

INFORMATION TECHNOLOGY POLICY

Objectives

- ❖ To provide IT infrastructure that would enable the students, staff, and teaching and non-teaching faculty members to identify opportunities, improve performance, and understand the IT
- ❖ To introduce new technologies to students on par with industry standards and evolving advancements.
- ❖ To ensure an effective annual maintenance plan that ensures the maximum configuration of systems and devices.
- ❖ To ensure all IT resources are updated and available to students as per policies, according to the college.
- ❖ To regularly monitor processes for software updates, firewall protection, anti-virus updating, network device status, system file cleaning, new web access policies, and backups to ensure continuity of IT resources 24/7 to the authenticator.

Roles & Responsibilities

- All IT systems are purchased with a warranty, and after the expiration of this warranty, they are efficiently maintained through an effective annual maintenance policy that is aligned with the distributors and vendors.
- Maintenance includes OS re-installation, virus scans, bandwidth capacity monitoring, internet downtime, communication cable faults, UPS monitoring, firewall renewal, antivirus upgrades, device replacements, software upgrades, utilization maintenance of software like Adobe, etc.
- All departments are provided with desktop computers or laptops with wifi internet connectivity, and a printer. These are for the use of department faculty members, who are responsible for ensuring compliance.
- Systems are purchased at the request of the head of the department, which goes through multiple levels of approval from the principal and financial authority. Troubleshooting and replacements are handled by external service engineers as per the annual maintenance policy of the college.

- All systems and network devices are connected to electrical points through UPS. A regular 24/7 power supply is provided to web servers through recharging batteries. Regular battery maintenance is undertaken for all UPS.
- All files and printers shared through the network are well protected with passwords to ensure the integrity of the data.

Hardware Installation Policy

- Computer systems on campus are administered by system administrators and system engineers.
- All devices are installed by service engineers who are deployed inside the campus from 9 a.m. to 5 p.m.

Software Installation Policy & Licensing

- The Microsoft Campus Licensing Agreement policy covers all computers on campus, and this license is renewed annually.
- OS is installed by external service engineers on call as per annual maintenance agreements.
- Application software licenses are well maintained and renewed regularly to ensure valid and current updates to all application software.
- Utilization is also measured by the system administrators to assess the current usage of the software applications across the campus.

Network Use Policy

- The Technical Support Team is responsible for maintaining the internet and intranet services of the college.
- All the departments and labs are WI-FI enabled and have internet availability.
- All systems are networked and secured.

E-Mail Account Use Policy

- All faculty, lab assistants, and administrative staff members are given individual institutional email IDs and passwords.
- Passwords are confidential, and sharing such credentials is strictly prohibited.



(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
Chittoor Main Road, Vellore – 632 059.

- Attempting to access another member's login is strictly prohibited.
- All email communication must adhere to institutional and ethical guidelines and should be completely free of offensive or controversial content (creation or distribution).
- Unlimited memory capacity is given to critical or important email IDs.
- Users should not share their email account(s) with others.

Faculty Use Policy/Responsibilities of Departments

- ❖ Faculty members are responsible for the computers and devices of their respective departments, and for ensuring compliance with institutional and process-specific policies.
- ❖ Passwords are confidential and sharing these would be in direct violation of institutional policy.
- ❖ Use of institution resources for personal business gain, or for purposes that are inconsistent with the mission of the institution is prohibited and considered completely unethical.
- ❖ Unauthorized use of another's individual identification and authorization access is strictly prohibited.

Student Usage Policy/Responsibilities of Students

- ❖ Sharing of passwords, or other confidential information is strictly prohibited.
- ❖ Students are responsible for careful and judicious usage of computers in all Labs.
- ❖ Accessing another user's personal/ private data is not allowed.
- ❖ Downloading, sharing, or using copyrighted material of the institution including music, movies, software, or textbooks without prior approval is prohibited.
- ❖ Connecting to the institution's restricted-access resources is prohibited.
- ❖ Connecting personal devices to the institution's internet without approval is prohibited.
- ❖ Students must adhere to ethical guidelines, reflect academic honesty, and show restraint in the
- ❖ consumption of shared resources. Downloading of any unethical photos or videos will not be encouraged and strict actions will be taken against those individuals.

Video Surveillance Policy

- ❖ CCTV is installed in the classrooms, laboratories, corridors and the majority of the college premises.
- ❖ Videos are monitored regularly.
- ❖ Unauthorized access to the Control Room is not permitted at any time.
- ❖ Footages are given on demand and with prior approval from the principal.
- ❖ Cameras are serviced regularly.
- ❖ Live coverage is monitored by the Principal and Administrative Head.

Anti-virus Protection and Renewal Policy

- ❖ All computer systems in the college are covered under anti-virus protection.
- ❖ Application and Data Web Servers are secured with antivirus protection.
- ❖ Cisco Network Manageable switches provide a seamless network with secure, scalable, and robust performance.
- ❖ Regular renewal and updating policies are in place for antivirus and firewalls and are implemented promptly.

Maintenance Policy for Systems and Network

- ❖ All Lab systems are maintained and overseen by lab assistants, system administrators, and lab faculty in-charge.
- ❖ Technical problems such as power issues, booting, network problems, software installation, hardware troubleshooting, hardware replacement, and internet issues are
- ❖ handled by Lab assistants and senior staff.
- ❖ Major Networking issues and Operating system failures are restored by the System administrator and engineers on call.
- ❖ All Lab Computers are cleaned and serviced regularly.
- ❖ UPS maintenance and monitoring of battery levels are undertaken regularly.
- ❖ All Desktop systems are connected to network switches and maintenance of network cables is done regularly.
- ❖ Internet cables are well planned across the campus and networking is well designed