SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
(Approved by AICTE, New Delhi& Affiliated to JNTUA, Ananthapuramu)
(Accredited by NBA for Civil, EEE, Mech., ECE & CSE
Accredited by NAAC with 'A' Grade)
Puttur -517583, Chittoor District, A.P. (India)

IMPLEMENTATION OF E-GOVERNANCE

3. Policy document on E-governance

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY, PUTTUR

(AUTONOMOUS)

(Approved by AICTE & Affiliated to JNTUA, Ananthapuramu)
(Accredited by NBA for Civil, EEE, Mech., ECE & CSE Accredited by NAAC with 'A' Grade)

Puttur -517583, Chittoor District, A.P (India)

IT Policy

This policy has been approved in Governing Body with vide ref. No **April-2019 dated 29.04.2019.**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
(Approved by A.I.C.T.E., New Delhi & Affiliated to J.N.T.U.A, Ananthapuramu)
(Accredited by NAAC with 'A' grade)
(Accredited by NBA for CIVIL, EEE, MECH, ECE & CSE Courses)
SIDDHARTH NAGAR, NARAYANAVANAM ROAD, PUTTUR – 517 583
CHITTOOR DIST., A.P., INDIA

IT POLICY

Purpose of IT Policy

- To maintain, secure, and ensure the legal and appropriate use of IT infrastructure established by the college on the campus.

- To establish College-wide strategies and responsibilities for protecting the information assets that are accessed, created, managed, and/or controlled by the college.

- To work as a guide to stakeholders in the usage of the college's computing facilities including computer hardware, software, e-mail, information resources, intranet and internet access facilities.

- To set direction and provide information about acceptable actions and prohibited actions or policy violations.

Scope of IT Policy

- College IT Policy applies to technology administered by the college centrally or by the individual departments, to information services provided by the College administration, or by all departments, or by individuals of the college community.

- This IT policy also applies to the resources administered by the departments, such as Library, Computer Labs, Laboratories, and Administrative Offices of the College Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus networks are subject to the Do's and Don'ts detailed in the College IT policy.

- Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the college's information technology infrastructure must comply with the Guidelines.

- IT policies broadly concentrates on the following areas
  - ✓ IT Hardware Installation and Maintenance Guidelines
  - ✓ Software Installation and Licensing Guidelines

✓ Network (Intranet & Internet) Use Guidelines

✓ E-mail Account Use Guidelines

✓ Web Site Hosting Guidelines

✓ College Database Use Guidelines

IT Hardware Installation and Maintenance Guidelines

- IT Hardware Installation and Maintenance is performed by System Administrators.

- Faculty and the departments can submit IT Hardware requirements based on their academic needs.

- Procurement of IT Hardware should be initiated based on the availability of stock and the requirements submitted by the departments.

- Stock Register should be updated immediately when IT Hardware is procured.

- IT Hardware Installation and maintenance services are provided only after receiving approval from the concerned Head of the Department and the Principal.

- Maintenance of Computer Systems should be done periodically by System administrators, and the same need to be recorded in the Maintenance register.

- The movement of IT Hardware within the college or outside the college should be recorded in the Movement Register.

- The major e-waste such as written off instruments /equipment's, CRTs, Printers, Computers, batteries should be sold regularly.

- The Faculty or the department is solely responsible for the IT Hardware provided to them, and any damage or loss or theft needs to be addressed bear by them only.

Software Installation and Licensing Guidelines

- College IT policy allows authorized and open source software installation on the college computers. In case of any violation, the college will hold the Department/Individual personally responsible.

- Open-source software should be used in their systems wherever possible.

- Licensed software needs to be installed in the systems.

- Antivirus Software needs to be procured and installed in the systems.

- The system administrators should take Backup of Data periodically and store it in External Hard Disk.

- Software's used for academic and administrative purposes should adhere to ISO standards.

Network (Intranet & Internet) Use Guidelines

- Any computer (PC/Server) that will be connected to the College network should have an IP address assigned by the System Administrators.
- 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.
- Change of the IP address of any computer by staff or student is strictly prohibited.
- Configuration of a network will be done by system administrators only.
- Individual departments/individuals connecting to the College network over the LAN may run server software only after bringing it to the knowledge of the System Administrators.
- Access to remote networks using a College's network connection must comply with all policies and rules of those networks.
- Internet and Wi-Fi facilities should be used for academic and administrative purposes only.

E-mail Account Use Guidelines

- Every faculty is provided with an E-mail.
- The E-mail facility should be used primarily for academic and official purposes and, to a limited extent, for personal purposes.
- Using the E-mail facility for illegal/commercial purposes is a direct violation of the College's IT policy and may entail withdrawal of the facility.
- Faculty should refrain from intercepting or trying to break into others e-mail accounts, as it is infringing the privacy of other users.
- Impersonating the e-mail account of others will be taken as a severe offence under the College IT security policy.
- Ultimately, each individual's responsibility is to keep their e-mail account free from violations of the college's e-mail usage policy.

Web Site Hosting Guidelines

- The College Website should be used to provide academic and administrative information for its stakeholders.
- Website Updating Committee is responsible for content updating and maintenance of the website.

- Maintain up to date website pages. Test the web page links before putting them on the Web, and regularly update the links.
- The contents hosted on the website should be correct and precise.
- The departments and associations of Teachers/Employees/Students may have an official Web page on the website. Official Web pages must conform to the College Web Site Creation Guidelines.
- Website Updating Committee needs to take proper measures in safeguarding the security of the data hosted on the website.

College Database Use Guidelines

- The databases maintained by the College administration under the college's e-Governance must be protected.
- College is the data owner of all the college's institutional data generated.
- Individuals or departments generate portions of data that constitute the college's database. They may have custodianship responsibilities for portions of that data.
- The college's data policies do not allow the distribution of identifiable data to a person outside the college.
- Data from the College's Database, including data collected by departments or individual faculty and staff, is for internal College purposes only.
- One's role and function define the data resources needed to carry out one's official responsibilities/rights. The college makes information and data available based on those responsibilities/rights through its data access policies.
- Data directly identifying a person and their 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 IQAC Office of the College.
- Requests for information from courts, attorneys, etc., are handled by the Office of the College, and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the IQAC Office of the College for the response.
- At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes.

- All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Dean, IQAC coordinator, Controller of Examinations and Finance officer of the College.
- Tampering the database by the department or individual user comes under violation of IT policy.
- Certain violations of IT policy laid down by the college by any College member may even result in disciplinary action against the offender by the College authorities. If the matter involves illegal activities, law enforcement agencies may become involved.

Responsibilities of Network/System Administrators

- To Design College Network and perform Backbone operations
- To follow Global Naming & IP Addressing conventions
- To review the existing networking facilities and the need for possible expansion.
- Configuring and maintenance of Wireless Local Area Networks
- To configure and maintain IT facilities provided in classrooms, Labs and Seminar Halls.
- To receive and address complaints from users of the college network.
- To maintain servers in the server room.
- To look into the maintenance of Computer Hardware, Peripherals and Networking devices.
- To discourage installing any unauthorized software on the computer systems of the users.

PRINCIPAL