SCMS GROUP OF EDUCATIONAL INSTITUTIONS, COCHIN

IT CODE OF CONDUCT / USERS POLICY

SECTION 1

SCMS is responsible for securing its computer systems in a reasonable and economically feasible degree against unauthorised access and /or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy may result in disciplinary action in the form of temporary revocation of user access, regardless of the success or failure of the attempt.

The users of the SCMS computer systems are responsible for respecting and adhering to local, state, national and international laws. Any attempt to break those laws through the user of the SCMS computer systems may result in litigation against the offender by the proper authorities. If such an event should occur, the SCMS will fully comply with the authorities to provide any information necessary for the litigation process.

PRIVACY

All electronic equipment used by employees is to be considered property of the SCMS. All data, messages, or other files created while using the equipment is also considered property of the SCMS. The SCMS reserves the express right to monitor and review all activities of the employee, including information created or obtained by the employee.

This monitoring includes, but is not limited to, reviewing files or correspondence created by any software medium and periodic scans of an employee's computer hard drive.

PERSONAL USE OF COMPUTERS

Employees are not to place personal copies of software or data on any SCMS equipment. If an employee requires the software, the SCMS may purchase a copy. This includes, but is not limited to games, screen savers, and questionable material. If found, that such software or data has been placed without the knowledge of SCMS, will be removed and a memo issued to the user, outlining what was found and the action taken to remove it.

It is SCMS policy that SCMS -owned software is not to be taken home and installed on an employee's home computer for personal or SCMS use, regardless of the software's licensing agreement.

CONFIDENTIALITY

Unless otherwise dictated by public disclosure laws, all information regarding the computers systems, or data created by employees, are to be considered confidential. Removing of data from the SCMS offices without the express consent of the IT dept/head of the organisation is considered a breach of this confidentially.

VIOLATIONS OF SCMS POLiCY

Violations of this SCMS policy may lead to revocation of computer use or disciplinary action, including discharge.

Employees will be required to sign a - Use of SCMS Network and Computers Form [see Appendix] before access to the computer systems will be made available to the user. Refusal to sign the form will result in the employee not receiving computer system access and possible disciplinary action.

SECTION2

USE OF LOCAL AND WIDE AREA NETWORKS

Once a user receives a network login account to be used to access the network and computer system, they are solely responsible for all actions taken while using that network login account.

REQUESTING A NETWORK LOGIN ACCOUNT

When a new user needs network access, his senior or HR must fill out the New User Request Form and sign it. Applying for a Network login account under false pretences is punishable disciplinary offense.

PROHIBITED ACTIONS

Sharing passwords- sharing your password with any other person is prohibited. In the result that you do share your password with another person, you will be solely responsible for the actions that other person appropriated.

Use of Files- deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.

Changing Resources - altering, or attempting to alter, yours or any other person's system configuration is prohibited. This includes attempting to gain greater access to the system or attempting to access data that you have not been given rights to.

Use of System resources - improper use of system resources (e.g. waste of hard drive space, network bandwidth) can result, after the user is formally warned in writing, in either denial of further access to the further disciplinary action.

Use of Computer System- use of facilities and/or services for commercial or personal purposes is prohibited.

Unauthorised use- any unauthorised, deliberate action which damages or disrupts the computer system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

APPROPRIATE ACTIONS

All users should logout of the network and turn off computer equipment during nonworking hours (i.e. weeknights, weekends, vacations, and holidays). This includes CPUs, monitors, printers and modems.

SECTION 3

SECURITY

As a user of SCMS computer systems, you may be allowed access to other computer systems belonging to SCMS or otherwise. This policy is used to describe types of security and prohibited actions regarding those computer system security also.

Computer Security Defined

Physical Security-this is the action taken to ensure that the computer system components (CPU, monitor, keyboard, mouse, modem, printer, etc.) are secure and not easily available by non –SCMS personnel. Physical security is the responsibility of the head of the department.

Access Security- this is the action taken by the user to ensure that the computer system data is not compromised or made available to unauthorised personnel within and outside SCMS.

Prohibited Actions

Accessing the use of computer system and/or networks in attempts to gain unauthorised access to remote systems is prohibited. The use of computer systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system or local system, is prohibited.

Passwords-decryption of system or user passwords, or any other method used in an attempt to gain unauthorised access to the computer systems, is prohibited.

System files- the copying or transferring of system files is prohibited. The copying of copyrighted materials, such as third-party software is prohibited.

Unauthorised use- intentional attempts to “crash” network systems or programs is prohibited. Attempts to secure a higher level of privileges on any computer system are prohibited.

Viruses- the wilful introduction of computer viruses or other disruptive/destructive programs into any SCMS computer system, or any external computer system, is prohibited. The unintentional introduction

of a computer virus or other disruptive/destructive programs into any SCMS computer system, or any external computer system, by the failure to follow SCMS will result in disciplinary action.

SECTION 4

ELECTRONIC MESSAGING SYSTEMS

This policy defines the framework for use of electronic message systems and communications media by employees of SCMS. This includes but is not limited to, electronic mail systems (e.mail), voice mail systems, calendar scheduling systems, faxes, internet and other electronic media that generate, store, transmit and display correspondence for internal and external business communication purposes.

(Note: if possible should include mobile also.)

DEFINITIONS

COMMUNICATIONS is defined as a system for sending and receiving messages, as by mail and telephone.

MEDIA is the plural of medium which is defined as agent by which something is conveyed, accomplished, or transferred.

COMMUNICATION MEDIA is that aspect of electronic messaging that contains the message.

EMPLOYEE is a person who is a permanent employee, temporary employee, contractor, student, intern or otherwise engaged at SCMS and has been given authorised access to any electronic messaging system.

ENCRYPTION is a method of “scrambling” data using cryptographic algorithm based on a secret key that is known only to the originating system and the destination system.

SECURING A DEVICE means to log off the network, invoke a keyboard locking feature requiring a password, or otherwise make the device inaccessible.

ELECTRONIC MESSAGING SYSTEMS EXPECTED USE

SCMS will provide electronic messaging systems , making them available to SCMS Associates/ employees as required subject to resources and other limitations. Employees with assigned access to electronic messaging systems are expected to use them

Employees with access to electronic messaging systems are expected to check for messages on a frequent and regular basis and respond within a reasonable time as needed. An employee's use of SCMS –provided communications media is restricted.

Employees are expected to use SCMS provided communications media only for SCMS business. However, the SCMS recognizes the occasional need to exchange personal messages. These should be kept to a minimum, both in number and length. At no time should personal messages be sent in a way that charges the SCMS for transmission.

Employees shall not use SCMS provided communications media in a fashion that constitutes or involves any unlawful activity including but not limited to:

a) Discrimination on the basis of race, creed, colour, sex, age, national origin, marital status, religion, disability, sexual orientation or veteran's status;
b) Harassment, sexual and otherwise.
c) Copyright infringement.
d) Expression of an employee's personal political beliefs or personal business interests.

Electronic communications resources are limited and employees must manage their allotted resources in a responsible manner. This includes but it not limited to deleting old messages and downloading e-mail messages to diskettes for long-term storage.

CONFIDENTIALITY

SCMS-owned electronic messaging systems will provide data confidentiality and integrity. Employees must use reasonable means to minimise unauthorised access to electronic messages.
Employees are responsible for protecting messages from unauthorised access by maintaining password confidentially and by securing the communications device to the extent possible before leaving it unattended.

Confidential and sensitive written information must be encrypted before transmitting electronically. This applies to information sent within the SCMS and especially information sent to external agencies.

ELECTRONIC MESSAGING PRIVACY

All SCMS information technology resources, including electronic messaging systems and files are the property of SCMS. The SCMS may, under certain circumstances and during normal business functions, access an employee's electronic messages without authorisation from the employee.

SENDING OF ELECTRONIC MESSAGES GLOBALLY

Electronic messages conform to all applicable statutes and regulations governing public records, records retention, and public disclosure. E-mail messages can only be stored for a limited time on the system. If an e-mail message needs to be preserved, it should be moved into media storage. Information requiring longer retention should be printed and stored as hard copies.

SECTION 5

INTERNET ACCESS

The internet, when used appropriately, is an extremely valuable tool for SCMS staff. It offers direct access to numerous agencies and organisations whose publication and information are sought by staff on a daily basis. Its use enables staff to locate materials without leaving their workstation. In addition, more elusive information can often be located in a highly time efficient manner by subject searching on the internet or querying a list server. It benefits SCMS to provide direct access to the internet to employees; contractors and volunteers who can use it to better perform their jobs.

DEFINITIONS

INTERNET – worldwide network of networks and computers.
HACKING- attempting to break into another system on which you have no account, and is treated as malicious intent.
NETIQUETTE – a word made from combining "network Etiquette" which is the practice of good manners in a network environment.
FLAME WARS- angry e-mail exchanges.
SURFING-random internet browsing, normally not work related.

GUIDELINES

When accessing the internet, employees are representing SCMS, therefore all rules of conduct and law that apply in your regular workplace also apply on the internet.

SCMS has the right to review user accounts; workstations and file sever space in order to make determinations on whether specific uses of the information systems are appropriate.
SCMS has the right to review the personal user accounts of all employees if the user accounts are being operated in the workplace.
SCMS may revoke an employee's, contractors or volunteer's access to the network and network services when there has been a clear violation of acceptable use principles and guidelines. In addition, where violations occur, employees, contractors and volunteers are subject to any disciplinary or corrective actions or penalties proscribed in law, rule or policy.

ACCEPTABLE USES OF THE INTERNET

SCMS encourages appropriate use of on-line resources. Acceptable uses include, but are not limited to:
* facilitating communication with other agencies or business partners,
* facilitating discussions aimed at professional development,
* gathering information on industry trends,
* use in grant related activities,
* legal and policy research,
* gaining timely access to government publications and statistics, and
* generally advancing the information needs of the organisation.

PROHIBITED USES OF THE INTERNET

Inappropriate behaviour may result in disciplinary actions ranging from verbal warnings to termination of network services and/or employment with SCMS . The severity of the misbehaviour governs the severity of the disciplinary action. Inappropriate on-line behaviour in the workplace would include, but is not limited to:
* Unauthorised attempts to break into any computer whether of SCMS or another organisation (hacking),
* Using SCMS time equipment and/other resources for non-work-related activity, personal gain or recreation,
* Sending threatening messages,
* Sending racially and/or sexually harassing messages,
* Theft, or copying, of electronic files without permission,
* Sending or posting SCMS confidential materials outside SCMS, or posting SCMS confidential material inside SCMS to non-authorised personnel,
* Sending chain letters through electronic mail,
*" surfing" pornographic and sexually oriented sites,
* Random "surfing" and "flame wars".

INTERNET ACCESS AUTHORIZATION

Access to the internet will be provided to SCMS employees, contractors and volunteers when deemed appropriate for their work. This is at the discretion of the department head or elected official for their department subject to resources and other limitations.

Use of computer and network

SCMS, or its authorised representatives, may monitor, review, and/or copy any information on the electronic data processing system, including the electronic mail system, whether stored or in transit, at any time, and may, without further notice, disclose such information to any third party or parties, including government and law enforcement agencies.

PREVENTION OF UNAUTHORISED ACCESS

Uses will maintain the confidentiality of system password and will not permit access to the network account or to the electronic mail account by any person unless the immediate supervisor has approved such access in advance. If the password is disclosed to any other individual, for whatever reason, or if to the knowledge of the users the security of the account is otherwise breached, it will immediately be notified to the IRT.

Enforcement:-

Any employee found to have violated this policy may be subject to disciplinary action: -

(a) A memo showing the reason for disciplinary action shall be served and explanation sought for the same.
(b) Withdrawing the access to IT infrastructure for a period not exceeding 28 days.
(c) The damage caused shall be investigated and evaluated.
(d) If the explanation is formed not satisfactory or in the event of the breach to the identified as illegal is against state/central laws.
    (i) Suspension of services.
    (ii) Immediate terminate.

As may be decided for the management shall be affected upon.

User Manual- Brief Summary

System: -

- Can access system using the Username and the Password only.
- Every user is responsible for his Username and Password
- Shall not copy, alter or delete data for the official resources without consent
- Shall not attempt to gain access to open user ID's.

- Shall not bring in unrelated data/software from external resources.
- Any external devices brought in shall the submitted to security check before introducing the use to the computer resources.
- Sharing passwords-sharing your password with any other person is prohibited. In the result that you do share your password with another person, you will be solely responsible for the actions that other person appropriated.
- Use of Files- deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
- Changing Resources- altering, or attempting to alter, yours or any other person's system configuration is prohibited. This includes attempting to gain greater access to the system or attempting to access data that you have not been given rights to.
- Use of System resources- improper use of system resources (e.g., waste of hard drive space, network bandwidth) can result, after the user is formally warned in writing, in either denial of further access to the further disciplinary action.
- Use of Computer System- use of facilities and/or services for commercial or personal purposes is prohibited.
- Unauthorised use- any unauthorised, deliberate action which damages or disrupts the computer system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

Internet:-

- Shall use the internet connection only for official purpose.
- Shall refrain from browsing personal sites.
- Shall refrain from downloading unofficial contents.
- Shall refrain from accessing internet from the resources other than those meant to do so.
- Unauthorised attempts to break into any computer whether of
- SCMS or another organisation (hacking),
- Using SCMS time equipment and/other resources for non-work-related activity, personal gain or recreation,
- Sending threatening messages,
- Sending racially and/or sexually harassing messages,
- Theft, or copying, of electronic files without permission,
- Sending or posting SCMS confidential materials outside SCMS, or
- Posting SCMS confidential material to non-authorised personnel,
- Sending chain letters through electronic mail,
- " surfing " pornographic and sexually oriented sites,
- Random "surfing" and "flame wars".

Email:-

- Shall not send official data to personal ID.
- Shall declare the personal e-mail ID used, if any in the official premises/resources
- Shall produce any personal e-mail ID for screening whenever asked for if it is used in the official resources/premises.

- Discrimination on the basis of race, creed, colour, sex, age, national origin, marital status, religion, disability, sexual orientation or veteran's status.
- Harassment, sexual and otherwise
- Copyright infringement
- Expression of an employee's personal political beliefs or personal business interests.

Revision History

Policy is in effect on 01/11/2022
Document revised on 28/10/2022