SETHU INSTITUTE OF TECHNOLOGY

An Autonomous Institution, Accredited with 'A' Grade by NAAC
Affiliated to Anna University Chennai and approved by AICTE New Delhi
Pulloor, Kariapatti – 626 115, Virudhunagar (Dt), Tamilnadu.

INFORMATION TECHNOLOGY POLICY

1. INTRODUCTION

Sethu Institute of Technology 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 and carry out their functions in an efficient and effective manner. This document establishes specific requirements for the use of all IT resources at SIT. This policy applies to all users of computing resources owned by SIT. 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 in a lawful and ethical way.

2. SERVICE AND SUPPORT

At the heart of the College's IT structure is the System and Network Administration department. The IT Administrator is responsible for the day-to-day running of IT services and for ensuring the priorities of work flow from the college helpdesk portal. There are separate administrators for taking responsibilities for servers, network, systems and software. In addition, there is a separate website administrator is exclusively responsible for the development of the College's websites and for web communications.

3. 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.

3.1. 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 Head should make an arrangement and make a person responsible for compliance.

3.2. What are End User Computer Systems?

The institute will consider servers not directly administered by Computer Centre, 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 Centre, are still considered under this policy as "end- users" computers.

3.3. Warranty & Annual Maintenance Service

Computers purchased by any Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance service. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

3.4. 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 earthling and have properly laid electrical wiring.

4. 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 .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.

4.1. 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 .

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.

4.2. Use of software on Desktop systems

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.

4.3. 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.

4.4. 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.

5. USE OF IT DEVICES IN SIT 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 SIT network.

5.1. Desktop Devices

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

5.2 Security and Proprietary Information:

- User shall take prior approval from the SNA to connect any access device to the SIT network.
- 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.

- 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.
- 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.
- User shall report any loss of data or accessories to the SNA and competent authority of SIT.
- User shall obtain authorization from the competent authority before taking any SIT issued desktop 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 Computer Centre from time to time.
- If users suspect that their computer has been infected with a virus it should be reported to the SNA for corrective action.

5.3 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.

5.4 Use of Portable devices

Use of the portable devices shall be governed by the following:

- User shall be held responsible for any unauthorized usage of their institute issued Computers/Laptops/Mobiles/iPads etc. by a third party.
- Computer Centre 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.
- Users shall wipe or securely delete data from the device before returning/ disposing it off.
- Lost, stolen, or misplaced devices shall be immediately reported to the SNA and the competent authority.

- When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider

6. NETWORK (INTERNET & INTRANET) USE POLICY

Network connectivity provided through the Institute, it is governed under the Institute IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of Wi-Fi applications. Problems within the institute network should be reported to the SNA department.

6.1 IP Address Allocation

- Any computer (PC/Server) that will be connected to the institute network, should have an IP address assigned by the SNA department. 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.
- 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.
- Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy 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.

6.2 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 Centre 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.

- Access to remote networks using a institute 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.
- Network traffic will be monitored for security and for performance reasons at SNA department.
- 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.

6.3 Internet Bandwidth obtained by the Departments

- Internet bandwidth acquired by any department of the institute under any research Programme / project should ideally be pooled with the institute Internet bandwidth, and be treated as institute common resource.
- Under particular circumstances, which prevent any such pooling with the institute Internet bandwidth, such network should be totally separated from the institute campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.
- 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 the SNA department.
- Non-compliance to this policy will be direct violation of the Institute IT policy.

7. EMAIL ACCOUNT USAGE POLICY

SIT 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 with Sethu Institute of Technology domain. In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the Institute administrators, it is recommended to utilize the institute 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.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 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 facility that 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 mail contains 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 infringing the 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 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.
- 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.

The above laid down policies are broadly applicable even to the email services that are provided by other service providers such as Gmail, Hotmail, Yahoo, Rediff mail 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

8. BREACH OF THIS POLICY

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the SNA network admin (admin@sethu.ac.in). On receipt of notice of any suspected breach of this Policy, the institute reserves the right to suspend a user's access to institute 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 may be taken in accordance with the institute disciplinary procedures.

9. REVISIONS TO POLICY

The Institute reserves the right to revise the terms of this Policy at any time. It is anticipated, with the speed of development in IT equipment and infrastructure, that revisions may from time to time be necessary to this policy document. In any case, the policy document will be reviewed annually and updated as necessary in the light of developments within the College.

PRINCIPAL
SETHU INSTITUTE OF TECHNOLOGY
PULLOOR, KARIAPATTI - 626 115
VIRUDHUNAGAR (Dt)