# SETHU INSTITUTE OF TECHNOLOGY

**PULLOOR, KARIAPATTI-626 115.**

**(AN AUTONOMOUS INSTITUITION)**

# IT POLICY

# CONTENTS

## 1. INTRODUCTION

The College has established Information Technology (IT) Infrastructure including Computers, servers, Intercom, Internet, Wi-Fi and provides them to the faculty, staff and students as per the prescribed norms and academic standards. The IT policy defines regulations and guidelines for the responsible usage of IT infrastructure and ensuring security in accessing the data by all the users. It provides the guidelines for maintenance and safety of IT infrastructure. It also provides guidelines for the procurement, management, support and services of the IT facilities.

## 2. SERVICE & SUPPORT

### 2.1 Structure

The College has established to The System and Network Administration (SNA) Department to take care of the establishment, maintenance and safety of IT infrastructure and IT enabled services such as Server Maintenance, Internet Security, Network Maintenance, Institution Website Maintenance, Hardware & Software support, etc. The SNA Department has Network Administrator, Server Administrator, System Administrator, Web Developer and Software Programmers and they are responsible for the above services for IT infrastructure and IT enabled services.

### 2.2 IT Support

1. The institution uses an Online Grievance Form or IT Support Email, to provide IT support to the faculty, staff and students (USERS). The URL is http://portal.sethu.ac.in (students) and admin@sethu.ac.in
2. When the users need any hardware/software installations or when they face any technical issues, they are expected to provide details of their issue, to get support from the SNA Dept. via the online Grievance System or the IT Support Email and by intercom support only. Information through any other media would not be entertained.

3. For specific issues such as damage to Computers, replacement of PC or other IT equipments due to malfunctioning, it is mandatory to get prior approval from the Principal/ Head of the Institution/ Head of the Institution.
4. After the Grievance Form being submitted online, the users can expect the response within 1 working day. If there is no response within 1 working day, then the SNA Dept. staff should be asked to provide the reason and if still no response is obtained for 3 working days, a complaint may be registered through an email to the Principal/ Head of the Institution, through the Head of the Department.
5. The problematic computers and equipments may be taken to the SNA Dept. and the time required for the repair/troubleshooting/maintenance may be informed to the user.
6. The issues will be resolved on the basis of First come First Served (FCFS).
7. First priority should be given to ensure the Uninterrupted functioning of IT infrastructure.
8. Upgradation and development of the network and servers in due time will take high priority.

## 3. SECURITY

A secured network policy has been defined for multi-person environment, such as Management, Principal, Head of the Departments, Faculty and Student users.

### 3.1 Network Security

1. All Computers being used in the institution are connected to the organization's intranet i.e. Local Area Network (LAN) as well as the Internet.
2. Network security is enabled in all Computers through Firewall, Web Security and Email Security software.
3. All users are expected to comply with the IT Policy rules and guidelines while using and maintaining any IT equipment, software or data.
4. Any faculty or staff who notices misuse or improper use of equipment or software or data within the institution must inform the IT administrator immediately, through Principal/Head of the Institution.
5. Inappropriate use of equipment, software or data by any user will be subject to disciplinary action as deemed fit by the Principal/ Head of the Institution of the institution.

6. Confidentiality should not be breached, so that information is accessed only by the responsible authorities.
7. VLAN based network solution is implemented for all end-users to ensure network security.

### 3.2 Firewall

The College network incorporates a firewall to protect the flow of data traffic into our local network; to increase the security of the network and it helps us to keep the threat of malicious attacks to a minimum and to secure confidential information from such attacks.

1. All internet access from the college network must pass through the firewall, which helps to prevent the network against worms, viruses and malware.
2. Invalid Access will be identified and the unwanted contents will be blocked.
3. Detailed logs must be kept (where ever possible on a separate server). It should be automatically analyzed, for critical errors generating alarms. Logs should be archived for at least six months and up to one year. Critical log entries should be daily examined.
4. The Firewall must fulfill the requirements including backup/restores functions etc.
5. Firewall policies are defined in such a way to block or allow certain types of network traffic which are not specified in the policy exception. It also defines which firewall features shall be enabled or disabled and to be assigned to one or more multiple User Profiles.

### 3.3 Anti-Virus Software

1. Approved licensed antivirus software is installed on all Computers and Servers in the institution.
2. Two configurations – Basic and Advanced are maintained for Antivirus software installed on organization's computers. The configurations are installed on Computers as per data & work importance and also based on the requirement of particular Dept./Project.
3. All servers and workstations that are connected to the network must be protected with a licensed anti-virus software. The software must be kept up-to-date.
4. The users are expected to make sure that their Antivirus is updated regularly. The SNA Dept. should be informed if the Antivirus expires.
5. Any external storage device like pen drive or hard disk connected to the PC needs to be

completely scanned by the Antivirus software before opening it and copying files to/from the device.

### 3.4 Data Security & Monitoring

The institution's data, applications and networks should be protected from unauthorized access, alteration and destruction.

1. Various methods like access control, authentication, monitoring and review will be used to ensure data security in the institution.
2. Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.
3. Appropriate training must be provided to data owners, data users, and system & network administrators to ensure data security.
4. The institution classifies data into three categories:

**3.4.1 Highly Confidential Data**:

1. It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure.
2. E.g. Payroll, personnel, financial, biometric data, examination data, administrative data,

**3.4.2 Confidential Data**:

1. It includes confidential data which would not impose losses on the institution if disclosed, but should not be publicly available.
2. E.g. Agreement documents, unpublished reports, etc.

**3.4.3 Normal Data**:

1. It includes information that can be freely disseminated.
2. E.g. brochures, published reports, Institution Regulations, Syllabus, Magazines and Newsletters, etc,
3. Different protection strategies must be developed by the SNA department for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.
4. All data must be backed up on a regular basis as per the regulations of the SNA Dept. at the proper time.

5. Access to the network, servers and systems in the organization will be achieved by
6. individual logins and will require authentication.
7. All users of systems which contain highly confidential or confidential data must have a strong password.
8. Default passwords on all computer systems must be changed after installation.

**3.5 Inappropriate Use of Data**

The following activities are prohibited on institution's Internet network. This list can be modified/updated anytime by the Management Authorities as deemed fit. Strict disciplinary action, can be taken against any user involved in the activities mentioned below:

1. Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
2. Downloading images, videos and documents unless required for official work
3. Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material
4. Accessing pirated software, tools or data using the official network or systems
5. Uploading or distributing software, documents or any other material owned by the institution online without the explicit permission of the Authorities
6. Engaging in any criminal or illegal activity or violating law
7. Invading the privacy of colleagues
8. Using the Internet for personal financial gain or for conducting personal business
9. Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
10. Carrying out any objectionable or illegal activity on the Internet that shall damage the institution's reputation.

## 4. SERVER

Servers are utilized to share various forms of instruction to all the departments regarding Teaching – Learning, Research, faculty development, student services, and administration. College-wide server management practices define the roles, responsibilities & procedures and controls the consistent, secure, and responsible delivery of services.

### 4.1 Server Administrator

Server Administrator is Principal/ Head of the Institutionly responsible for performing all Domain Controllers, Application Servers, File Servers and Web Server and its functions, including the installation, configuration, security, monitoring, maintenance, registration, and assessment of the Server.

The Server Administrator retains ultimate responsibility for the Server. The Server Administrator will:

1. Register the server with IT Services by physical means or hosting the Server outside the Campus.
2. Provide financial resources required to maintain servers, which includes Server Management Compliance in Fiscal Planning, Business/Academic Continuity Planning, and Personnel Resource Planning.
3. Evaluate the capabilities required to maintain server prior to the purchase of any new server for compliance and review the alternative solutions, wherever and whenever applicable.
4. Conduct routine scans of the College Server Environment and resolve the vulnerability within 3 days.
5. Inform immediately to the Principal/ Head of the Institution and Management, if the server fails to adhere the above provisions of Server Policy, for necessary actions.
6. Each Faculty have the respective credentials to access their data from the server.

### 4.2 Back -up Procedure

1. HP Data Protector Software is automated with backup and recovery software for the institution's IT environment.
2. The Backup Server with capacity of 18 TB is supported with RAID 5 storage space
3. Periodical backup will be taken through TAPE Drive with capacity of 6.4 TB
4. **File Backup System**:
    a) Institution will be providing a file server for each department for backing up data of all users in the department. All users are expected to keep official data on the file system.
    b) The system administrator, Network Administrator, Principal/ Head of the Institution and the Authorities will have access to that data.

c) All users will login to the file server through a user ID and password.

5. **Server backup**:
    a) SNA Dept. is expected to maintain an incremental backup of all servers periodically.
    b) Replica mode of all running servers will be offline and it should maintain half-hourly backup.
    c) The hard disk of every server should be in the RAID5 mode.

## 5. SOFTWARE

Faculty, Staff and Students of Various departments may use Licensed Software as well as Open Source Software for Academic and Administration Purposes. The policy provides guidelines for appropriate installation, usage and maintenance of software products installed in the institution-owned computers.

1. Prior approval from Principal/ Head of the Institution and Management should be obtained by the concerned Department Head or through SNA Department before purchase/ acquisition of any Software.
2. Software licensed or purchased by the institution must be registered in the name of the institution with the Department in which it will be used and not in the name of an individual.
3. All Software must be Registered and must be renewed periodically. A copy of all license agreements must be maintained by the SNA Dept.
4. Software will be installed by SNA or by any of the department level Technicians.
5. After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in the SNA Dept.
6. Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the institution is strictly prohibited. Any such act will be subject to strict disciplinary action.
7. Users are not permitted to bring Software from Home (or any other external source) and load it onto official computers.
8. No user is allowed to install pirated software on official computing systems. Such breaches of software license agreements and piracy with respect to the software packages usage will lead to strict disciplinary actions.

## 6. PROCUREMENT OF IT EQUIPMENT

### 6.1 Purchase

Generally, Computers and Other Equipment used by College are procured by the System Administrator of the SNA Dept.

1. SNA Dept. will evaluate the best, standard and most cost-effective hardware or software to be purchased for a particular dept./project/purpose based on the requirement.
2. Placing orders for the hardware/software is made through SNA department with the guidance of Principal/ Head of the Institution and Management from the standard supplier.
3. All newly purchased computers will have appropriate Anti-Virus, Anti-Spyware and Anti-Malware Software installed, and generally software updates will either be automatic or organized through the Lab Technicians on a routine basis
4. In general, Computers used for administrative purposes have a common program suite to cover most daily tasks as well as specific departmental software. Other additional software can be arranged through the Software Administrator /corresponding lab technician subject to the user's need.

### 6.2 IT Inventory Record

1. The following information of the IT facilities in the institution should be maintained in an Inventory Sheet:
    - Item
    - Purchase Order Number
    - Brand/ Company Name
    - Quantity
    - Invoice Number
    - Serial Number
    - Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.)
    - Physical Location
    - Date of Purchase
    - Purchase Cost
    - Current Person In-Charge
2. Proper information about all IT facilities provided to a specific department, project or center must be regularly maintained in the respective Stock Register by an in-charge from

that department, project or center on a regular basis.

3. When any IT equipment is being transferred or condemned, it should be updated in the Stock Register and the previous version of the document should be retained, with the date of modification.
4. Periodic inventory audits will be carried out by the SNA Dept. to validate the inventory and make sure all assets are up-to-date and in proper working condition.
5. No user is allowed to carry official electronic devices out of the institution, without permission from Principal/ Head of the Institution and SNA Dept.

## 7. NETWORK

Institution Network comprises of Optical Fibre, Wired and Wireless Connections throughout the Campus to various Department Buildings. Switch Gear (SG), L2 Switches and Wireless Access Points (WAP) will be maintained by the SNA Dept. for the institution's Academic Pursuits and Administration purposes. SNA department shall have direct access to any hardware component of the network, and interfering with any part of the Wiring, Optical Fiber and Hardware in the Campus by any member of the institution will be deemed as a serious matter.

### 7.1 Internet

1. Internet is a paid resource and therefore shall be used for learning and for official work only.
2. The institution reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the institution's network.
3. The institution has installed an Internet Firewall to assure safety and security of the institutional network. Any user who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.
4. All users may be provided with a Username and Password to login to the Internet network in the campus and to monitor their individual usage.
5. Username and password for a new user must be requested in writing through the Head of the Dept. and Principal/ Head of the Institution.
6. Sharing the Username and Password with another user, visitor or guest user is strictly prohibited.

7. Any password security breach must be notified to the SNA Dept. immediately.
8. Username and password allotted to an user will be deleted upon resignation/termination/retirement from the institution or completion of course by a student.

**8.1 Wi-Fi**

1. The Wi-Fi access for connection to the institutional network throughout the Campus, in the form of Intranet and Internet, is provided to the Students and Faculty based on the growing need for Academic and Administrative Purpose.
2. The growing use of mobile equipment is expanding accordingly to the growing demand of the Institution and hence the Wi-Fi strength and accessibility should be periodically monitored and updated to provide the facility without interruption.
3. The Wi-Fi devices will be periodically maintained by the SNA Dept.

**8.2 Intercom**

1. Intercom/Phone are installed in the Institution's offices and various departments to communicate internally with other faculty and staff and make external calls.
2. The intercom/phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the institution.
3. The SNA Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones, it should be informed to SNA Dept.
4. Faculty and Staff should remember to follow telephone etiquette and be courteous while representing themselves and the institution using the institution's phone services.

## 9. EMAIL ACCOUNT

1. A faculty or staff who joins the institution, is provided with an official email address, which should be used for official purposes only. To obtain a college e-mail Account a user first requires a faculty ID from Admin Office. Once it has been issued, an email account and Internet ID are created automatically by the SNA Department.
2. Any email security breach must be notified to the SNA Dept. immediately.
3. Upon termination, resignation or retirement from the institution, the organization will deny all access to electronic messaging platforms owned/provided by the institution.

4. All email signatures must have appropriate designations of faculty & staff.
5. Network Administrator should hold all relevant details of the account including passwords which should be sufficiently strong to ensure necessary security.
6. Inappropriate use of email accounts or the Internet may lead to Suspension from the Network.
7. The institution reserves the right to alter, modify, re-route or block messages as deemed appropriate.
8. Network Administrator can change the email system password and monitor email usage of any user for security purposes.

**10. INSTITUTION WEBSITE**

1. The Web Administrator, is responsible for the institution's website development and web communications.
2. The institution Domain needs to be purchased through a Government Authorized Reseller and its Renewal needs to be monitored by the Web Administrator.
3. The Web Administrator and Department Coordinators are responsible for content accuracy and to ensure that the site is kept up-to-date.
4. Updating the College Website is done by the SNA department based on the request by the Department Coordinators, and approval from Principal/ Head of the Institution.
5. Details of various events planned to be conducted in the Institution and Departments, achievements, information to staff and students, visitors, documents necessary, etc. should be updated in the website periodically.

**11. E-LEARNING**

All the computers in the institution are provided with internet or Wi-Fi connections. Users can access Digital Library from anywhere in the institution. Remote Access also has been provided for enhancing the e-learning. Website http://sitlib.sethu.ac.in

1. The e- Content management system in the Digital Library for e-learning should be taken care of by the Central Library, in order to promote self-learning capabilities among the students.
2. The faculty and staff can access any e-learning resource for upgrading their knowledge in the Teaching – Learning Process.
3. The e- learning resources which includes NPTEL videos, NPTEL Web courses, e-Books and

MIT Materials, DIGITAL LIBRARY which contains e-books for the benefit of the users, should be monitored for availability across time and location, by the library and SNA Dept.

4. The e-content available in the Digital Library, should be upgraded by the Central Library, every year by addition of new learning resources, with the help of SNA Dept.
5. The Central library of the institution should ensure timely renewal of the subscription for e-journals and Institutional Membership for the following:
    - E-journals (IEEE, ASME, ELSEVIER – SCIENCE DIRECT)
    - DELNET – Developing Library Network, New Delhi
    - British Council Library
    - American Information Resource Council (AIRC)
    - e- Sodhsindhu
    - Sodhganga
    - National Digital Library
6. The availability of the e-learning resources without any interruption should be monitored periodically by the library officials and if any problem arises, it should be solved with the help of SNA Dept.

## 12. REVISION

The right to revise this policy is with the Principal/ Head of the Institution and the Management based on the necessary developments in the IT infrastructure of the Campus. A committee framed by the Principal/ Head of the Institution may review and update the policy document, whenever necessary.

***Reviewed and Modified on: 01-04-2020***