Information Technology (IT) Policy

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

1. Introduction

Sri Satya Sai University of Technology & Medical Sciences 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 Confidentiality, Integrity, and Availability (CIA) 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.

Over the last many years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the university's academic environment.

University has too many network connections covering all buildings across the campus. 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, DHCP, DNS, email, web and application servers and managing the network of the university.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Guidelines are created and provided to help organization, departments and individuals who are part of university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies.

The current IT policy is sub-divided into following:

- IT Services Policy
- Data backup Policy for faculty, staff, students.
- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- IT Services helpdesk policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Website Hosting Policy
- University Database Use Policy
- CCTV Surveillance Policy
- Data Recovery in case of disaster
- Power Backup policy for IT hardware
- Cyber Security and Data Privacy

It may be noted that university IT Policy applies to

1. The technology administered by the university centrally or by the individual departments
2. The information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorized resident or non-resident visitors on their own hardware connected to the university network.
3. The resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognized Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the university.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

4. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do’s and Don’ts detailed in the university IT policy.

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. The violation of this IT policy by any university member may result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

IT Services Policy

IT Services provides a wide range of computing and communication facilities for faculty, staff and students. IT Services has a clear user focus, which is aimed at “providing a high-quality service”, includes

- Ensuring services meet user requirements
- Observing the performance of services
- Providing a economical service
- Applying a flexible operation appropriate to the vision of the University
- Providing effective communication and keeping the users informed
- Achieving user satisfaction

The purpose of this policy is to set out the services provided by IT. The Services IT manages includes:

1. Desktop & Laptop computing and support
2. Central computer hardware and networks
3. IT Strategy and the introduction of new systems
4. Day to day operation of existing systems

A brief summary of the range of services offered by IT Services is set out below.

1. Desktop computing and Support
2. IT Helpline the IT Services Helpline provides a first point of contact to IT Services for most users. Helpline Advisers provide help with a wide range of standard queries and ensure that problems are dealt with. The Helpline also deals with requests for new IT equipment and manages the communications to all staff about service availability for all systems.
3. Standard Hardware IT Services advise and recommend the choice of IT equipment. This includes purchases made with external/research funding. IT Services also co-ordinates ordering of all IT equipment and software to ensure cost-effective investment in IT.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

4. License Software

   University’s desktop software is licensed under a central license agreement form Microsoft. Other software, which has been properly evaluated, is available from a recommended software list. Requests for software can be made through IT Services Helpline.

5. Networks Manages the University networks including the campus’ mobile network and importantly its connection, which interconnects each other.
6. Servers
   Management of the University's core servers housed in specially equipped data centers with secure, temperature-controlled environments. Key activities include server back-ups, upgrades, patches, and service enhancements. These servers host main University systems, departmental systems, web sites, and student and staff network file space.

7. Telecommunications

   IT Services are responsible for the management of the University's Telephone systems, which includes all cordless handsets, desk sets and mobile phones. Security Maintaining IT Security and virus protection and providing advice and guidance.

8. Developing and maintaining Standard and specialist software ‘images’ for staff desktops, open access areas and IT teaching lab. IT Services also maintains a University wide printer strategy including deployment of MFP & Scanner.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

9. Operational Services
   a. IT Helpline & Problem Resolution
   b. New Username & Password: for Access the University internet and network
   c. New or replacement standard PC
   d. Specialist computer Hardware
   e. Mobile phone or mobile computing device
   f. Specialist computer Software
   g. Desktop software
   h. Network access and Wi-Fi connectivity
   i. Personal Storage
   j. Email Services – Students& staff

Services Provided - First line support to staff, students, external customers and partner Universities is available 24 hours a day all year round.

End-User responsibilities - Provide adequate information in order that a ticket can be logged relating to the nature of the query.

IT Team monitors all open incidents and escalate unresolved incidents to individuals and groups who can help to resolve the problem. When a problem arises, we will deal with it based on an initial assessment using severity table.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

IT Hardware Installation Policy

The life of any desktop, laptop, or peripheral at the University should be at least two years. Desktop computers, laptops, and peripherals should not be replaced until their minimum life has expired, unless the device encounters malfunctions which cannot be repaired. The Information Technology team is responsible for supervising the acquisition of desktop computers, laptops, and peripherals in the departments.

No academic or administrative staff member may obtain more than one computer (either desktop or laptop). Devices whose guarantee periods have expired, will be assessed and maintained as needed after obtaining the approval of the IT Manager.

IT Manager assesses and prepares the reports and plans the replacement of devices annually, at the beginning of each academic year, in consultation with the university fraternity. Applications for replacements that are outside the ordinary replacement cycle are submitted to the IT Manager.

The Manager, Information Technology evaluates and consults specialized sales agents to choose the best national/international brands and quality of model, price, and efficiency that are suitable for university.

The Manager, Information Technology supervises the purchase and distribution process for desktop computers, laptops, and peripherals.

All the desktop and laptop computers are equipped with a preloaded operating system in line with the needs of the different colleges and departments, after being approved by the Manager of Information Technology.

E-waste management is done in accordance with the E- Waste (Management) Rules, 2016 (amendment, 2018) [Government of India], under which it is ensured by the authority that the electronic waste is delivered to authorized recyclers or dismantlers annually after complete documentation is done.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Software Installation and Licensing Policy

The purpose of this Policy is to underline the importance of compliance with software licensing provisions and to define specific responsibilities relating to this compliance.

Responsibility for ensuring software license compliance rests with the Head of Department.

The specific responsibilities are to:

- Maintain a register to provide proof of purchase of software.
- Maintaining a register of disposal of software through on-sale.
- Maintaining an inventory detailing where licensed software is installed.

In the interests of ensuring compliance with licensing requirements, IT Department from time to time investigates a software compliance audit.

To ensure the continuous education of students, the university encourages the usage of

- Open-source software
- Virtual labs for conduction of practical
- LMS complier
- Licensed software
- Coursera for online certifications

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

IT Services helpdesk policy

IT Team provides a wide variety of technical support to students, faculty and staff to enhance learning through the use of technology.

Campus Support Request

- Get Support via ERP

  User can lodge the complaint using the option available in the university's ERP system, by logging in using authorized ID and password, followed by the completed details of the issue/problem encountered. The complainant is advised to mention their correct contact information (especially mobile number).

- Get Support via Email

  User can email our helpdesk request to info@sssutms.co.in. Please include your name, email address (if different), phone number and a detailed description of the problem.

- Call Us

  If your email and Internet service is unavailable you can contact the IT help desk at (+91) 07562-292740 | 7562292720, (+91) 7748900027 | 7748900028.

- Visit Data center

  You can visit to datacenter to lodge the complaint manually.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Network (Intranet & Internet) Use Policy

The university will take reasonable and appropriate steps to protect the information shared with it from unauthorized access or disclosure. The university strives to implement security measures that protect the loss, misuse, and alteration of data collected. The university maintains a computer security policy.

The IT Manager is responsible for ensuring the security of information maintained on computer systems in accordance with government guidelines. All information maintained on University computers is considered the property of Sri Satya Sai University of Technology & Medical Sciences. Access to University computer systems is restricted to authorized users only. Access to administrative applications is determined by the owners of the institutional data.

Security Arrangements:

The university's intranet has been secured by using the Firewall – Cyberoam – CR2500ING-XP.

Cyberoam's product range offers network security (Firewall and UTM appliances), Cyberoam network security appliances include multiple features like Firewall – VPN (SSL VPN & IPsec), Gateway Anti-Virus, Anti-Spyware & Anti-Spam, Intrusion Prevention System (IPS), Content & Application Filtering, Web Application Firewall, Application Visibility & Control, Bandwidth Management, Multiple Link Management for Load Balancing and Gateway Failover, over a single platform.

To access the intranet facility, each member of the university – student, research scholar, faculty and staff has been provided with a unique login ID and password, this ensures the network security from the premises outside of the university.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, 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, students and vice-versa. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. To use this facility faculty, staff, and students must log-in on Gmail based domain with their university’s email id and password. For obtaining the university’s user email id, user is to contact Registrar office/data center by submitting an application in a prescribed Performa.

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 university’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, offensive, explicit or fake 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 all most 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 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

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

potential to damage the valuable information on your computer.

- Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
- User should not share his/her email account 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 university IT security policy. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university'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. If so, user may forward that mail ID to info@sssutms.co.in for necessary action to delete from the spam mail category. 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 sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Website Hosting Policy

Sri Satya Sai University Official Pages

Schools, departments, and Associations of Teachers/Employees/Students may have pages on University Intranet Channel of the official Web page. Official Web pages must follow the University Website Creation Guidelines for Website hosting. As on date, the university's webmaster is responsible for maintaining the official web site of the university i.e. www.sssutms.co.in.

Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

Web Pages for eLearning

This Policy relates to requirements for Web pages for eLearning authored as a result of Teaching/Learning process.

Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

University Database Use Policy

This Policy relates to the databases maintained by the university administration under the university’s E-Governance.

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. University has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

Database Ownership: Sri Satya Sai University is the data owner of all the University's institutional data generated in the university.

Custodians of Data: Individual Sections or departments generate portions of data that constitute University’s database. They may have custodianship responsibilities for portions of that data.

Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

ERP Components: For the purpose of E-Governance, ERP System of the university may broadly be divided into seven categories. These are:

- Employee information management system
- Students’ information management system
- Financial information management system
- Project information monitoring system
- Library information management system
- Examination management information system
- Attendance management information system
- Student admission management system
- Student placement management system
- Alumni information management system

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

General policy guidelines and parameters for schools, departments and administrative unit data users:

1. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.
2. Data from the University’s Database including data collected by departments or individual faculty and staff, is for internal university purposes only.
3. One’s role and function define the data resources that will be needed to carry out one’s official responsibilities/rights. Through its data access policies, the university makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the University Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for response.
6. At no time information, including that identified as ‘Directory Information’ be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.
7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar of the University.
8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.
9. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:
    a. Modifying/deleting the data items or software components by using illegal access methods.
    b. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
    c. Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
    d. Trying to break security of the Database servers.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

CCTV Surveillance Policy

The system comprises of fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy.

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Security Control Room Administration and Procedures

Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

Recording

Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time. Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

All hard drives and recorders shall remain the property of university until disposal and destruction.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

Request to prevent processing

An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Head Security Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

Complaints

It is recognized that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Head Security Officer; these rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

Compliance monitoring

The contact point for members of University or members of the public wishing to enquire about the system will be the Security Office which will be available during the University timing from Monday to Saturday, except when University is officially closed. Upon request enquirers will be provided with:

- A summary of this statement of policy
- An access request form if required or requested
- A subject access request form if required or requested
- A copy of the University central complaints procedures

All documented procedures will be kept under review and a report periodically made to the Estates Management Committee.

The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)

13 Power Backup policy for IT hardware

Galgotias University is having its power back up (generators) unit rated 300 KVA, 125 KVA & 25 KVA enough back up energy around 10 hours for entire load. The generators turned on and all the protected electric loads seamlessly transferred to the backup power system.

For IT enabled essential applications are on UPS power supply. All academic blocks are having central UPS which are with redundancy. There is a separate UPS for Data Center.

Registrar
Sri Satya Sai University of Technology
& Medical Sciences Sehore (M P)