Technology Policy

1. Preface

The Sreenidhi University is committed to fostering a culture of efficient communication, collaboration, and knowledge sharing, and achieving a paperless environment through the strategic integration of Information & Communication Technology (ICT) in accordance with the UGC Guidelines for Institutional Development Plan for Higher Education Institutions (HEIs). It is also committed to move towards the idea of complete 'Digital Institution' in the lines of the NEP 2020. To support this vision, and in recognition of its increasing reliance on ICT, the University necessitates this comprehensive policy to ensure that ICT resources are used in a secure, effective, and responsible manner within the institution that mitigates risks and liabilities, maximizes benefits, safeguards institutional assets, and maintains integrity and security of the institutional data.

2. Objectives

This policy therefore aims outlining the regulations and guidelines for the proper use of the ICT resources and systems made available to the users by or on behalf of the University including desktops, laptops, mobile phones, network devices, internet, intranet, Wi-Fi, external storage devices, and peripherals like printers, scanners, copying machines, and such other equipment. It also applies to use of world-wide-web, blogs and wikis, e-mails, social networking or collaboration services. The objectives of this Policy are:

2.1. To regulate ICT Resource Usage: Establish regulations and guidelines for the proper use of ICT resources and systems made available by the University.

2.2. To ensure Secure and Responsible Use: Promote secure and responsible use of ICT resources, including desktops, laptops, mobile phones, network devices, internet, intranet, Wi-Fi, and peripherals.

2.3. To govern Online Activities: Regulate the use of online platforms, including the world-wide-web, blogs, wikis, e-mails, social networking, collaboration services, and system and application software.

2.4 To protect University Assets: Safeguard University ICT assets, services, and databases from unauthorized access, misuse, and other security threats.

2.5. To foster a Culture of Compliance: Educate users about their responsibilities and obligations when using University ICT resources, ensuring a culture of compliance and responsible ICT usage.

3. Scope and Applicability

This policy supplemented by the following policies, applies to all users of the University's computing, networking, and IT facilities, including students, faculty, staff, and administration. It is also applicable to the third-party contractors, agents, and suppliers wherever they are involved.

3.1. Hardware Procurement and Maintenance Policy
3.2. System Condemnation Policy
3.3. Website Policy
3.4. E-Mail Usage Policy
3.5. Anti-Virus Policy
3.6. Usage Policy
3.7. Network Access Monitoring Policy
3.8. Server Access and Maintenance Policy

These policies collectively govern the use of University IT resources and ensure their secure, efficient, and effective operation.

i. Services and applications that will not be used must be disabled where possible.
ii. Access to services should be logged and/or protected through access-control.
iii. The most recent security patches must be installed on the system as soon as practical.
iv. Trust relationships between systems are a security risk, and their use should be avoided.
v. Do not use a trust relationship when some other method of communication will do.
vi. Always use standard security principles of least required access to perform a function.
vii. Do not use root when a non-privileged account will do.
viii. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH).
ix. Servers should be physically located in an access-controlled environment.
x. Servers are specifically prohibited from operating from uncontrolled cubicle areas

b. Monitoring

i. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
   - All security related logs would be kept online for a minimum of 1 year.
   - Daily incremental backups will be retained for at least 1 week.
   - Weekly full backups of logs will be retained for at least 1 month.
   - Monthly full backups will be retained for a minimum of 3 years.

ii. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
   - Port-scan attacks
   - Evidence of unauthorized access to privileged accounts
   - Anomalous occurrences that are not related to specific applications on the host.

c. Routine Precautions

a. Only authorized administrators are authorized to login to the mail, web, proxy and other servers.
b. The designated system administrator/operational group receives an email alert whenever such an advice is released by the official maintainers of the software.
c. The software is updated periodically and whenever required.
d. All ports except those necessary for functioning of the servers are blocked (firewalled) both from outside and inside.

e. Standard intrusion detection software is run on the Sreenidhi network to monitor any change of MAC addresses corresponding to IP addresses of trusted machines. The Systems Manager automatically receives an email alert in such cases.

d. DHCP Server

i. The DHCP service of Sreenidhi to enable automatic IP configuration of clients.

ii. Installation of unauthorized DHCP servers, without explicit consent from the Computer Centre, will not be permitted in any VLAN as such DHCP servers can interfere with normal usage.

e. Compliance

i. Audits will be performed on a regular basis by authorized organizations within Sreenidhi.

ii. The Computer Centre group, in accordance with the Audit Policy, will manage audits.

iii. Computer Centre Group will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

iv. Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

Any employee/user found to have violated this policy may be subject to disciplinary action and as per IT laws of Govt. of India.