IT Policy

Velagapudi Ramakrishna
Siddhartha Engineering College
(Autonomous)

Index

1. Introduction

1.1 Purpose:

The purpose of the policy is to provide guidelines for the proper use, management, and security of Information Technology resources at Velagapudi Ramakrishna Siddhartha Engineering College (VRSEC). The policy aims to ensure the integrity, confidentiality, and availability of IT resources to support academic, administrative, and research activities.

1.2 Scope and Applicability:

The policy applies to all users, including students, faculty, staff, and authorized external entities, who access or use the IT resources of VRSEC.

2. IT Infrastructure Usage

2.1 Acceptable Use:

- IT resources should be used solely for educational, administrative, and research purposes only.
- Users must ensure their activities comply with all relevant laws, college regulations, and ethical standards.
- Integration of IT devices such as network switches, Wi-Fi access points, Wi-Fi routers, CCTV cameras, and any electronic devices must be carried out under the supervision of the HOD, CSE.
- Ensure that any modifications or new deployments of IT devices are first approved by the HOD, CSE to ensure compatibility with the existing infrastructure.

2.2 Unacceptable Use:

- Unauthorized access to systems, networks, or data.
- Sharing login credentials or attempting to gain unauthorized privileges.
- Accessing or sharing obscene, discriminatory, or unlawful content.

2.3 Access Control and Authentication Policies:

- All users must use unique usernames and strong passwords for accessing IT resources.
- Passwords must be strong, containing a combination of uppercase and lowercase letters, numbers, and special characters. They must be changed periodically, and sharing credentials is strictly.

3. Data Management

3.1 Data Protection and Privacy:

- Sensitive data, including student records and financial data, must be securely stored and accessed only by authorized personnel.
- Users must not share or disclose confidential data without prior approval.

3.2 Retention and Backup Policies:

- All critical data must be regularly backed up to secure storage.
- Data retention periods will comply with institutional and legal requirements.

4. Internet Usage

4.1 Guidelines for Internet Access:

- Internet usage is monitored to ensure compliance with college policies.
- Excessive bandwidth usage for non-academic purposes is prohibited.
- Internet access is permitted to authorized users only, user should use campus-provided internet credentials. Sharing of login credentials with others is strictly prohibited.
- Usage of Internet through Mobile devices should be done for academic, professional, or institution-related activities while on campus.

4.2 Network Security Measures:

- Firewalls and intrusion detection systems must be in place to protect the network.
- Users are prohibited from installing/connecting unauthorized devices or software on the network.
- The use of remote applications for accessing the internet is strictly prohibited to maintain network security and integrity.
- Personal network devices, including Wi-Fi hubs, routers, or switches, are strictly prohibited within the college network.

4.3 Bandwidth Management:

- Bandwidth allocation will be prioritized for academic and research activities.
- Streaming, gaming, and other non-essential activities may be restricted during peak hours.
- Bandwidth download manager applications are strictly prohibited.

5. Email and Communication Policy

5.1 Official Communication Channels:

- All official communications will be conducted through the college's email system.
- Users must regularly check their official email accounts to stay informed.

5.2 Guidelines for Email Usage:

- Emails must not contain spam, phishing links, or inappropriate content.
- Users must exercise caution when opening attachments or clicking on links from unknown sources.
- Passwords must be strong, containing a combination of uppercase and lowercase letters, numbers, and special characters. They must be changed periodically, and sharing credentials is strictly.
- Recommended to use Two Factor Authentication for Email login

5.3 Prohibited Content:

- Distribution of obscene, offensive, or discriminatory content via email is strictly prohibited.

6. Software and Hardware Policies

6.1 Approved Software and Licensing:

- Only authorized software with valid licenses may be installed on college systems.
- Users are prohibited from installing pirated or unapproved software.
- All software installations must be performed by the Respective Lab Technical Person/Central Server Room team. Installation requires prior approval from the respective department head and authorization from the college administration.

6.2 Hardware Procurement and Maintenance:

- All IT hardware must be procured through the designated administrative process.
- Maintenance and repairs must be carried out by authorized personnel.

6.3 Inventory Management:

- An up-to-date inventory of all IT assets will be maintained through stock registers and verified with the signature of respective heads of departments.
- Respective In-charges are responsible for reporting any loss or damage to IT assets.

7. Cyber Security Policy

7.1 Antivirus and Malware Protection:

- All systems must have up-to-date antivirus software installed.
- Users must avoid downloading or executing unverified files.

7.2 Incident Response Plan:

- Any cyber security incidents, such as data breaches or malware infections, must be reported immediately to the central server room.
- The CSE Technical team will take appropriate measures to mitigate and resolve incidents.

7.3 User Training and Awareness:

- Regular training sessions will be conducted to educate users about cyber security best practices.
- Awareness campaigns will be conducted to highlight common threats, such as phishing and ransom ware.

8. Bring Your Own Device (BYOD) Policy

8.1 Usage of Personal Devices:

- Personal devices may be used to access college IT resources only after prior authorization.
- Users must adhere to security protocols when accessing sensitive data.
- Personal devices must have updated antivirus software and operating systems.
- Don't Leave Your Device Unattended!.

9. Technical Support and Maintenance

9.1 Reporting and Resolving Technical Issues:

- All technical issues must be reported to the CSE Technical Team via the designated helpdesk system.
- The CSE Technical team will prioritize and address issues based on their severity.

9.2 IT Support Availability:

- CSE Technical Team support will be available during official working hours.
- Emergency support will be provided as needed.

9.3 Escalation Process:

- Unresolved issues may be escalated to relevant authorities for further action.

10. Computer Access and Usage Guidelines in Laboratories

- Laboratory computers are intended strictly for academic, research, and official institutional purposes.
- Access is permitted only to authorized students, faculty, and staff.
- Users must log in with their credentials and ensure to log out after completing their work.
- Sharing of login credentials is strictly prohibited for security and accountability.
- Administrative accounts for laboratory computers will not be provided to students and are strictly maintained by the lab in-charges to ensure system security and proper management
- Installing, modifying, or uninstalling software or hardware without prior approval is not allowed.
- Tampering with system configurations or network settings is strictly forbidden.
- Use of laboratory computers must comply with ethical and legal standards; accessing inappropriate or unauthorized content is prohibited.
- Personal usage such as gaming or social media is discouraged during laboratory hours.
- Data storage on laboratory computers is temporary; users should save work to personal storage devices or cloud services.
- Food, drinks, or any behavior that may cause damage to computer equipment is strictly prohibited.
- Any technical issues or malfunctions must be reported to the lab in-charge immediately.
- All activities on laboratory systems are subject to monitoring to ensure compliance.
- Non-compliance with this policy may result in restricted access or disciplinary action as per institutional regulations.
- Users are expected to treat all equipment with care and adhere to additional instructions from the lab in-charge.

11. Compliance and Enforcement

11.1 Monitoring and Auditing:

- The CSE Technical Team reserves the right to monitor and audit IT resource usage to ensure compliance with policies.
- Monitoring will be conducted in accordance with privacy regulations.

11.2 Consequences of Policy Violation:

- Violations of this policy may result in disciplinary action, including suspension or termination of IT access.
- Serious violations may be reported to legal authorities.

11.3 Policy Review and Updates:

- The policy will be reviewed annually to address emerging challenges and technological advancements.
- Updates will be communicated to all users through official channels.

12. CCTV Surveillance System Installation & Usage:

- CCTV systems are implemented to enhance security, ensure the safety of students, staff, and visitors, and protect college property from theft, vandalism, and other criminal activities.
- CCTV cameras are installed in key areas throughout the college campus to ensure comprehensive monitoring. The designated areas include:
    - Entrances and exits
    - Classrooms & Laboratories
    - Library
    - Parking
    - Canteen,
    - Corridors & etc.
- CCTV cameras will not be installed in private areas such as restrooms, staff rooms, or changing areas to ensure privacy.
- Notices will be displayed in areas under surveillance.
- CCTV footage will be stored for a minimum period of 30 days and deleted thereafter unless required for investigation purposes.
- Only designated individuals are allowed to access recorded footage for security investigations or audits.
- Any malfunctions will be addressed immediately, and the system will be repaired or replaced as necessary.

13. Website Maintenance Guidelines

- Ensure the website remains accurate, secure, and relevant for stakeholders.
- All departments and personnel must contribute to website content and updates.
- Website team manages updates, technical functionality, and security.
- Departments must submit accurate and timely updates via designated channels.
- Approval authorities review updates for compliance and accuracy before publication.
- Routine updates are published within 3-5 working days; urgent updates within 24 hours.
- Content must be professional, accurate, and comply with institutional policies.
- Quarterly reviews are conducted to remove outdated content and ensure functionality.
- Secure credentials are required for updates; regular backups and security patches applied.
- Staff receives periodic training on content submission and website policies.

14. Social Media Policy

- Official social media accounts represent the college and must be managed by authorized personnel only.
- All posts must align with the college's values, mission, and branding guidelines.
- Content must be professional, accurate, and respectful, avoiding controversial or offensive topics.
- Personal opinions must not be expressed on official accounts.
- Confidential information about the college, staff, or students must not be shared.
- Use appropriate language and ensure proper grammar in all communications.
- Images and videos used must be of high quality and comply with copyright laws.
- Comments and feedback must be monitored regularly; inappropriate content must be addressed promptly.
- Social media posts should be approved by the designated authority before publication.
- Students and staff must refrain from using the college's name or logo on personal accounts without prior permission.
- Periodic reviews of social media accounts and their content are required to ensure relevance and compliance.
- Non-compliance with the social media policy may result in disciplinary actions

15. The supervision of IT facilities by the Head of the Department of Computer Science and Engineering (HOD, CSE)

The HOD, CSE is responsible for overseeing the efficient and effective functioning of IT facilities across the entire campus. This includes ensuring that all IT infrastructure, systems, and resources are up-to-date, secure, and fully support both academic and administrative requirements. The HOD, CSE also coordinates with relevant bodies to ensure the smooth procurement, maintenance, and upgrade of IT assets.

The Head of the Department, CSE will supervise and monitor all the following Functions:

- Campus Network Implementation (LAN and Wi-Fi)
- Server Infrastructure
- CCTV Surveillance System
- Biometric Registration & Management
- Website Maintenance
- Software License Procurement/Renewals
- Procurement of ICT Infrastructure
- Integration of IT Devices
- IT Incident Reporting
- Training and Awareness

✓ Acknowledgment of IT Policy

All users must acknowledge and agree to abide by the IT policy. By using the IT resources of VRSEC, users consent to the terms outlined in this document.

✓ Contact Information

For any queries or support regarding the IT policy & Technical Suggestions users may contact the Department of CSE.

- Email: hodcse@vrsiddhartha.ac.in
- Phone Ext. : HOD, CSE : 301 & Central Server Room: 305

V.R. Siddhartha Engineering College 520 007 VIJAYAWADA.

18/6/2024

PRINCIPAL
V.R. Siddhartha Engineering College
AUTONAMOUS
VIJAYAWADA-520 007.