POLICIES AND GUIDELINES
FOR
INFORMATION SYSTEMS AND TECHNOLOGY

Approved by the Information Technology (IT) Committee, SCTIMST held on 15/03/2016 chaired by President Shri. K. M. Chandrasekhar

Members:

- Sri. K.M. Chandrasekhar (President of SCTIMST & Chairman)
- Dr. Asha Kishore (Director, SCTIMST)
- Sri. G.Vijayaraghavan, Former CEO Technopark, Member of Planning Board
- Sri. K. Mohammed Y.Safirulia IAS, Director, Kerala State Information Technology Mission, Department of Information Technology, Govt. of Kerala
- Sri .G.Jayakumar, Senior Technical Director, NIC, Kerala
- Mr. Ishaque Mannisheri, Technical Specialist, Kerala State Information Technology Mission, Govt.of Kerala
- Dr. Geetha G. (Convener)

SCTIMST Information Systems and Technology Policies and Guidelines

Overview

SCTIMST maintains certain policies with regard to the use and security of its computer systems, networks and information resources. Information Systems and Technology (IS & T) policies are implemented through Computer Division. Policies are guided by the Director of the Institute.

I. IS & T Policies in General

1. All users of these facilities, including technology developers, end users and resource administrators, are expected to be familiar with the policies and the consequences of violation.

2. Users are expected to respect the privacy of other users and they may not allow any other person to use their password or share their account. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever, is strictly prohibited.

3. Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorized access to institute LAN or network resources is forbidden. Users may not use another person's computing account; attempt to forge an account identity, copy institute data for personal use or use a false account or e-mail address.

4. Uses are adviced never to leave a computer logged on to networks, email and web sites. Uses have to activate a password-protected screensaver. Never to save passwords under browser sessions.

5. Should NOT attempt to install software or hardware or change the system configuration including network settings

6. Respond immediately to any virus warning message on your computer by raising the service request.

7. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. It is also forbidden to send emails or messages concealed as another person or to hide the sender's identity. Chain letters are not allowed.

8. To the extent possible, users are expected to use only their official email addresses provided by the institute for all official communications.

9. Users are encouraged to use/update the official social media pages of the institute within the guidelines published by the institute.

10. No food/drink is permitted in the computing periphery. Smoking is strictly prohibited. Also making noise either through games/ music is prohibited. Work area to be kept neat and clean by the user.

11. Shutdown and power off the PCs and peripherals when not in use.

12. USB access is not provided in shared PC's and USB is enabled in individual PC's where official data transfer is required. Antivirus checking is mandatory before any data transfer from USB.

13. Disconnection/removal of peripherals of institute PC like keyboard, mouse, network etc. is not allowed.

14. All IT units (Hardware/Software) to have the display/marking of department stock number.

15. All licenses to be registered under Director, SCTIMST.

16. Any Hardware/Software service is executed on receipt of request from the concerned either through online service request or on paper mentioning the stock number.

17. Hardware service request received will be attended based on priority and availability of spares/man power.

18. If any software request / integration with equipments is received from any department for their automation; Computer Division will do a detailed system study to assess the feasibility. On acceptance of system design by the requested department; To the extent possible, customized software development will be undertaken in house by staff from Computer Division than procuring off-the-shelf products.

19. Institute softwares used for official activity/ patient care are installed only in institute units located in corresponding work places.

20. Printing is permitted only for official/patient care purpose. Users must make efforts to limit paper usage by taking advantage of double-sided printing.

21. Connecting unauthorized devices into the institute network is not allowed.

22. All devices to be handled with care. Any physical damage due to careless usage will be charged to the user.

23. Unauthorized access/transfer of data/information/material in either through print or by electronic method should be avoided.

24. Hardware/Software facility provided to Staff/Student will get disconnected on their retirement/relieving. Staff has to hand over the hardware/software to the Officer in – charge before 'No dues' settlement.

25. Institute affirms its commitment to environmental protection by ensuring proper e-waste management. The disposal of obsolete IT equipments shall be made in accordance with e-waste management rules of the Institute.

26. Servers and information that require protection are placed in secure rooms and access is restricted to authorized staff. System Manager is responsible for approving physical access to this area.

II. Policy on available computing services

Staff Access to institute software's in each department

Regarding staff access to modules for office work

Each staff can access their department software through their login. Transferring data/information/material from one department to another, either by print or email or any other electronic methods without proper consent is a violation. Login is validated with their working department code and authentication to use the modules. On transfer; their access will get disconnected automatically. The Institute maintains application usage log by the user for five years.

SCTNET Rules of Use

Describes the use of the service SCTNET' in the network for all staff

Each Staff/Student will be provided with a login screen where login id is his/her employee code. On joining; Staff /Student can set his/her own password. They can access all personal information like their salary, PF, Income Tax, leave details, duty roster, attendance, reimbursement, PF, HTC, LTC. etc. Screen for raising purchase indent, request for maintenance/service, request for store issues, condemnation, making duty roster, viewing general reports etc. is also provided. According to the staff/student designation/category; additional modules are assigned for viewing department purchase orders, expenditure, project costs, etc. Staff/Students are advised to keep strong passwords secured.

Internet Access Policy

Regarding the internet connection to faculty/supervisors/senior residents /students / technical staff.

Wired internet connection is issued in institute PCs of Supervisors/Dept heads for official use. Additional wired internet connection is issued in institute PCs as per the requirements projected by Head of Department/SIC for official use.

Wireless Internet connection to one personal device is provided to all Academic Staff, Supervisors, Senior Residents,Students and Technical Staff. (subject to the availability of infrastructure) strictly for academic/research/official activites

Wireless controller is configured for internet access through access points installed in the campus. The mac address and wep key is mapped for security.

For general use, internet connection is provided in Library PC's. Gateway security software is used for blocking unauthorized sites.

Antivirus

It is mandatory that reliable antivirus software with updates to be installed in all personal devices / official computers having internet access. Any data transfer from USB storage to be initiated only after virus check.

Institute's license for antivirus is issued only to Institute units. The User is responsible for any data/e-mail that is transmitted using the Institute internet service.

Users shall be responsible for all the activities carried out on the Internet including social media. Institute maintains Internet usage log for six months.

Intranet Access Policy

Intranet can be accessed from outside campus based on staff/student authorisation. Orders/Circulars will be published in intranet for easy reference.

Institute Email Policy

Describes the use Email service in the network

Institute is issuing email id to all academic staff, senior residents, students, head of departments/sections for official campus/outside communication. Staffs in each section are also provided with email id for internal communication.

To the extent possible, users having institute email ID's are expected to use only their official email addresses for official communications. Password change is forced every year. Email id issued will get disconnected on their retirement/relieving.

<u>Inappropriate use of the e-mail service</u>

- Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.
- Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.
- Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.

- Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.
- Creation and exchange of information in violation of any laws, including copyright laws
- Willful transmission of an e-mail containing a computer virus.
- Misrepresentation of the identity of the sender of an email
- Use or attempt to use the accounts of others without their permission.
- Transmission of e-mails involving language, derogatory of religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing antinational messages, sending e-mails with obscene material, etc.
- Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

  Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation of the account.

User's Role

- The User is responsible for any data/e-mail that is transmitted using the Institute e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
- Sharing of passwords is prohibited.
- The user's responsibility shall extend to the following:
  - Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.
  - The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.
  - A backup of important files shall be taken by the user at regular intervals. The Institute shall not restore the data lost due to user's actions
- Users shall hand over the designation based email id to their successor prior to transfer/retirement. Prior to leaving an organization on transfer, the user to whom the designation based id had been assigned shall ensure that the password for the id is changed. The successor shall need to get the password reset after taking over the post.

Data Retention

Users are responsible for e-mails saved in their folders e.g. Inbox, Sent Mail, any other folder created by the user. E-mails shall be automatically purged from "Trash/Deleted items" and "Spam" folders after two months.

Email Data Backup

a) The Institute takes a backup of the e-mail data on a regular basis to ensure timely recovery from a system failure/crash/loss impacting the service.
b) Each user is responsible for the individual e-mails stored in their folders. The Institute shall not be responsible for any accidental deletion of emails by the user.
c) The Institute shall not offer a service for restoration of lost data due to an action committed by the user.

d**)** In the eventuality of a disaster/calamity, all possible attempts to restore services and content shall be made. However, in circumstances beyond the control of the Institute, it would not be held responsible for loss of data and services.
e) Institute maintains an email usage log for last six months

III. INSTITUTE Data Backup

Describes the policy for data backup

Database, patient's data (images, lab reports, summaries, scanned files), official documents stored in institute storage are backed up into tape library on regular intervals.

Users having PC with USB storage facility are advised to do their own data backup to their external storage devices regularly. The Institute is not responsible for any data loss from these units.

IV. IT infrastructure management policy

Monitoring of system access and usage

a. Access and use of IT systems should be logged and monitored in order to detect unauthorized information processing activities.
b. Computer Division should register substantial disruptions and irregularities of system operations, along with potential causes of the errors.
c. Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.
d. Computer Division should log security incidents for all essential systems.
e. Computer Division should ensure that system clocks are synchronized to the correct time.

Intrusion detection

a. Intruder detection must be implemented on all servers and workstation Containing data classified as high or confidential risk.
b. Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
c. Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
d. Intrusion tools should be installed where appropriate and checked on a regular basis.

V. DISCIPLINARY ACTION

A penalty system will be implemented, in case someone is found violating the above guidelines mentioned.