EDUCATION IS DEDICATION

SAHRDAYA

COLLEGE OF ENGINEERING & TECHNOLOGY
Kodakara, P.B.No.17, Thrissur (Dt), Kerala State, India - 680684
Ph. 0480-2726630, 2759275, Fax: 0480-2726634, info@sahrdaya.ac.in, infosahrdaya@gmail.com;www.sahrdaya.ac.in

Cyber security & Internet policy

In the digital age, cyber security and internet policy have become critical considerations for higher education institutions. With the increasing reliance on technology and online resources, Sahrdaya College of Engineering and Technology has strived to establish robust policies to protect sensitive information, ensure secure communication, and promote responsible internet usage. This document aims to outline the importance and key elements of a comprehensive cyber security and internet policy for our institution.

PURPOSE

The purpose of this policy is to provide guidelines and procedures for safeguarding digital assets, protecting against cyber threats, and promoting responsible use of internet resources. The policy aims to ensure the confidentiality, integrity, and availability of institutional data, as well as to educate and raise awareness about Information/cyber security, network usage, and email account usage best practices.

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

Approved

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.

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 unauthorized 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.

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.