that must be met to be reconnected.

Responsibilities of Department

- User Account

  Any Centre, department, or cell or other entity can connect to the Institute network using a legitimate user account (Net Access / Captive Portal ID) for the purposes of verification of affiliation with the institute. The user account will be provided by Computer Center, upon filling up the prescribed application form and submitting it to Computer Center.

  Once a user account is allocated for accessing the institute's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the institute for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID to prevent un-authorized use of their user account by others.

  It is the duty of the user to know the IT policy of the institute and follow the guidelines to make proper use of the institute's technology and information resources.

- Supply of Information by Department, or Cell for Publishing on /updating the MIET Web Site

  All Departments or Cells should provide updated information concerning them periodically (at least once in a month or earlier).

  Hardcopy or softcopy to be sent to the IT Cell. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Department, or Cells.

  Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the IT cell upon receiving the written requests. If such web pages have to be directly added into the official web site of the institute, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the In Charge, Computer Center well in advance.

- Security

  In connecting to the network backbone, department agrees to abide by this Network Usage Policy under the Institute IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact (POC) in the originating department. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

- Preservation of Network Equipment and Accessories

  Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the institute are the property of the institute and are maintained by Computer Center and respective departments.

  Tampering of these items by the department or individual user comes under violation of IT policy.

- Additions to the Existing Network

  Any addition to the existing network done by department or individual user should strictly adhere to the institute network policy and with prior permission from the competent authority and information to Computer Center.

  Institute Network policy requires following procedures to be followed for any network expansions:

  1. All the internal network cabling should be as on date of CAT 6 UTP.
  2. UTP cabling should follow structured cabling standards. No loose and dangling UTP cables are drawn to connect to the network.
  3. UTP cables should be properly terminated at both ends following the structured cabling standards.
  4. Only managed switches should be used. Such management module should be web enabled. Managed switches give the facility of managing them through web so that Computer Center can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

5. As managed switches require IP address allocation, the same can be obtained from Computer Center on request.

- Campus Network Services Use Agreement

  The "Campus Network Services Use Agreement" should be read by all members of the institute who seek network access through the institute campus network backbone. This can be found on the institute web site. All provisions of this policy are considered to be a part of the Agreement. Any Department or individual, who is using the campus network facility, is considered to be accepting the institute IT policy. It is user's responsibility to be aware of the Institute IT policy. Ignorance of existence of institute IT policy is not an excuse for any user's infractions.

- Enforcement

  Computer Center periodically scans the Institute network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

Responsibilities of the Administrative Department

IT Cell needs latest information from the different Administrative Department for providing network and other IT facilities to the new members of the institute and for withdrawal of these facilities from those who are leaving the institute, and also for keeping the MIET web site up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- Information about New Appointments.
- Information about Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Information on Important Events/ Achievements.
- Information on different Rules, Procedures, and Facilities.

Guidelines for Those Running Application or Information Servers

Departments may run an application or information server. They are responsible for maintaining their own servers.

- Obtain an IP address from Computer Center to be used on the server.
- Get the hostname of the server entered in the DNS server for IP Address resolution.
- Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.
- Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.
- Operating System and the other security software should be periodically updated.

Guidelines for Desktop Users

These guidelines are meant for all members of the MIET Network User.

Due to the increase in hacker activity on campus, Institute IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1) All desktop computers should have the latest version of antivirus. And should retain the setting that schedules regular updates of virus definitions from the central server.

2) When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.

3) The password should be difficult to break.

4) The guest account should be disabled.

5) In addition to the above suggestions, Computer Center recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

Web Application Filter

Application	Management	Staff	Student	Guest
Captive portal Session	2 concurrent sessions / user			
Sites Blocked	Porn, torrents, Proxy & Hacking, Gambling, Marijuana, Criminal Activity			
YouTube	Allow	Time based	Time based	Block
YouTube Educational	Mandatory Certificate needs to be purchased			
What's App	Allow	Block	Block	Block
Facebook	Allow	Block	Block	Block
Skype or Video calling	Allow	Allow	Time based	Allow
Entertainment	Allow	Block	Block	Block
TV news Channel	Allow	Allow	Time based	Allow
Online Games	Deny	Deny	Deny	Deny
Windows Update	Allow	Allow	Allow	Allow

Default Block Category in Firewall:

- Weapon
- Phishing and fraud
- Militancy and Extremist
- Gambling
- Pro-Suicide and self-Harm
- Criminal Activity
- Marijuana
- Intellectual Piracy
- Hunting and Fishing
- Legal highs
- Controlled substances
- Anonymizers
- Sexually Explicit
- Nudity
- Advertisement

Appendix I

Campus Network Services Use Agreement

Read the following important policies before applying for the user account/email account. By signing the application form for Net Access ID (user account)/email account, you agree to act in accordance with the IT policies and guidelines of MIET. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of the institute. User can have a copy of the detailed document from the website & various intranet servers. A Net Access ID is the combination of a username and a password whereby you gain access to Institute computer systems, services, campus networks, and the internet.

- Accounts and Passwords

  The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the Institute.

  Students, staff and faculty who leave the Institute will have their Net Access ID, email id and associated files deleted.

  No User will be allowed more than one Net Access ID at a time, with the exception that faculty or heads that hold more than one portfolio are entitled to have Net Access ID related to the functions of that portfolio.

- Limitations on the use of resources

  On behalf of the Institute, IT cell reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

- Data Backup, Security, and Disclaimer

  IT cell will not be liable for the loss or corruption of data on the individual user’s computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of Computer Center staff member in the process of helping the user in resolving their network/computer related problems. Although Computer Center make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, Computer Center makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold IT cell, as part of MIET, harmless for any such liability or expenses. MIET retains the right to change and update these policies as required without notification to the User.

- Account Termination and Appeal Process

Accounts on MIET network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources.

If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may approach the In Charge, Computer Center, justifying why this action is not warranted.

Appendix II

Model Institute of Engineering and Technology, Kot Bhalwal

IT Cell MIET

Requisition Form for E-Mail Account

1. Full Name: ____

   (First Name) (Middle Name) (Last Name)

2. Designation: ____
3. Department: ____
4. Mobile No: ____
5. Existing Mail Id : _______________________________________

Date: Signature of Applicant: ………………………………

……………IT Cell Use only……………

The following email ID is created for Prof. /Dr. /Mr. /Ms.

____on *@mietjammu.in*

Signature on Behalf of In Charge,IT Cell

Appendix III

Model Institute of Engineering and Technology, Kot Bhalwal

IT Cell MIET

Application for Net Access ID Activation

1. Full Name : ____

   (First Name) (Middle Name) (Last Name)

2. Employee Id : ____
3. Department : ____
4. Mobile No: ____
5. Email Mail Id : ____________________________________

Date: Signature of Applicant: …………………………………

……………Computer Center Use only……………

Net access ID is activated for the applicant.

Signature on Behalf of In Charge,
IT Cell MIET

Appendix IV

Model Institute of Engineering and Technology, Kot Bhalwal

IT Cell MIET

Requisition for CCTV Footage

1. Name of Applicant: ____
2. Employee / Student Id: ______________________________________
3. Department: ______________________________________
4. Mobile No: ______________________________________
5. Email Mail Id: ____________________________________
6. Date of Footage:______________________Time: From________To______
7. Camera Location: ____________________________________
8. Description: ______________________________________

Date: ………………………………… Signature of Applicant:

……………Computer Center Use only……………

CCTV Footage is given to Applicant.

Signature on Behalf of In Charge,Computer Center

Director
Model Institute of
Engineering & Technology
JAMMU-181122