Date : 09-08-2022

IT POLICIES & GUIDELINES

The **IT Policies & Guidelines** of a college are established to regulate the use of information technology resources, ensure data security, maintain ethical standards, and support academic and administrative functions. These policies govern the usage of **computers**, **networks**, **software**, **data management systems**, and other IT infrastructure within the college.

The policies are designed to provide a safe, efficient, and productive IT environment for students, faculty, and staff while ensuring compliance with legal and ethical standards.

Objectives of IT Policies

- **Ensure Proper Use of IT Resources**: To ensure that all IT resources are used responsibly and effectively in line with the college's mission.
- **Data Security and Privacy**: To safeguard sensitive information and ensure the privacy of students, staff, and faculty.
- **Maintain System Integrity**: To prevent unauthorized access, misuse, or damage to the college's IT infrastructure.
- **Promote Ethical IT Practices**: To enforce ethical use of IT resources and prevent any illegal or inappropriate activities.
- **Support Educational and Administrative Needs**: To enhance the academic and administrative experience by providing reliable and secure IT services.

Scope of the Policy

The IT policy applies to all members of the college, including:

- **Students**
- **Faculty**
- **Administrative Staff**
- **External Contractors and Visitors**

It covers all IT-related resources, such as:

- **Network access** (Wi-Fi, wired networks)
- **Email services**
- **Software applications**
- **Computer labs**
- **Library IT resources**
- **Personal devices connected to the network**

Key IT Policies

a) Acceptable Use Policy

- All users must use IT resources in a manner that is ethical, legal, and aligned with the college's educational mission.
- Users must refrain from engaging in any activities that compromise the security or functionality of IT systems.
- Access to college IT systems is provided for academic and administrative purposes only. Personal use should be minimal and not interfere with these primary functions.
- Unauthorized access to systems, data, or networks is strictly prohibited.

b) Network Usage Policy

- The college network (both wired and wireless) is for educational and administrative use only.
- Users must not attempt to bypass network security measures, such as firewalls or authentication mechanisms.
- The college reserves the right to monitor network traffic to ensure compliance with this policy.
- Downloading or distributing illegal or inappropriate content (e.g., pirated software, copyrighted material) is prohibited.

c) Data Security and Privacy Policy

- The college is committed to protecting the confidentiality, integrity, and availability of data.
- Personal and sensitive information (such as student records or financial data) must be handled according to relevant data protection laws.
- Access to sensitive data is restricted based on user roles and responsibilities.
- Users must avoid storing sensitive information on unsecured devices or cloud services without encryption or proper authorization.

d) Email Usage Policy

- College-provided email services should be used for official communication only.
- Users are prohibited from sending spam, unsolicited bulk emails, or any form of harassment via email.
- Attachments or links containing malicious software must not be distributed.
- Users must avoid sharing their email credentials or accessing others' email accounts without permission.

e) Password Policy

- All users must create strong, unique passwords for accessing college systems.
- Passwords should be changed regularly and never shared with others.
- Multi-factor authentication (MFA) should be enabled for sensitive systems where applicable.

- Users are responsible for safeguarding their credentials and reporting any suspected breaches immediately.

f) Software Usage and Licensing Policy

- Only legally licensed software should be used within the college.
- Installing unauthorized or pirated software on college systems is strictly prohibited.
- Users should follow software license agreements and avoid copying or distributing software without permission.
- The college's IT department will manage the installation and updating of software.

g) Bring Your Own Device (BYOD) Policy

- Students, faculty, and staff may use their personal devices (laptops, smartphones, tablets) for academic or work purposes.
- Personal devices connected to the college network must comply with security guidelines, including the use of up-to-date antivirus software.
- The college reserves the right to limit or block access to the network for any device that poses a security risk.
- Users are responsible for the security of their personal devices and any data stored on them.

h) Social Media Policy

- Users must adhere to college policies when using social media platforms for academic or administrative purposes.
- The posting of defamatory, abusive, or inappropriate content related to the college, its staff, or students is prohibited.
- Personal opinions shared on social media must be clearly distinguished from official college communications.
- Sharing confidential information about the college or its members on social media platforms is strictly prohibited.

IT Support and Maintenance

a) IT Helpdesk

- The college maintains an IT helpdesk to assist users with technical issues related to hardware, software, and network access.
- Users should report any IT-related problems to the helpdesk for prompt resolution.
- Regular maintenance schedules will be in place to minimize system downtime.

b) Hardware and Software Maintenance

- The college's IT department is responsible for maintaining all hardware and software used on campus.
- Regular updates and patches will be applied to keep systems secure and functioning optimally.
- Any hardware malfunctions should be reported immediately to the IT department for repair or replacement.

Enforcement and Compliance

a) Monitoring

- The college reserves the right to monitor IT system usage, including network traffic, email communication, and access logs, to ensure compliance with the IT policies.
- Monitoring will be conducted in accordance with relevant privacy laws and only when necessary for security or legal purposes.

b) Disciplinary Actions

- Violations of the IT policies may result in disciplinary actions, including suspension of IT privileges, academic or administrative penalties, and, in serious cases, legal action.
- Any illegal activities, such as hacking or distributing illegal content, will be reported to law enforcement authorities.

c) Reporting Violations

- Users are encouraged to report any suspicious activity, security breaches, or policy violations to the IT department or relevant authorities within the college.

Policy Review and Updates

The IT Policies & Guidelines will be reviewed annually or as necessary to ensure they remain current and aligned with evolving technological advancements, legal regulations, and institutional requirements.

Any changes to the policy will be communicated to all users through official channels, and training or awareness programs will be conducted to familiarize users with the updates.

PRINCIPAL

Principal
Srinivasa Institute of Management Studies
Pothinamallayya Palem, Madhurawada,
Visakhapatnam - 530041

SIMS Dt:..... Madhurawada VIZAG - 41

SECRETARY