



IT POLICY & GUIDELINES

Centre of Information and Technology Management (CITM)

Thapar Institute of Engineering & Technology



Centre of Information and Technology Management-CITM
Thapar Institute of Engineering & Technology
P.O. Box 32, Bhadson Road,
Patiala -147004,
Punjab, India

Point No	Table of Contents	Page No
1	Abbreviation	2
2	Introduction	3
3	Scope	4
4	Objective	4
5	Roles and Responsibilities	4
6	Acceptable Use	5
7	Privacy and Personal Rights	6
8	Privacy In Email	6
9	User Compliance	6
10	Access To The Network	6
10.1	Access To Internet And Intranet	6
10.2	Access To TIET'S Wireless Networks	7
10.3	Filtering and Blocking of Sites:	7
11	Monitoring and Privacy	7
12	E-Mail Access From The Institute Network	7
13	Access to Social Media Sites from TIET Network	7
14	Use of It Devices Issued by TIET	8
15	Security Incident Management Process	8
16	Intellectual Property	8
17	Enforcement	9
18	Deactivation	9
19	Audit of TIET Network Infrastructure	9
20	Review	9
21	IT Hardware Installation Policy	9
22	Software Installation and Licensing Policy	10
23	Use of IT Devices on TIET Network	11
23.1	Desktop Devices	11
23.2	Sharing of Data	12
23.3	Use of Portable Devices	12
24	Network (Intranet & Internet) Use Policy	13
25	Email Account Usage Policy	15
25.1	Guidelines for Sending/Forwarding Information to Email Groups	17
25.2	Beware/Careful From Email Phishing Attacks	17
26	Disposal of ICT Equipment	19
27	TIET E-Ticket Support System	19
28	Breach of This Policy	20
29	Revisions To Policy	21
30	Contact Us	21
	Appendix – I: Request For Creation Of Sophos Id, WebKiosk Id, Email	22
	Appendix – II: Requisition Performa To Resolve Internet Connectivity Problems	23
	Appendix – III: Requisition Performa for repair of equipment	24
	Appendix – IV: Requisition Performa to Delete an Article from TURNITIN Repository	25
	Appendix – V: Requisition Performa to Video Conferencing	26

1. ABBREVIATION

Sr. No.	Abbreviation	Description
1.	TIET	Thapar Institute of Engineering and Technology
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
14.	CITM	Centre of Information and Technology Management

2. INTRODUCTION

Thapar Institute of Engineering and Technology (TIET) provides IT resources to support the educational, instructional, research, and administrative activities of the Institute and enhance the employees' efficiency and productivity. These resources are meant to access and process information related to their work areas. These resources help them to remain well informed and carry out their functions efficiently and effectively. Centre of Information and Technology Management (CITM) of Thapar institute is cater the needs of users involving implementation, maintenance and support activities related to LAN/WLAN, software and hardware; procurement, support and maintenance of various equipment's of users. CITM of Thapar institute offers Internet access and network services to Thapar Institute.

CITM of Thapar institute also provides repair and maintenance of Electronic Instruments/Equipment and PCs and peripherals used in various Laboratories. CITM contributes to implementing LMS and ERP software that includes financial management, inventory management, human resource management, purchase management, academic activities modules, and its related support to the users of Thapar Institute. The main objective of Centre is to provide better support and services to the users for their individual and collective growth.

This document establishes specific requirements for using all IT resources at TIET. This policy applies to all users of computing resources owned or managed by TIET. Individuals covered by the policy include (but are not limited to) TIET faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, affiliated colleges and any other entity which fall under the management of Thapar Institute of Engineering and Technology accessing network services via TIET's computing facilities.

For the purpose of this policy, the term 'IT Resources' includes all Institute owned, licensed, or managed hardware and software, and use of the Institute network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risk and liabilities for the Institute. It is, therefore, expected that these resources are used primarily for Institute related purposes and lawfully and ethically.

3. SCOPE

This policy governs the usage of IT Resources from an end user's perspective. This policy applies to all individuals/ users/ entities, as defined in Section 2, who use the IT Resources of TIET.

4. OBJECTIVE

The objective of this policy is to ensure proper access to and usage of TIET's IT resources and prevent their misuse by the users. Use of resources provided by TIET implies the user's agreement to be governed by this policy.

1. TIET IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the Institute on the campus.
2. This policy establishes Institute-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the Institute.
3. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, documents and verbally communicated information.

5. ROLES AND RESPONSIBILITIES

The following roles and responsibilities are envisaged from each entity respectively.

- 1) TIET shall implement appropriate controls to ensure compliance with this policy by its users. CITM shall be the primary Implementing Agency and shall provide necessary support in this regard.
- 2) CITM shall ensure the resolution of all incidents related to the security aspects of this policy by its users. Implementing Agency shall provide the requisite support in this regard.
- 3) Use TIET's IT resources for those activities that are consistent with the academic, research and public service mission of the Institute and are not "Prohibited Activities".
- 4) All users shall comply with existing national, state and other applicable laws.
- 5) Abide by existing telecommunications and networking laws and regulations.
- 6) Follow copyright laws regarding protected commercial software or intellectual property.
- 7) As a member of the Institute community, TIET provides the use of scholarly and/or work-related tools, including access to the Library, particular computer systems, servers, software and databases and the Internet. It is expected from

Institute Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of non-electronic communication.

- 8) Users of TIET shall not install any network/security device on the network without consultation with the CITM.
- 9) It is responsibility of the Institute Community to know the regulations and policies of the Institute that apply to the appropriate use of the Institute's technologies and resources. Institute Community is responsible for exercising good judgment in the use of the Institute's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
- 10) As a representative of the TIET community, each individual is expected to respect and uphold the Institute's good name and reputation in any activities related to use of ICT communications within and outside the Institute.
- 11) Competent Authority of TIET should ensure proper dissemination of this policy.

6. ACCEPTABLE USE

1. An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.
2. A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the Institute for all use of such resources. As an authorized TIET user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of TIET or a personal computer that is connected to the TIET campus wide Local Area Network (LAN).
3. The Institute is bound by its End User License Agreement (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.
4. Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
5. No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
6. Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.

7. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

7. PRIVACY AND PERSONAL RIGHTS

- 1) All users of the Institute's IT resources are expected to respect the privacy and personal rights of others.
- 2) Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
- 3) While the Institute does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

8. PRIVACY IN EMAIL

While every effort is made to ensure the privacy of TIET email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct Institute business, there may be instances when the Institute, based on approval from competent authority, reserves and retains the right to access and inspect stored information with the consent of the user.

9. USER COMPLIANCE

When an individual uses TIET's IT resources, and accepts any Institute issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of TIET and adapt to those changes as necessary from time to time.

10. ACCESS TO THE NETWORK

10.1. Access to Internet and Intranet

- 1) A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the Institute Campus wide LAN.
- 2) TIET maintains two independent networks, i.e. Internet and Intranet. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.
- 3) Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

10.2. Access to TIET's Wireless Networks

For connecting to a TIET's wireless network, user shall ensure the following:

- 1) A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the TIET's wireless network.
- 2) Wireless client systems and wireless devices shall not be allowed to connect to the TIET's wireless access points without due authentication.

10.3. Filtering and blocking of sites:

- 1) CITM may block/filter content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
- 2) CITM may also block content that, in the opinion of the Institute, is inappropriate or may adversely affect the productivity of the users.

11. MONITORING AND PRIVACY

- 1) CITM shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.
- 2) For security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on Institute provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
- 3) CITM may monitor user's online activities on Institute network.

12. E-MAIL ACCESS FROM THE INSTITUTE NETWORK

- 1) E-mail service authorized by TIET and implemented by the CITM shall only be used for all official correspondence.
- 2) More details are provided in the "E-mail Account Usage Policy of TIET".

13. ACCESS TO SOCIAL MEDIA SITES FROM TIET NETWORK

1. Use of social networking sites by TIET users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".
2. User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.

3. User shall adhere to the “Terms of Use” of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
4. User shall report any suspicious incident as soon as possible to the competent authority.
5. User shall always use high-security settings on social networking sites.
6. User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
7. User shall not disclose or use any confidential information obtained in their capacity as an employee of the Institute.
8. User shall not make any comment or post any material that might otherwise cause damage to TIET’s reputation.

14. USE OF IT DEVICES ISSUED BY TIET

IT devices issued by the TIET to a user shall be primarily used for academic, research and any other Institute related purposes and in a lawful and ethical way and shall be governed by the practices defined in the Section “Use of IT Devices on TIET Network”. The aforesaid section covers best practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

15. SECURITY INCIDENT MANAGEMENT PROCESS

1. A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Institute’s data.
2. CITM reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the Institute.
3. Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) or CITM.
4. Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.
5. IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

16. INTELLECTUAL PROPERTY

Material accessible through the TIET’s network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use TIET’s network and

resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

17. ENFORCEMENT

1. This policy is applicable to all the users of TIET as specified in Section 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.
2. Each entity of TIET shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.

18. DEACTIVATION

1. In case of any threat to the security of TIET's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA or CITM.
2. Subsequent to such deactivation, the concerned user and the competent authority of the Institute shall be informed.

19. AUDIT OF TIET NETWORK INFRASTRUCTURE

The security audit of network infrastructure shall be conducted periodically by Head, CITM.

20. REVIEW

Future changes in this Policy, as deemed necessary, shall be made by Head, CITM.

21. 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.

A. Who is 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 administrator of the computer should make an arrangement and make a person responsible for compliance.

B. What are End User Computer Systems

Apart from the client PCs used by the users, the Institute will consider servers not directly administered by CITM, 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 CITM, are still considered under this policy as "end- users" computers.

C. Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty.

D. 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, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

E. Network 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.

F. 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.

G. Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the Institute maintain the computer by Repair & Maintenance Lab of CITM.

22. SOFTWARE INSTALLATION AND LICENSING POLICY

Any computer purchases made by the individual departments/projects 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.

A. Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or month.

Institute as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

B. Use of software on Desktop systems

- a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.
- b. Any software installed should be for activities of the Institute only.

C. Antivirus Software and its updating

Computer systems used in the Institute should have anti-virus software (window securities, etc) 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.

D. Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

23. USE OF IT DEVICES ON TIET NETWORK

This section provides the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on TIET's network.

23.1. Desktop Devices

1) Use and Ownership

Desktops shall normally be used only for transacting Institute's works. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

2) Security and Proprietary Information

- a. User shall take prior approval from the CITM to connect any access device to the TIET's network.
- b. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy of the application.
- c. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.
- d. Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.
- e. User shall report any loss of data or accessories to the CITM.
- f. User shall obtain authorization from the competent authority before taking any TIET issued desktop outside the premises of the Institute.
- g. Users shall properly shut down the systems before leaving the office/ department.
- h. Users shall abide by instructions or procedures as directed by the CITM from time to time.
- i. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the Repair & Maintenance Lab (CITM) for corrective action.

23.2. Sharing of data

Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

23.3. Use of Portable devices

Devices covered under this section include TIET issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices shall be governed by the following:

- a. User shall be held responsible for any unauthorized usage of their TIET issued access device by a third party.
- b. Users shall keep the TIET issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. classrooms, meeting rooms, restaurants etc.).

- c. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.
- d. CITM shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.
- e. Users shall wipe or securely delete data from the device before returning/ disposing it off.
- f. Lost, stolen, or misplaced devices shall be immediately reported to the IA/ and the competent authority.
- g. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

24. NETWORK (INTRANET & INTERNET) USE POLICY

Network connectivity provided through the Institute, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the Institute IT Policy. The CITM 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 CITM through online eticket support system <https://eticket.thapar.edu>.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the Institute network, should have an IP address assigned by the CITM. Following a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN (VLAN) created against each entity or objective. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.

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 address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

B. DHCP and Proxy Configuration by Individual Departments /Schools/Centre/Sections/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch 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 services run by the CITM.

Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

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.

C. Running Network Services on the Servers

- a. Individual Departments /Schools/Centre/Sections/ Users 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 CITM 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.
- b. CITM takes no responsibility for the content of machines connected to the Network, regardless of those machines being Institute or personal property.
- c. CITM 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.
- d. Access to remote networks using a Institute's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the Institute Network connects. Institute network and computer resources are not to be used for personal commercial purposes.
- e. Network traffic will be monitored for security and for performance reasons at CITM.
- f. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

D. Internet Bandwidth obtained by Other Departments

- a. Internet bandwidth acquired by any department of the Institute under any research programme/project should ideally be pooled with the Institute's Internet bandwidth, and be treated as Institute's common resource.
- b. Under particular circumstances, which prevent any such pooling with the Institute Internet bandwidth, such network should be totally separated from the Institute's campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.
- c. IP address scheme (private as well as public) and the Institute gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the Institute IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to CITM.
- d. Non-compliance to this policy will be direct violation of the Institute's IT security policy.

25. EMAIL ACCOUNT USAGE POLICY

TIET provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email of Thapar Institute of Engineering and Technology's domain.

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

E-mail 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 <http://gmail.com> with their User ID and password. For obtaining the Institute's email account, user may fill the form available on www.thapar.edu and sent at the

<https://eticket.thapar.edu> for email account and default password by submitting an application in a prescribed proforma.

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

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. 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.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. 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 in 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.
6. User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
7. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
8. 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.
9. Impersonating email account of others will be taken as a serious offence under the IT security policy.
10. It is ultimately each individual's responsibility to keep their e-mail account free from violations of Institute's email usage policy.
11. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.

25.1 Guidelines for Sending/Forwarding Information to Email Groups

The purpose of email groups is to circulate the academic/research circular, information and news of Thapar Institute's to faculty, employees and students. In the past few months, we have observed that the group emails defying the above-said purposes are sent by faculty and staff.

Please go through the guidelines before sending group emails to faculty, employees, students, all other UG, PG and PhD groups.

1. Any news or achievement will only be forwarded by the Head of the department/school/Centre/unit before checking and verifying the contents and claims mentioned in the email. The head of the unit may seek approval from the appropriate competent authority.
2. Any workshop/symposium or conference announcement should be forwarded by the head of the department/school/unit. The faculty can forward the email to the head with the request and name of the email groups to which it is intended to be forwarded.
3. Any circular of Hackathon or any other technical event will be forwarded by the head of the unit only to the student's groups it is meant for. The faculty having information may forward such contents to their head of the unit.
4. The student's societies can send email content relevant to their society only with the prior approval of the competent authority.
5. No groups email having buying/selling of items contents like online courses, other products etc. Please do not forward such content to students unless it has approval from the competent authority. Only the head of the unit or higher authority can forward such emails.

The sole purpose of the above guidelines is to communicate with the groups with quality, precise content of information regarding academics and research and also guard the faculty, staff and students from predatory marketing practices.

25.2 Beware/careful from eMail Phishing Attacks.

Follow the instructions to wipe out the chances of an email phishing attack that has gained momentum on the Internet.

To fight against such email phishing attacks, all students and employees need to be aware and educated of such possibility of bogus emails landing in your Inbox. The awareness is the only way to thwart such attacks.

Email phishing is an attempt to obtain sensitive data such as usernames, passwords, financial transaction or financial information by emailing someone while pretending to be a coworker, relative, friend, or business associate.

“Spear email Phishing” is a dangerous new wave of email phishing attacks. In this, criminals or attackers target specific individuals in an attempt to win his/her confidence and obtain information they can use to steal money, secret information or force you to do financial transactions. The cyber criminals will impersonate your email address, name and email signatures to gain confidence of target and write email to target in such a way that looks more authentic.

In case, you find any email asking for secret/financial information or persuade you to do a financial transaction immediately. Always keep in mind it could be an attack and check the following points to avoid such email phishing attacks:

1. Always check the “from” email field before doing anything. The “from” email addresses can sometimes also be spoofed, so always double check by clicking “reply” to see what email address appears in the “To” field. It is the actual email address from where you got the email. You do not actually need to send a reply to the attacker email. Marks this email as spam.
2. Such emails you receive looks like it is from someone you know very well. Always check it carefully for the phrasing, tone, or language used in email matches about the person you know. Generally, such emails have a strange tone and text as these are scripted in more authoritarian manner. Such contents should always trigger an alarm in your mind.

What to do next? Check the "from" email address, always double check by pressing reply and check the "To" field. Don't press the send button.

Type of contents in email phishing attacks:

Following are some texts that generally appear in such email phishing attacks. There could be many more.

Attacker Email Content 1: An employee received an email that appeared to be from his boss/reporting officer asking, “Are you available for a quick task as I am struck in some emergency?” The task involves sharing financial information and other secret information. Sometimes to commit some financial transaction on his/her behalf that he would reimburse later.

Attacker Email Content 2: An employee received an email that appeared to be from his boss asking, “You buy six amazon coupons of Rs 5000 each as in am struck in Hospital due to some disease or COVID-19?”

Attacker Email Content 3: An employee received an email supposedly from her boss asking if she was available to make a wire transfer.

What to do if you have such a message in your inbox? Firstly, don’t panic and do the action mentioned in email!!!

Check "from" email address and then press reply check "To" field. If you found any such phishing email then mark it as spam. Your email data is safe and your account is not hacked/compromised. No need to worry further.

If you are still not able to judge from “from” the email address field, you can call that known person to reconfirm the task mentioned in email. In any case do not reply to these emails and become targets of starting chain emails.

We have formed Computer Emergency Response Team (CERT-TIET) to analyze such cyber-attacks in TIET periphery and help our community in a better way. Kindly share such emails, instances with us at cert@thapar.edu with CC to Mr. Harcharan Jit Singh, Sr. Systems Analyst, CITM on his email harcharan@thapar.edu to study the intentions of an attacker in detail.

26. DISPOSAL OF ICT EQUIPMENT

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the Institute.

27. TIET E-Ticket Support System

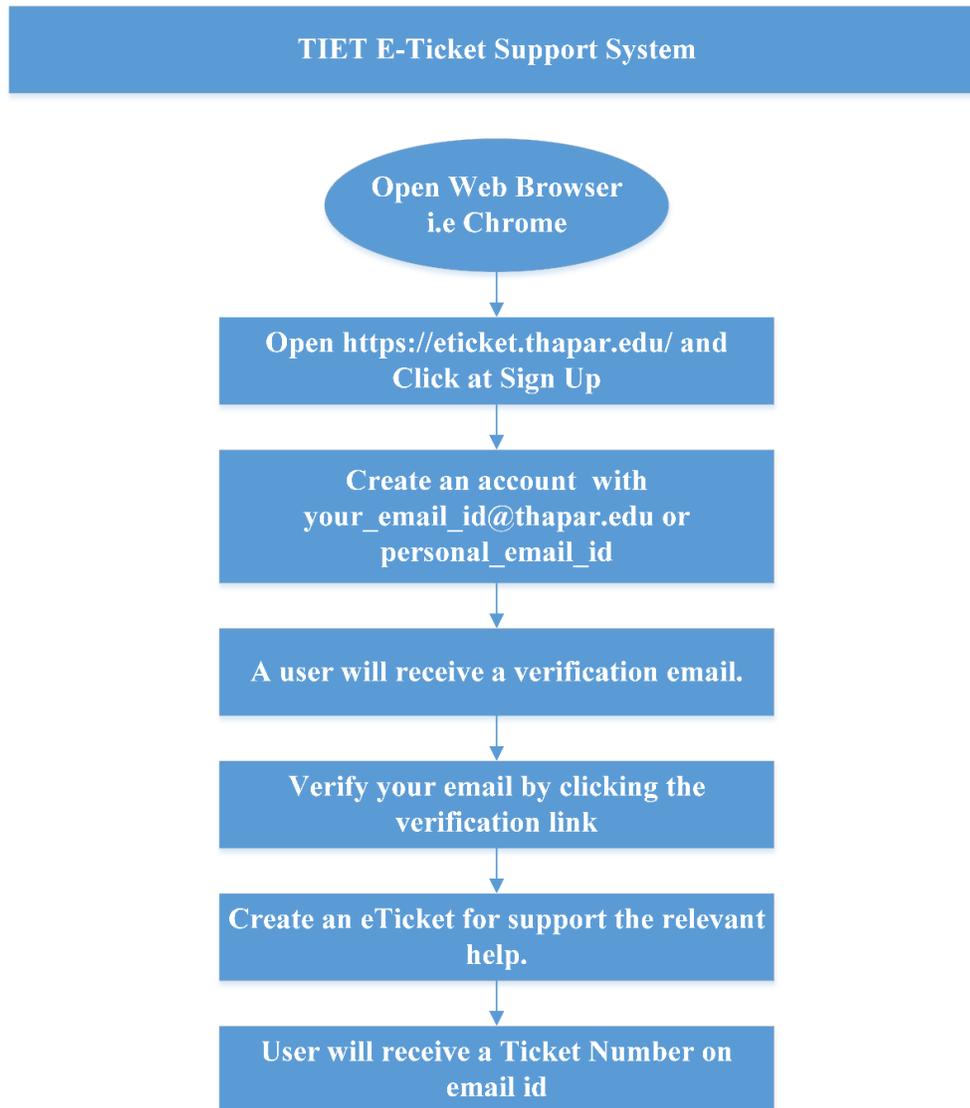
In order to streamline support requests and better serve you, TIET utilizes an e-ticket support system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference TIET e-ticket provides complete archives and history of all your support requests. A valid email address preferable @thapar.edu is required to submit a ticket. Please submit complete information like nature of support, its location, contact and mobile number to process your support request.

Easy Step to get online help/support

1. Create an account with your_email_id@thapar.edu or personal_email_id.
2. A user will receive a verification email.
3. Verify your email by clicking the verification link.
4. Create an eTicket for support under the relevant help.

Help Topic for online Support

Sr. No	Help Topic for online Support
1	Online Support Topics:
2	Creation of Email ID & WebKiosk
3	Email Support of @thapar.edu
4	Internet WiFi/ LAN Support
5	LMS Faculty Subject Support
6	LMS Student-Subject Support
7	LMS Technical Support
8	MATLAB Software Support
9	Repair of Equipment Support
10	Repair of PC-Laptop Support
11	SPSS Software Support
12	TURNITIN Article Deletion
13	WEBKOISK Reset Password

Flow Chart:**28. BREACH OF THIS POLICY**

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the harcharan@thapar.edu and cc to hcitm@thapar.edu. On receipt of notice (or where the Institute otherwise becomes aware) of any suspected breach of this Policy, the Institute reserves the right to suspend a user's access to Institute's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the Institute's disciplinary procedures.

29. REVISIONS TO POLICY

The Institute reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the TIET website.

30. CONTACT US

If you have any queries in relation to this policy, please contact:

HEAD, CITM

Email: hcitm@thapar.edu



APPENDIX – I: REQUEST FOR CREATION OF SOPHOS ID, WEBKIOSK ID, EMAIL

Thapar Institute of Engineering & Technology (Deemed to be University) Centre of Information & Technology Management	CITM/S1/4  <small>THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY (Deemed to be University)</small>								
REQUEST FOR CREATION OF SOPHOS ID, WEBKIOSK ID, EMAIL AND LINUX USER ID									
TO: HEAD, CITM									
Initiated by Name: _____ Signature: _____									
Designation: _____ Employee No / Roll No: _____									
Department/ School/Centre/Section/Unit: _____									
Present email id, if any: _____									
Mobile Number: _____									
<i>{Note: Please fill all the above fields and tick (✓) the services you are requesting for}</i>									
Sophos Account <input type="checkbox"/>	Email id @thapar.edu <input type="checkbox"/>								
Webkiosk <input type="checkbox"/>	Linux User ID <input type="checkbox"/>								
Forwarded and Recommended to HCITM									
SIGNATURE OF HEAD (Head of Department School/Centre/Section/Unit)									
To be filled by CITM	Received on dated: _____								
Sr. No. _____ Job assigned to:									
(HCITM)									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Sophos Account Name</td> <td></td> </tr> <tr> <td>Email id @thapar.edu</td> <td style="text-align: right;">@thapar.edu</td> </tr> <tr> <td>Webkiosk ID</td> <td></td> </tr> <tr> <td>Linux User ID</td> <td></td> </tr> </table>	Sophos Account Name		Email id @thapar.edu	@thapar.edu	Webkiosk ID		Linux User ID		
Sophos Account Name									
Email id @thapar.edu	@thapar.edu								
Webkiosk ID									
Linux User ID									
(System Analyst)									

Note: From June 2020, This Performa shifted to online support system at <https://eticket.thapar.edu/>. Now, Users can create an eTicket for this service with help topic “Creation of Email ID & Webkiosk”.

APPENDIX – II: REQUISITION PERFORMA TO RESOLVE INTERNET CONNECTIVITY PROBLEMS

Thapar Institute of Engineering & Technology (Deemed to be University) Centre of Information & Technology Management		CITM/IN/01  <small>THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY (Deemed to be University)</small>	
REQUISITION PERFORMA TO RESOLVE INTERNET CONNECTIVITY PROBLEM			
Sr. No.: _____ (To be filled by office of CITM)		Received on dated: _____	
Name	Designation	Department	Signature with Date
Sr. No.	Problem	Response	
1.	Internet is not working	Yes/No:	
2.	LAN port is not working	Yes/No:	
3.	Internet works sometimes	Yes/No:	
4.	Any other problem (Please give enough details)		
Location of affected user			
Mobile No			
Forwarded and Recommended to HCITM			
SIGNATURE OF HEAD (Head of Department School/Centre/Section/Unit)			
To be filled by CITM Job assigned to with date: _____			
_____ (System Analyst / HCITM)			
Problem Identified: _____			
_____ Signature(Technician/Attendant)			
Problem resolved on: _____			
Signature of User: _____			
(HCITM)			

Note: From June 2020, This Performa shifted to online support system at <https://eticket.thapar.edu/>. Now, Users can create an eTicket for this service with help topic “Internet WiFi/ LAN Support”.

APPENDIX – III: REQUISITION PERFORMA FOR REPAIR OF EQUIPMENT

Thapar Institute of Engineering & Technology (Deemed to be University) Centre of Information & Technology Management		CITM/RAM/01  <small>THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY (Deemed to be University)</small>		
REQUISITION PERFORMA FOR REPAIR OF EQUIPMENT				
Sr. No.: _____ (To be filled by office of CITM)		Received on dated: _____		
TO: HEAD, CITM				
Name	Designation	Department	Mobile No	Signature with Date
Sr. No.	Equipment	Qty	Remarks/Problem	
<i>Note: Please fill all the above fields</i>				
Budget Head: _____		SIGNATURE OF HEAD (Head of Department School/Centre/Section/Unit)		
<i>To be filled by CITM</i>				
Estimated repair cost of the above mentioned equipment is Rs. _____ only.				
SIGNATURE OF HEAD, CITM				
CERTIFICATE				
Certified that the budget provision exists for the repair of above item(s) and that the funds are available. Recommended for approval.				
Dated: _____		SIGNATURE OF HEAD (Head of Department School/Centre/Section/Unit)		
FOR USE IN ACCOUNTS SECTION				
Sufficient funds are available/not available under budget Head _____ of (Department/school/Unit) _____ Funds amounting to Rs. _____ may be redeployed from Head _____ of Department/school/Unit) _____ Funds cleared vide Sr. No. _____ on _____ for Rs. _____.				
Approved Redeployment of Funds				
ACCOUNTS SECTION			DIRECTOR	
<small>(Please send this form to HCITM after fund Clearance)</small>				
APPROVED/NOT APPROVED DY. DIRECTOR /DIRECTOR				

Note: From June 2020, This Performa shifted to online support system at <https://eticket.thapar.edu/>. Now, Users can create an eTicket for this service with help topic “Repair of PC-Laptop Support” & “Repair of Equipment Support”.

APPENDIX – IV: REQUISITION PERFORMA TO DELETE AN ARTICLE/PAPER FROM TURNITIN REPOSITORY

<p>Thapar Institute of Engineering & Technology (Deemed to be University) Centre of Information & Technology Management</p>	<p>CITM/TUR/01  THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY (Deemed to be University)</p>										
<p>REQUEST TO DELETE AN ARTICLE/PAPER FROM TURNITIN REPOSITORY</p> <hr style="border: 1px solid red;"/>											
<p>To: Head, CITM</p> <p>I/We have submitted an article which was saved in Turnitin Repository.</p>											
<p>1. Paper Title (In Capital): _____</p> <p>_____</p>											
<p>2. Author Name 1. _____ Mobile No. _____</p>											
<p>3. Author Name 2. _____</p>											
<p>4. Turnitin Submission No: _____</p>											
<p>5. Class Id: _____</p>											
<p>6. Date of Submission: _____</p>											
<p>7. Turnitin Login ID used for Check plagiarism. _____</p>											
<p><i>Note: The above fields are mandatory to submit an article delete request with Turnitin. Turnitin may take 2 to 14 days to delete after submission request.</i></p>											
<p>DECLARATION</p>											
<p>This is certified that article details mentioned above belong to me/us.</p>											
<p>Author 1</p>	<p>Author 2</p>										
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;">Name :</td></tr> <tr><td style="padding: 2px;">Designation/ Roll No.:</td></tr> <tr><td style="padding: 2px;">Email ID:</td></tr> <tr><td style="padding: 2px;">Date:</td></tr> <tr><td style="padding: 2px;">Signature:</td></tr> </table>	Name :	Designation/ Roll No.:	Email ID:	Date:	Signature:	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;">Name:</td></tr> <tr><td style="padding: 2px;">Designation/ Roll No.:</td></tr> <tr><td style="padding: 2px;">Email ID:</td></tr> <tr><td style="padding: 2px;">Date:</td></tr> <tr><td style="padding: 2px;">Signature:</td></tr> </table>	Name:	Designation/ Roll No.:	Email ID:	Date:	Signature:
Name :											
Designation/ Roll No.:											
Email ID:											
Date:											
Signature:											
Name:											
Designation/ Roll No.:											
Email ID:											
Date:											
Signature:											
<p>Forwarded and Recommended to HCITM</p>											
<p>SIGNATURE OF HEAD (Head of Department School/Centre/Section/Unit)</p> <hr style="border: 1px solid red;"/>											
<p>To be filled by CITM</p>	<p>Received on dated: _____</p>										
<p>Sr. No. _____ Job assigned to:</p>											
<p>Approved/ Not Approved</p>											
<p>(System Analyst)</p>	<p>(HCITM)</p>										

Note: From June 2020, This Performa shifted to online support system at <https://eticket.thapar.edu/>. Now, Users can create an eTicket for this service with help topic “TURNITIN Article Deletion”.

APPENDIX – V: REQUISITION PERFORMA TO VIDEO CONFERENCING

Thapar Institute of Engineering & Technology (Deemed to be University) Centre of Information & Technology Management	CITM/VC/01  <small>THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY (Deemed to be University)</small>						
REQUEST FOR VIDEO CONFERENCING REQUEST FORM							
TO: HEAD, CITM							
A. REQUESTOR CONTACT INFORMATION							
Initiated by Name: _____	Signature with Date: _____						
Department/ School/Centre/Section/Unit: _____							
Designation: _____	Mobile Number: _____						
Official Email Id, _____							
B. EVENT INFORMATION							
Event Name: _____ Event Date: _____							
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;">Begin Time (HH/MM):</td> <td style="width: 15%;"></td> <td style="width: 15%;">AM/PM</td> <td style="width: 25%;">End Time (HH/MM):</td> <td style="width: 15%;"></td> <td style="width: 15%;">AM/PM</td> </tr> </table>	Begin Time (HH/MM):		AM/PM	End Time (HH/MM):		AM/PM	
Begin Time (HH/MM):		AM/PM	End Time (HH/MM):		AM/PM		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">How Many Attendees</td> <td style="width: 50%;">How Many Presenters</td> </tr> </table>	How Many Attendees	How Many Presenters					
How Many Attendees	How Many Presenters						
<i>(Note: Kindly inform us 2 days before the Event.)</i>							
C. VIDEO CONFERENCING INFORMATION (Required):							
FAR-END Contact Name: _____							
Department: _____ Mobile Number: _____							
Official Email Id: _____							
IP Address: _____							
Forwarded and Recommended to HCITM							
SIGNATURE OF HEAD (Head of Department School/Centre/Section/Unit)							
To be filled by CITM Sr. No. _____ Job assigned to:	Received on dated: _____						
(System Analyst)	(HCITM)						

Note: From June 2020, This Performa shifted to online support system at <https://eticket.thapar.edu/>. Now, Users can create an eTicket for this service with help topic “Video Conferencing Support”.