SETHU INSTITUTE OF TECHNOLOGY
(An Autonomous Institution)

Estd. 1995

Pulloor, Kariapatti – 626 115.

ISO 9001-2008
FS 70973

IT POLICY

1. INTRODUCTION

The purpose of this document is to inform members of College of what can be expected in terms of Information Technology (IT). This covers the use of all Computers and other related hardware such as printers and the use of the network infrastructure. The use of computers connected to the College network both for academic and administrative purposes is covered together with the procurement of IT equipment and the maintenance and support of it by the College.

2. SERVICE AND SUPPORT

2.1 Structure

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 separateWeb Administratoris exclusively responsible for the development of the College's websites and for web communications.

2.2 Support Priorities

a) **The first priority is to ensure the IT infrastructure:** This includes both the network and servers works and ensured that they function without any interruption. From time to time upgrades and developments to the network and servers will be necessary and will take high priority in order to minimise overall disruption.

b) **The College administration infrastructure:** this includes Administrative Office, Principal office and Accounts office to ensure that there is no serious interruption in the operation of their IT equipment.

c) **Academic priorities:** This includes College Faculty and supporting staff to ensure that there is no serious interruption in the operation of their IT equipment.

d) **The College computer labs:** This includes students and faculty rooms to ensure there is no serious interruption in the operation of their IT equipment.

e) Help and advice on equipment, software upgrades and general IT requests from Faculty and students.

3. SECURITY

3.1 Network and Computers

Security of our network and of the computers used for the administration of College is a crucial aspect of our IT policy.For this reason, all computers attached to the network must have anti-virus software installed and in general should be checked before any connection is made to the network by the SNA department.The College is committed to protecting the security of its information and Information systems in order to ensure that,

a) The integrity of information is maintained, so that it is accurate, up to date and fit for purpose;

b) Information is always available to those who need it and there is no disruption to the regular activities;

c) Confidentiality is not breached, so that information is accessed only by those authorized to do so;

3.2 Firewall

The College network incorporates a firewall to control data traffic into and out of our local network; this increases the security of our network and helps to keep the threat of malicious attacks to a minimum and to keep confidential information secure.

a) All internet access from the college network must pass through the situated firewall. The default configuration, and other specified services are forbidden.

b) Detailed logs must be kept (where possible on a separate server). They should be automatically analyzed, with critical errors generating alarms. Logs should be archived for at least six months and up to one year. Critical log entries should be examined daily.

c) The Firewall must be high availability and fulfill the requirements (including backup/restores functions etc.)

d) The following incoming services are required from specific internal hosts to the internet:

- All User Should able to receive/send email
- Collage IP ranges, RDP

e) The following out going services are required from specific internal hosts to the internet:
- Email, www (http), ftp, telnet, SSH, News (NNTP),
- DNS (resolve Internet names), NTP (Network Time service),
- Aero hive (WiFi AP) Management connection

f) Anyone requiring other internet services will need to get approval from the principal and contact the SNA department for internet connectivity.

3.3 Monitoring

The College SNA department will continue to monitor, evaluate, develop and, where applicable, incorporate new rules and checks into the firewall. The College SNA department will also monitor the traffic going through the firewall, to identify any threats or misuse of the network.

3.4 Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be Modified/updated anytime by the Management/Head of the Institution.

- Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

- Playing online games, downloading and/or watching games, videos or entertainment software or online activity which compromises the network speed and consumes unnecessary Internet bandwidth

- Downloading images, videos and documents unless required to official work

- Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work

- Accessing pirated software, tools or data using the official network or systems

- Uploading or distributing software, documents or any other material owned by the Institution online without the explicit permission of the Management Committee

- Using the Internet for personal financial gain or for conducting personal business

3.5 System Audit

The SNA Department will conduct periodic system audit to make sure all compliances are being met. Prior notice may be provided by the SNA Department before conducting the System Audit. During this audit, the IT Dept. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes. The full cooperation of all the staff members required during such audits.

4. SERVER

Servers are utilized to deliver critical components of instruction, research, faculty development, student services, and administration. College-wide server management practices that define roles, responsibilities, procedures and controls encourage consistent, secure, and responsible delivery of services.

4.1 Server Administrator

An individual principally 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, at a minimum of capabilities:

- Register the server with IT Services by physical or hosting the server outside the campus.
- Provide financial resources required to maintain servers, includes server management compliance in fiscal planning, business/academic continuity planning, and personnel resource planning.

- Prior to the purchase of any server, the Server Administrator to evaluate the capabilities required to maintain server compliance and review alternative solutions where applicable.
- Server Administrator will conduct routine scans of the college server environment and Vulnerability will be resolved within 3 days.
- If failure to adhere the provisions of server policy shall be inform to management for necessary actions.

5. SOFTWARE

For the purposes of the College's administration, computer software will be installed by SNA as well as all department level technicians. College must be use licensed software as well as open source software for development and academic purposes.

5.1 Software Acquisition

- Software acquisition must begot prior approval from management and acquired by concern Department Head or through SNA Department.
- All the software must be registered and get updates from internet for upgrade periodically.
- Users are not permitted to bring software from home (or any other external source) and load it onto college computers
- The College takes serious actions for breaches of software license agreements and piracy with respect to software packages.

5.2 Antivirus Software

Approved licensed antivirus software is installed on all PCs owned by the SNA Department. Two configurations – Basic and Advanced are maintained for Antivirus software installed on All the computers. The configurations are installed on PCs as per work requirement of particular Department. Staff members are expected to make sure their Antivirus is updated regularly. The SNA Department should be informed if the Antivirus expires. Any external storage device like pen drive or hard disk should be prohibited.

5.3 Data Backup Procedure

Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that staff members keep important official data in some external storage device also.

File Backup System:

SNA Department will be installing a file server for backing up data of all staff members. All Staff members are expected to keep official data on the file system.

Server backup:

SNA Department is expected to maintain an incremental backup of all servers with at least 4 Copies of all servers. At any time, 4 backups of all servers must be maintained.

.

6. PROCUREMENT OF IT EQUIPMENT

In general computers and other equipment used by college are procured by the IT Administrator under a rolling renewal policy. Computers used for administrative purposes have in general a common program suite to cover most daily tasks as well as specific departmental software. Other additional software can be arranged through the IT Administrator /corresponding lab technician subject to the user's need in relation to their College duties.All new college computers will have appropriate anti-virus, anti-spyware and malware software installed, and generally software updates will either be automatic or organised through the lab technicians on a routine basis.

The following are the basic configuration for the desktop and laptop from the year 2019,

- Processor: Core i5 and Above
- RAM : 8 GB
- Hard disk: 1 TB

Placing orders for the College is made through SNA department with the guidance of Principal and Management from the standard supplier.

6.1 Compliance

All staff members are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the Management. Any employee who notices misuse or improper use of equipment or software within the Institution must inform his/her higher authorities immediately. Inappropriate use of equipment and software by an employee will be subject to disciplinary action.

6.2 Staff Training

Basic IT training and guidance is provided to all new staffs about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the Institution, accessing the network and using application software.

6.3 IT Support

Staff members may need hardware/software installations or may face technological issues which cannot be resolved on their own. They are expected to get help from the SNA Dept. for such issues through proper channel. For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all staff members to inform the SNA Department through channel. 6) For any damage to Personal Computers, approval from Reporting Manager would be required for PC replacements. Problems will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the Management/Head of the Institution.

6.4 Inventory Management

The Individual Department is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the Institution. The following information is to be maintained for above mentioned assets in Stock Register.

a. Item

b. Brand/ Company Name

c. Serial Number

d. Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.)

e. Physical Location

f. Date of Purchase

g. Purchase Cost

h. Current Person In-Charge

Proper information about all technological assets provided to a specific department must be regularly maintained in their respective stock register by an assigned coordinator from that department on a regular basis. The information thus maintained must be shared with the higher authorities as and when requested. Periodic stock audits will be carried out to validate the

inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

7. THE COLLEGE NETWORK

The College network comprises optical, wired and wireless connections throughout the various department buildings. Switch gear and wireless access points are the property of the College and are maintained by the College for its academic pursuits and administration.

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 Campusby any college member will be deemed to be a serious matter.

8. EMAIL ACCOUNT AND THE INTERNET

To obtain a college E-Mail Account a user first requires a faculty ID from Admin Office. Once this has been issued, an email account and Internet ID are automatically created by SNA Department.

The IT Administrator should hold all relevant details of the account including passwords which should be sufficiently strong to ensure necessary security. Inappropriate use of email accounts or the internet may lead to sanctions and to suspension from the network.

9. MANAGEMENT OF THE COLLEGE WEBSITE

The Domain needs to be purchased through a government authorized reseller and its renewal needs to be monitored by IT Administrator. A convener and department coordinators take responsibility for accuracy of the content and ensuring that the site is kept up to date. Updating the College Website is done by the SNA department based on the request by the department coordinators through website updating request form.

10. WIFI

The College is aware of the growing use of mobile equipment and is expanding its WiFi provision accordingly for all members of College. Around the campus there are WiFi access points for connection to the college network, the college's intranet and the internet.

WiFi access is provided to the students and staff on request for academic and administrative purpose only.

12. e-LEARNING

The purpose of the eLearning Policies and Procedures is to assure high quality in the delivery of eLearning with regard to instruction and learning. With effective eLearning Policies and Procedures, students will be provided the knowledge needed to achieve their professional and career goals in a student-centered learning environment. Faculty and staff will be provided the guidelines, which govern the teaching, learning, and support services for eLearning.

The College is aware of the benefit of free eLearning courses offered by NPTEL, MIT Open Courseware, etc., like

- To provide an alternative education delivery system for greater access by our students;
- To provide flexibility of time and location;
- To promote the integration of technology in the learning environment;
- To promote globalization of education through electronic access to information and experts worldwide.

The students those are interested to register for the e-Learning courses are given provision to register, attend the classes, submit their assignments and appear for the online exam for certification.

12. REVISIONS TO THIS POLICY

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.

Committee Members:

S. No.	Name & Designation	Signature
1	Dr.S.SivaRanjani, Professor & Dean (CS & IT)	

2	Dr.V.Shunmughavel, PG Head, M.E.CSE	
3	Mr.Dinesh, SNA/ADMIN	