SAVEETHA

INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES
(Declared as Deemed to be University under Section 3 of UGC Act 1956)

IT Policies & Guidelines

Requisite for IT Policy

- Basically the University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the **Co**nfidentiality, **I**ntegrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

    - Internet Unit is the department that has been given the responsibility of running the university's intranet & Internet services.
    - Internet Unit is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university.
    - SIMATS is getting its Internet bandwidth from VODAFONE IDEA LTD. Total bandwidth availability from ILL source is 310 Mbps (leased line).

While educational institutions are providing access to Internet to their faculty, students and staff, they face certain constraints:

- Unlimited Internet bandwidth.
- Limited infrastructure like computers, computer laboratories,
- Limited financial resources in which faculty, students and staff should be provided with the network facilities and

IT policies may be classified into following groups:
- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- University Database Use Policy

Further, the policies will be applicable at two levels:
- End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- Network Administrators

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities.

IT –Hardware policy

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, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In

case of any such instances, university 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

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. University as a policy encourages user community to go for open source software such as MAC OS, Keynotes and pages to be used on their systems wherever possible.

3. Key notes and Pages in Ipad and Mac IOS is used by the students and faculty instead of Microsoft office. This will be scrutinized meticulously by the IT Team every week.

B. Antivirus Software and its updating

1. Computer systems used in the university 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.

2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

C. Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not Foolproof solution. Apart from this, users we provide network sharing options for data storage.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Communication & Information Services (INTERNET UNIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to INTERNET UNIT.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the INTERNET UNIT. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building 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.

We are using DHCP server for Allocating IP for New systems. Its auto IP Generation and we are using class 3 protocol

IT POLICY – SIMATS

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 addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by filling up a requisition from meant for this purpose.

B. Running Network Services on the Servers

Individual departments/individuals connecting to the university 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 INTERNET UNIT in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

INTERNET UNIT takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

INTERNET UNIT 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.

Access to remote networks using a University'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 University Network connects. University 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 INTERNET UNIT.

Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University 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 University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

SIMATS –INFRASTRUCTURE

SIMATS has determined, provided and maintained the infrastructure necessary for the operation of its processes and to achieve conformity of products and services.

Buildings, Workspace and associated utilities

Library is fully automated using Autolib (OPACS)Software. All documents are bar coded and E-prints software is used for digital library.

Employee management system: HR management system and ARMS, is an Web application which helps us make a to do list and have a check on all the work that is happening currently. This also enables to allocate work to all, right from housekeeping and to all teaching and not teaching faculty to associate deans wherein they check it every day about the new allotted work and also updates on the completed task. This helps in smooth governance of all the work.

Hospital Management system: In the age of green technology, we have adopted an iPad-based Hospital Information System. It goes hand-in-hand with our aim to provide quick, seamless and comprehensive treatment to our patients while educating and training our students in toto. This system allows information to be accessed easily by both students and faculty at any given time on campus. It also

aids in recording procedures completed by students for patients which is simultaneously graded by the staff in-charge. A sense of responsibility and accountability is instilled in all.

Digital Class Rooms: The classrooms are equipped with smart boards extended into each individual student's iPad. The lectures prepared by the staff are uploaded on the UNIO Harness Touch on Cloud system and the students have access to the notes and presentations of the lecture. These lectures can be visited at any time for reference purposes in 3 layers namely original lecture layer, layer with student's notes and layer with staff notes. Students who have missed out on lectures also have the opportunity to catch up on the notes and presentation of the class.

OPAC system in Library: The following facilities are provided - AutoLib Software; Journal Management System; Shibboleth Athens; Wiley online portal; Content Management System in the form of iBook's. National knowledge network connectivity is available, wherein access to e-journals is available through INFLIBNET, DELNET, IUC facilities in addition to ERNET and other software.

Recruitment: SAP (Systems Application Product) is a digital application we use for recruitment. Any application received via online or in person is collected and it is saved in the SAP database. This is reviewed and updated on a regular basis. When there is a requirement for any position the database is analyzed for a suitable candidate and placement is provided. The same app is also used for maintaining the attendance, pay- roll, ESI, promotion, appraisal are all managed through this app.

Cafeteria: Food is an important component for anybody and our students have 5 cafeterias within the campus and are provide with smart cards. Ours is the first institution to introduce an allocate based smart mess. Students can choose anywhere across these places to swap and have their hearts content. They serve everything possible from pastries to biryani.

Indenting Software: Indenting the Monthly Requirement from Purchase department through Cranium Software.

SAP software: SAP is installed in the Accounts and Purchase department for managing purchases and easy approvals of the orders

DTP Centre: Well-equipped DTP center attached to the library with 5 high end Xerox machines.

ERP system: ERP is used for documentation purpose.

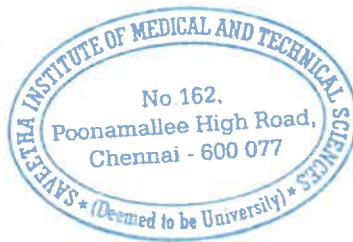**DREEM:** Students feedback is obtained and analyzed through online DREEM analysis.

Computer, Internet access, training to teachers and students and any other programmer for technology upgradation (Networking, e-Governance etc.)

I. Data Backup, Security, and Disclaimer

- INTERNET UNIT or COMPUTER CENTER will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an

- INTERNET UNIT/COMPUTER CENTER staff member in the process of helping the user in resolving their network/computer related problems. Although INTERNET UNIT/COMPUTER CENTER make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, INTERNET UNIT makes no guarantee concerning the security or privacy of a User's electronic messages.

- Security: We are Using Fortinet Firewall for blocking vulnerability attack and network attack in our INTRANET and INTERNET. We update the patches and maintained weekly once.

- We are Using AAA server for maintaining the local traffic and identification, authentication for entering in to the local network and equalized the bandwidth to all faculties and students

- The User agrees to be held liable for the improper use of equipment or

software, including copyright violations and agrees to defend, indemnify and hold INTERNET UNIT or COMPUTER CENTER, as part of SIMATS, harmless for any such liability or expenses. SIMATS retains the right to change and update these policies as required without notification to the User. We are using cloud storage and local network sharing drive for data backup.