IT POLICY

Table of Content

About the Information Technology Policy

1. IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, faculty, Staff, Management and visiting Guests and Research Fellowship Members.
2. The IT policy of the college is formulated to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established on the campus and provide guidelines on acceptable and unacceptable use of IT resources of the college.
3. This policy establishes strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by the College
4. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information. In addition, this policy supports effective organizational security and protects users and IT resources from, but not limited to cyber criminals, bullying, misuse of accounts and assets as well as the spread of malicious software
5. Stakeholders on Campus or Off Campus
    - Students UG, PG, research Scholars
    - Faculty
    - Administrative Staff (Non-Technical/Technical)
    - Higher Authorities and Officers
    - Guests
6. Resources
    - Network Devices wired/wireless
    - Internet Access
    - Official websites
    - Official email services
    - Data storage
    - Desktop/server computing facility
    - Documentation facility (Printers/Scanners)
    - Multimedia Contents, Surveillance network
    - Learning Management Systems

IT infrastructure Installation Policy

1. College network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures
2. Computers purchased by any Department/ should preferably be with 3-year on site comprehensive warranty.
3. All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.
4. While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.
5. File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

Software Installation and Licensing Policy

1. Any computer purchases made by the individual departments should make sure that such computer systems have all licensed software installed.
2. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.
3. College as a policy encourages user community to go for open-source software such as Linux to be used on their systems wherever possible.
4. Computer systems used in the College should have anti-virus software installed in Major Official Systems and at least 1 system in Labs, and it should be always active. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
5. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency
6. Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. users should keep their valuable data either Google Cloud Storage and/or College Central Server.

Network (Internet & Intranet) Usage Policy

1. Any computer (PC/Server) that will be connected to the College network, should have an IP address assigned by the System Administrator. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other unauthorized person can use that IP address unauthorisedly from any other location. 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.
2. Individual Laptops/Mobile Can connect to College Network through Wi-Fi network and will get a dynamic ip through DHCP service in the UTM.
3. All individuals will get login credential for the use of Internet in the campus when they arrive/start the work/Course. Guest users can collect credentials from the front office
4. Access to remote networks using a college network connection must follow all policies and rules of those networks. This applies to any and all networks to which the College Network connects. College network and computer resources are not to be used for personal and commercial purposes.
5. Network traffic will be monitored for security and for performance reasons.
6. Nobody is allowed to Connect Any Network Devices in the College network without the prior permission from the System Administrator.

Information Security Policy

1. Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.
2. All data must be backed up on a regular basis as per the rules defined by the IT Dept. at that time.
3. Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.
4. Default passwords on all systems must be changed after installation.
5. All servers and Official Computers connected to the network must be protected with licensed anti-virus software. The software must be kept up to date. Others must keep USB Drive inaccessible.
6. Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.
7. Server/Desktop, firewall and critical system logs must be reviewed frequently.
8. Working Files shared via network with a File Server named PCSHARE and accessed with password.

Email Account Use Policy

1. To increase the efficient distribution of critical information to all faculty, staff and students, and the College administrators, it is recommended to utilize the College e-mail services, for formal College communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal College communications are official notices from the College to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general College messages, official announcements, etc.
2. For obtaining the College email account, user may contact System Administrator for email account and default password.
3. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:
    - the facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
    - using the facility for illegal/commercial purposes is a direct violation of the College's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
    - while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
    - User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
    - User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
    - User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users and also against policy..
    - While using the computers that are shared by other users as well, any email

account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

- It is ultimately everyone's responsibility to keep their e-mail account free from violations of College's email usage policy.

Approved By

Fr. George Pareman
Executive Director,
Sahrdaya College of Engineering and Technology.