IT POLICY

TECNIA INSTITUTE OF ADVANCED STUDIES
GRADE "A" INSTITUTE
Approved by AICTE, Ministry of Education, Govt. of India, Affiliated to G.G.S.I.P. University
Recognized Under Sec. 2(f) of UGC Act 1956.
INSTITUTIONAL AREA MADHUBAN CHOWK,ROHINI,DELHI 110085
Tel:91-11-27555121-24, E-Mail : directortias@tecnia.in, Website: www.tiaspg.tecnia.in

Introduction

Tecnia Institute of Advanced Studies provides IT resources to support the educational, instructional, research, and administrative activities of the Institute and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed/updated and carry outtheir functions in an efficient and effective manner.

This document establishes specific requirements for the use of all IT resources at Institute. This policy applies to all users of computing resources owned or managed by Institute. Individuals covered by the policy include Institute faculty and visiting faculty, staff, students, alumni, guests, external individuals andany other entity who fall under the management of Institute accessing network services via computing facilities of the Institute.

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.

Objective

- Institute IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the Institute on the campus. Misuse of these resources canresult in unwanted risk and liabilities for the Institute. It is, therefore, expected that these resourcesare used primarily for Institute related purposes and in a lawful and ethical way.
- 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.
- Information assets addressed by the policy include data, information systems, computers, networkdevices, intellectual property, as well as documents and verbally communicated information.

Roles and Responsibilities

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

- Institute shall implement appropriate controls to ensure compliance with this policy by their users. Computer Science Department shall be the primary Implementing Agency and shall provide necessary support in this regard.
- Use Institute's IT resources for those activities that are consistent with the academic, research andpublic service mission of the Institute and are not "Prohibited Activities".
- All users shall comply to existing national, state and other applicable laws.
- Abide by existing telecommunications and networking laws and regulations.
- Follow copyright laws regarding protected commercial software or intellectual property.
- As a member of the Institute community, Institute provides use of scholarly and/or

work-related tools, including access to the Library, certain computer systems, servers, software and databasesand 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 of protection from abuse and intrusion by others sharing these resources.

- Users of Institute shall not install any network/security device on the network without consultationwith the Implementing Agency.
- It is the responsibility of the Institute Community to know the regulations and policies of the Institutethat applies to appropriate use of the technologies and resources. Institute Community is responsible for exercising good judgment in the use of the available technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
- As a representative of the Institute community, each individual is expected to respect and uphold the Institute's good name and reputation in any activities related to use of ICT communicationswithin and outside the Institute.
- Competent Authority of Institute should ensure proper dissemination of this policy.

Acceptable Use

- An authorized user may use only the IT resources he/she has authorization. No user should useanother individual's account, or attempt to capture or guess other users' passwords.
- A user is individually responsible for appropriate use of all resources assigned to him/her, includingthe 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 Institute user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of Institute or a personal computer that is connected to the Institute campus through the Local Area Network (LAN).
- The Institute is bound by its End User License Agreement (EULA), respecting certain third partyresources; a user is expected to comply with all such agreements when using such resources.
- Users should make a reasonable effort to protect his/her passwords and to secure resourcesagainst unauthorized use or access.
- No user must attempt to access restricted portions of the network, an operating system, securitysoftware or other administrative applications without appropriate authorization by the system owner or administrator.
- Users must comply with the policies and guidelines for any specific set of resources to which he/shehave been granted access.
- When other policies are more restrictive than this policy, the more restrictive policy takesprecedence.

Privacy and Personal Rights

1) All users of the Institute's IT resources are expected to respect the privacy and personal rightsof others.

2) Do not access or copy another user's email, data, programs, or other files withoutauthorization and approval of the Competent Authority (CA).
3) While the Institute does not generally monitor or limit content of information transmitted onthe campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

Privacy in Email

While every effort is made to ensure the privacy of Institute 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 theuser.

User Compliance

When an individual uses Institute'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 Institute and adaptto those changes as necessary from time to time.

Access to the Network

- 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.
- Wireless client systems and wireless devices shall not be allowed to connect to the Institute's wirelessaccess points without due authentication.
- To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.
- Implementing Agency (IA) may block 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 threatto the network.
- Implementing Agency (IA) may also block content which, in the opinion of the Institute, is inappropriate or may adversely affect the productivity of the users.

Use of IT Devices Issued by Institute

IT devices issued by the Institute to a user shall be primarily used for academic, research and any other Institute related purposes and in a lawful and ethical way. This covers use of desktop devices, portable devices, external storage media and peripherals devices such as projectors, Wi-Fi, copiers, printers and scanners etc.

Enforcement

- This policy is applicable to all the users of Institute. It is mandatory for all users to adhere to the provisions of this policy.
- Each entity of Institute 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.

Deactivation

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

Audit of Institute Network Infrastructure

The security audit of NIC network infrastructure shall be conducted periodically by an organization approved by the Institute.

Review

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee (ICT)with the approval of the Competent Authority 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.
- 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 make an arrangement and makea person responsible for compliance.
- Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.
- All the computers and peripherals should be connected to the electrical point strictly throughUPS. 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 earthling and have properly laid electrical wiring.

- While connecting the computer to the network, the connecting network cable should be awayfrom 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 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 withpassword and also with read only access rule.
- For all the computers that were purchased by the Institute centrally and distributed to the departments, IA will attend to the complaints related to any maintenance related problems.

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 (antivirus software and necessary application software) installed.

- 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 updatingof the OS should be performed at least once in a week or so.
- 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.
- 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.
- Any software installed should be for activities of the Institute only.
- Computer systems connected to the internet, 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.
- 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.

Best Practices

Following best practices shall be adhered to, related to the use of desktop devices, portable devices,external storage media and peripheral devices such as printers and scanners on the Institute network.

- Firewall should be enabled at all times.
- User shall take prior approval from the IA to connect any access device to the Institute's network.
- User shall keep their passwords secure and not share their account details. Users shall keep strongand secure passwords as per the password policy of the application.
- All active desktop computers shall be secured with a password-protected screensaver which shouldbe set with automatic activation at 10 minutes or less.
- 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 theymay contain viruses, e-mail bombs, or Trojan horse code.
- User shall report any loss of data or accessories to the IA and competent authority of Institute.
- User shall obtain authorization from the competent authority before taking any Institute issueddesktop outside the premises of the Institute.
- Users shall properly shut down the systems before leaving the office/ department.
- Users shall abide by instructions or procedures as directed by the IA from time to time.
- If users suspect that their computer has been infected with a virus (e.g. it might have becomeerratic or slow in response), it should be reported to the IA for corrective action.
- 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.

Email Account Usage Policy

E-mail for formal communications facilitates 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 their mail account with their User ID and password.

Users may be aware that by using the email facility, they 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.
- While sending large attachments to others, user should make sure that the recipient has email facilitythat allows him to receive such large attachments.
- 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 mailcontains large attachments.
- 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.
- 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.
- User should refrain from intercepting, or trying to break into others email accounts, as it is infringingthe privacy of other users.
- 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 ITsecurity policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations ofInstitute's email usage policy.
- 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 stampedas SPAM mail lying in the folder. It is recommended to empty this folder as frequently as possible.

The above laid down policies are applicable to all email services that are provided by service providerssuch as Gmail, Hotmail, Yahoo, RediffMail 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.

Disposal of ICT equipment

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

Budgetary provisions for ICT

At Tecnia Institute of Advanced Studies use of ICT facilities has always been encouraged. In viewof this, Institute intends to provide budgetary provisions as follows:

- Budgetary provisions are made to maintain all the existing ICT infrastructure for smoothfunctioning of all the ICT enabled services.
- Adequate budgetary provisions under capital head are kept for up gradation andaugmentation of ICT infrastructure

Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediatelyto the IT Helpdesk. 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.

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 Institute website and by continuingto use the Institute's IT Resources following any update it is considered acceptance on the revised termsof this Policy.

Appendix – I: IT Service/Repair Requisition Slip(For Teachers & Staff only)

Requisition form (IT equipment)

Department:

Problem:

Date of request:

Name & Signature of requisitioner:

Approved by Principal:

Appendix – II: Requisition Slip for use of Auditorium/Lecture Theatre(For teachers & Staff only)

Requisition slip for use of Auditorium/Seminar Hall
(to be submitted at least one-day prior)

Department:

Program to be organized (Seminar/workshop/Lecture):

Requirement of Projector (Y/N):

Date, Time & Duration of program:

Name & Signature of requisitioner:

Approved by Principal: