SRI MUTHUKUMARAN MEDICAL COLLEGE HOSPITAL AND RESEARCH INSTITUTE

Title:	IT Policy		
Policy No.:	18	Issue No.:	001
No.of pages:	27	Date:	02.02.2022
Effective from:	02.02.2022	Next revision:	01.02.2026

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

IT POLICY

Introduction:

The Center for Technical Support (CTS) adheres to the SMMCHRI Data Processing and Telecommunications Resource Use Policy. The IT policy process also includes an annual review of existing policies and selection of those policies to be reviewed for compliance with SMMCHRI.

Every member of the SMMCHRI community is bound by these policies and is expected to be thoroughly familiar with them. Violators will be subject to the full range of disciplinary sanctions, up to and including expulsion or termination.

In order to retain necessary flexibility in the administration of policies, the SMMCHRI reserves the right to interpret, revise, or delete any of the provisions of these policies as the SMMCHRI deems appropriate in its discretion.

Need for IT Policy:

The purpose of an IT policy is to guide and provide information about acceptable and prohibited actions or rule violations. The guidelines are created and provided to help the organization, SMMCHRI community departments and individuals understand how institutional policies are implemented in some important areas and to harmonize reported practices.

IT policies may be classified into following groups:

- Acceptable Use Policy
- Hardware and Software Procurement Policy
- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- SMMCHRI Database Use Policy

Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- Network Administrators

It may be noted that SMMCHRI IT Policy applies to technology administered by the institution centrally or by the individual departments, to information services provided by the SMMCHRI

administration.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the Institution, hostels and guest houses, or residences wherever the network facility was provided by the Institution. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the SMMCHRI IT policy.

Resources

- Network Devices
- Wired/wirelessInternet Access
- Official Websites
- Web applications
- Official Email services
- Data Storage
- Mobile / Desktop / Server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

EMPLOYEE ACCEPTABLE USE POLICY

Purpose

Access to computer systems and networks owned or operated by SMMCHRI imposes certain responsibilities and obligations and is granted in accordance with institutional policy. Acceptable use must be ethical, reflect academic integrity and show moderation in the consumption of shared resources. It shows respect for intellectual property rights, data ownership, system security mechanisms, and the rights of individuals to privacy and protection against intimidation and harassment.

Policy Statement

Sharing of passwords, PINs, tokens or other authentication information is strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).

Use of SMMCHRI resources for, continuation of, or other participation in activities contrary to the mission of the agency is prohibited. This includes, but is not limited to: illegal activity, overtly sexual material, hate speech, violent behavior and harassment, spamming, hacking, etc. If consistent with SMMCHRI, an exemption applies to individuals engaged in regular teaching or research activities. mission.

In addition to standard electronic resources, members of the Institution community are expected to make appropriate use of the Institution Telephone system. Examples of inappropriate actions:

Unauthorized use of another individual's identification and authorization code
Use of the Institution telephone system to send abusive, harassing, or obscene messages

The use of SMMCHRI resources to conduct business for personal financial gain is prohibited.

Anti-virus and anti-malware software must be installed on your computer, kept up to date and currently enabled. If your software is not up to date or disabled it may lead to an infection which may result in your network access being disabled.

While CTS deploys Windows patches to facility equipment, employees are responsible for keeping their computers up to date with all other related software update service security fixes/patches. This includes updating applications such as MS Office, Adobe, iTunes, Firefox, Chrome, etc. This also includes operating system fixes for non-institutional devices. If your computer is not updated, it can lead to a malware infection that can block your network connection.

Employees are responsible for their computer, including its hardware, software, and any network traffic transmitted by it. Please contact Centre for Technical Support (CTS) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.

The use of personal routers (wireless or wired) and/or DHCP servers outside of a contained lab environment is strictly prohibited. CTS will assist you if you require additional connectivity.

Using the institution network to provide any service that is visible off campus without prior CTS approval, is prohibited. This applies to services such as, but not limited to, HTTP

(Web), SSH, FTP, IRC, email, private VPN, etc.

Configuring your computer to provide Internet or SMMCHRI network system access to anyone whois not a SMMCHRI faculty, staff member or student is prohibited.

Connecting any device or system to the institution data networks without the prior review and approval of CTS is prohibited.

STUDENT ACCEPTABLE USE POLICY

Purpose

Access to computer systems and networks owned or operated by SMMCHRI imposes certain responsibilities and obligations and is granted in accordance with institutional policy. Approved use must be ethical, Academic integrity and moderation in the use of shared resources. It respects intellectual property, data property, system security mechanisms and the rights of individuals to privacy and freedom from intimidation and harassment.

Policy Statement

Sharing of passwords, PINs, tokens or other authentication information are strictly prohibited.Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).

The use of SMMCHRI resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behaviour & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with SMMCHRI mission.

The use of SMMCHRI information systems for commercial gain is prohibited.

Anti-virus and anti-malware software must be installed on your computer, kept up to date and currently enabled. If your software is not up to date or disabled it may lead to an infection which may result in your network access being disabled.

Students are responsible for keeping their computer updated with security patches/fixes from the appropriate software update services (Windows Update on windows computers, Software Update on

Apple computers). This includes updating applications, such as MS Office, Adobe, iTunes, or Firefox. If your computer is not up to date it may lead to virus infection which may result in your network access being disabled.

Students are fully responsible for their computer, including its hardware, software, and any network traffic transmitted by it, regardless if this traffic was authorized by you or not. Please contact Centre for Technical Support (CTS) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.

The use of personal routers (wireless or wired) and/or DHCP servers is strictly prohibited.

Using the institution network to provide any service that is visible off campus is prohibited. This applies to services such as, but not limited to, HTTP (Web), FTP, IRC, peer-to-peer (p2p) multimedia sharing, game servers and email.
Configuring your computer to provide Internet or SMMCHRI network system access to anyone who is not an authorized SMMCHRI faculty, staff member or student is prohibited.
Connecting standard mobile devices used for the pursuit of academic work to SMMCHRI wireless network is permitted. Connecting any other device or system to the institution data networks without the prior review and approval of CTS is prohibited.

Some examples of policy violations:

- Accessing another user's personal private data
- Consuming a disproportionate amount of bandwidth
- Attempting or coordinating a denial-of-service attack
- Probing and/or exploiting security holes in other systems either on or off campus
- Using unauthorized IP addresses
- Using a network protocol analyzer or similar mechanism without prior authorization
- Degrading or restricting network access for others, either on or off campus
- Connecting to Institution systems that one has not been expressly permitted to access
- Downloading, sharing or using copyrighted material including music, movies, software or
- text books
- Participating in activities which are not consistent with the Mission of the institution

In addition, your network access may be disabled if SMMCHRI receives complaints about or otherwisedetects inappropriate behavior.

VENDOR ACCEPTABLE USE POLICY

Policy Statement

Vendor agrees to develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, security, integrity and availability of all maintained or transmitted SMMCHRI data.

Vendor agrees to only use SMMCHRI data, systems, resources, integrations, and access solely for the original purpose for which it was intended as stipulated in any contract which exists between Vendor and SMMCHRI.

Vendor will not mine SMMCHRI data for any purpose whether internal or external to Vendor Company.

Vendor will not share SMMCHRI data with any third party, without express permission of the Institution in writing.

Vendor agrees to use SMMCHRI data, systems, resources, integrations and access in a manner whichis consistent with the Mission of the institution.

Vendor agrees to comply with all local laws as they apply to SMMCHRI systems and data.

Vendor agrees to be knowable about and comply with all other SMMCHRI policies.

The use of SMMCHRI resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behaviour & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with SMMCHRI mission.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

NETWORK SECURITY POLICY

Purpose

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access and performance for the Institution community. This policy is necessary to provide a reliable campus network to conduct and prevent unauthorized access to institutional, research or personal data. In addition, the Institution has a legal responsibility to secure its computers and networks from misuse.

Addressing and Domain Services

Centre for Technical Support (CTS) is solely responsible for managing any and all Internet domain names related to SMMCHRI. Individuals, academic Schools/Departments or administrative departments may not create nor support additional Internet domains without prior approval from CTS.

To ensure the stability of network communications, CTS will solely provision and manage both the public and private IP address spaces in use by the Institution.

CTS may delegate administrative responsibilities to individuals for certain network ranges, but retains the right of ownership for those networks.

Network Connections

SMMCHRI faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system to the Institution networks without the prior review and approval of CTS.

Schools, Centers and Departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the Institution must obtain prior approval from CTS.

In order to maintain reliable network connectivity, no other department may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus without prior review and approval of CTS.

Users are permitted to attach devices to the network provided that they are: for use with normal Institution or student operations, do not interfere with other devices on the network are in compliance with all other SMMCHRI policies.
Unauthorized access to Institution networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with Institution network equipment.

Unauthorized access to Institution equipment/cabling rooms is also prohibited. Wireless

Centre for Technical Support (CTS) is solely responsible for providing wireless networking services on campus. No other department may deploy wireless routers, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus.

CTS is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.

The Institution will maintain a campus wireless network based only on IEEE 802.11 standards. CTS will collaborate with academic departments where devices used for specific educational or research applications may require specific support or solutions.

CTS will provide a general method for network authentication to Institution systems. The IEEE 802.1x standard is the currently supported authentication method. Additional security protocols may be applied as needed.

All users of wireless network resources at SMMCHRI are subject to the applicable Network Acceptable Use Policy. Users of wireless resources at SMMCHRI agree to have read and be bound by the terms and conditions set forth in that policy.
External Traffic, Services and Requests

CTS will take action to prevent spoofing of internal network addresses from the Internet. CTS will also take action to protect external Internet sites from source address forgery from devices on the Institution network.

The default policy of an educational institution's external Internet firewall is to block all external Internet traffic to the educational institution's network unless specifically authorized. To facilitate

this, academic schools, centers and departments, and other administrative entities must register systems with CTS that require access from the Internet. Users who want to request access through the educational institution's firewall must open a help ticket and fill out a firewall request.
Access and service restrictions may be enforced by Device, IP address, Port number or Application behavior.

CTS reserve the right to decrypt SSL traffic which transits the Institution network.

Network Security

CTS can investigate unauthorized access to computer networks, systems or equipment. CTS will work with academic or administrative departments and law enforcement as needed. All network devices must be installed/maintained and configured and maintained with adequate security to prevent unauthorized access or misuse. If a security issue is observed, it is the responsibility of all SMMCHRI users to report the issue tothe appropriate supervisor or CTS for investigation.

CTS reserve the right to quarantine or disconnect any system or device from the Institution network at any time.

Network usage judged appropriate by the Institution is permitted. Some activities deemed inappropriate include, but are not limited to:

Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCPor DNS servers; or a computer set up to act like such a device.

- Engaging in network packet sniffing or snooping.
- Setting up a system to appear like another authorized system on the network (Trojan).
- Other unauthorized or prohibited use under this or any other Institution policy.
- Students may consult the Student Acceptable Use Policy for further information.

Employees may consult the Employee Acceptable Use Policy for further information.

Enforcement

Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the Institution network. CTS may subsequently require specific security

improvements where potential security problems are identified before the device may be reconnected.

Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.

The Institution reserves the right to test and monitor security, and to copy or examine files and information resident on institution systems related to any alleged security incident or policy violation.

Monitoring and Auditing

CTS will maintain and monitor traffic logs for all network devices and systems for security auditing purposes.

CTS reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a Institution policy violation, criminal activity, monitoring required by law enforcement or with appropriate management request. Reasonable cause may be provided by the complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of CTS staff.

CTS may perform penetration testing of any Institution owned devices or systems on its networks in order to determine the risks associated with protecting Institution information assets. CTS may further perform non-intrusive security audits of any system or device attached to the Institution's networks in order to determine what risks that system may pose to overall information security.

EMAIL USE POLICY

Summary

This policy covers appropriate use of any email sent from SMMCHRI email address and applied to allEmployees, Students.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Guidelines

SMMCHRI email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual

orientation, religion, or national origin. Employees who receive any emails with this content from any SMMCHRI employee should report the matter to the Registrar/Dean – SMMCHRI immediately.

All email sent or received from a SMMCHRI server must comply with the Acceptable Use Policy.

Violations of this policy will be handled in accordance with SMMCHRI policies and procedures.

Employees

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the Institution's administrators, it is recommended to utilize the SMMCHRI e-mail services, for all formal SMMCHRI communication and for academic & other official purposes.

Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institution communications are official notices from the Institution to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institution messages, official announcements, etc.

Users may be aware that by using the email facility, the users are agreeing to abide by the followingpolicies:

- The facility should be used primarily for academic and official purposes and to a limited extentfor personal purposes.

- Using the facility for illegal/commercial purposes is a direct violation of the SMMCHRI 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 keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially whenthe incoming mail contains 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 damage the valuable information on your computer.

- Users should configure messaging software (Outlook / Thunderbird client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

HARDWARE AND SOFTWARE PROCUREMENT POLICY

Policy

The procurement of all computing and communication hardware and software is coordinated by the office of Centre for Technical Support (CTS) in order to maximize investment in Information Technology (IT).

To take advantage of IT tools in the most cost-effective manner possible, the SMMCHRI has standardized a series of hardware and software products that integrate easily with the Institution's IT infrastructure. An up-to-date list of supported hardware and software is available from CTS. When considering the purchase of hardware or software, departments should choose products from this list and coordinate their purchase with CTS.

While the acquisition of standard products is encouraged, some departments have need for special equipment or software not included in the list of supported products. CTS will consult with the department to select the most appropriate equipment and to work out an agreement for continued support.

Departments who choose to buy IT resources not approved by CTS are responsible for their implementation and ongoing maintenance. CTS will not be responsible for interfacing such

hardware or software to the campus network or information repository.

IT HARDWARE INSTALLATION POLICY

Institution 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.

Who is 'Primary' User?

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

What are End User Computer Systems?

Apart from the client PCs used by the users, the institution will consider servers not directly administered by CTS, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the CTS, are still considered under this policy as "end- users" computers.

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract either with a third party or with support from CTS. Such maintenance should include OS re-installation and checking virus related problems also.

Power Connection to Computers and Peripherals

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, as continuous power supply to UPS is requiredfor battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

Network Cable Connection

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 thecomputer and its peripherals are connected.

File and Print Sharing Facilities

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.

Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written intimation to the CTS, as CTS maintains a record of computer identification names and corresponding IP address.

Such computer identification names follow the convention that it comprises building name abbreviation and Room No. As and when any deviation (from the list maintained by CTS) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs CTS in writing/by email, connection will be restored.

Maintenance of Computer Systems provided by the Institution

For all the computers that were purchased by the institution centrally and distributed by the Purchase Department, CTS Department will attend the complaints related to any maintenance related problems.

SOFTWARE INSTALLATION AND LICENSING POLICY

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, Institution IT policy does not allow any pirated/unauthorized software installation on the institution owned computers and the computers connected to the institution campus network. In case of any such instances, institution will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Operating System and its Updating

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 Microsoft Windows computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides 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.

Institution as a policy encourages user community to go for open-source software such as Windows, Open office to be used on their systems wherever possible.

Any MS Windows OS based computer that is connected to the network gets OS patch free updates from the central server located in the Data Centre. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is user's responsibility to make sure that the updates are being done properly.

Antivirus Software and its updating

Computer systems used in the institution should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

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.

Backups of Data

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. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on DVD, Flash Drive or other storage devices.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

WEB SITE HOSTING POLICY

Policy

SMMCHRI Chennai has an official website chennai.vit.ac.in or the public access. Schools, Centers and Departments of Teachers / Employees / Students may have pages on SMMCHRI's official Web page. Official Web pages must conform to the Institution Web Site Creation Guidelines for Website hosting. As on date, the Web Team at CTS is responsible for maintaining the official website of the institution.

Responsibilities of Centre for Technical Support (CTS)

Campus Network Backbone Operations

The campus network backbone and its active components are administered, maintained and controlled by CTS.

CTS operates the campus network backbone such that service levels are maintainedas required by the Institution Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

Physical Demarcation of Campus Buildings Network

CTS is responsible for the physical connectivity of campus buildings already connected to the campus network core. CTS is responsible for physically mapping newly constructed buildings to the "core network". In practice, this means that where the fiber backbone reaches buildings, CTS terminates. CTS is also responsible for how the building is connected to the campus network core (whether the connections must be fiber optic, wireless or other media).It is the institution's policy not to actively monitor Internet activity on the network, sometimes it is. it is necessary to investigate such activity when a problem occurs or the institution When optimizing Internet connection traffic.

Network Expansion

Major network expansion is also the responsibility of CTS. Network expansion will be carried out by CTS when the institution makes the necessary funds available based on the requirement.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Wireless Local Area Networks

Where access through Fiber Optic/UTP cables is not feasible, in such locations, CTS considers

providing network connection through wireless connectivity.

CTS is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from CTS prior to implementation of wireless local areanetworks.

CTS is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

Global Naming & IP Addressing

CTS is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. CTS monitors the network to ensure that such services are used properly.

Providing Net Access

By default, all the faculty members are given internet access in their official laptops. However, in case the official laptops are not given to the faculty, net access is given to their personal laptops only after installing Institution AV agent in their laptop.

Research scholars can request internet access by sending an e-mail to systems@vit.ac.in marking a copy of the e-mail to their guide. Internet is enabled only if the Institution AV installed. CTS is authorized to remove internet access at any point in time in case if the scholar is found to be misusing the facility given. Misusing means, removal of AV installed by the Institution, abnormal download using web crawlers or by proxy tools or any such unethical activity.

Network Operation Center

CTS is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available 12hours a day, 7 days a week. All network failures and excess utilization are reported to the CTS technical staff for problem resolution.

CTS routinely monitors campus-wide network traffic in both intrusive ways. If traffic patterns indicate that system or network security, integrity or network performance has been compromised, CTS will analyze network traffic for violating activities or devices will be identified and security

restrictions will be applied until the situation is resolved or the problem is resolved. During this process, if necessary, a message is sent to higher authorities if the crimes are of a very serious nature.

Guidelines for Desktop Users

These guidelines are meant for all members of the Institution Network User Community and users ofthe Institution network. Due to the increase in hacker activity on campus, Institution IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

All desktop computers should have the latest version of antivirus such as K7 Anti-Virus (PC) and should retain the setting that schedules regular updates of virus definitions from the central server.

When a desktop computer is installed, all operating system updates and patches should be applied.In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.

All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.

The password should be difficult to break. Password, defined as:

- must be minimum of 6-8 characters in length
- must include punctuation such as! % & * , . ? + -=
- must start and end with letters
- must not include the characters # @ ' " `
- must be new, not used before

Avoid using your own name, or names of your wife or children, or name of your department, or Room No. or House No & etc.

Passwords should be changed periodically and also when suspected that it is known toothers.

Never use 'NOPASS' as your password. Do not leave password blank and

DEAN
SRIMUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Make it a point to change default passwords given by the software at the time ofinstallation

The password for the user login should follow the same parameters outlined above.
The guest account should be disabled.
New machines with Windows XP should activate the built-in firewall.
All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.
When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.
All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).
Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

In addition to the above suggestions, CTS recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise.

Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

If a machine is compromised, CTS will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.

VIDEO SURVEILLANCE POLICY

The system includes: Fixed cameras; Pan Tilt and Zoom cameras; Screens: multiplexers; digital recorders; SAN/NAS storage; Public information signs.The cameras will be placed at strategic points on the campus, mainly at the entrances and exits of objects and buildings. No cameras are hidden and anyone is prohibited from focusing on the facades or rear of a private building.Signs

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

will be placed in strategic locations and prominently at campus entrances and exits to inform staff, students, visitors and the public that a CCTV/IP camera is in use. Although every effort has been made to ensure maximum system performance, it is not possible to guarantee that the system will detect all events within the range.

Purpose of the system

The system has been installed by institution with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

The Security Control Room

The images taken by the system are monitored and stored in a security control room, or "monitor room". The monitors are not visible from outside the control room. Unauthorized access to the control room is not permitted at any time. Access is strictly limited to teachers, authorized members of senior management, police and other persons with legal access rights. Employees, students and visitors may enter the control room on a case-by-case basis and only with the written permission of the Dean/Vice Principal Admin. In an emergency and where prior authorization cannot reasonably be obtained, individuals may be admitted to the control room for a legitimate reason.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Security Control Room Administration and Procedures

Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

Recording

Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

Images will normally be retained for 20 to 30 days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

All hard drives and recorders shall remain the property of institution until disposal and destruction.

Complaints

It is recognized that members of Institution and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Chief Security Officer.

MAINTENANCE POLICY – SYSTEMS & NETWORK

Lab System Maintenance Policy

Lab systems are maintained by the Lab assistant. Primary level problems are taken care by Lab assistant.

- Power connections

- Booting problem
- Network problem
- Software installation / uninstallation
- Hardware troubleshoots
- Hardware replacement
- Time schedule Internet maintenance.
- Clearing the Junks and cache through CCleaner.
- Major Network, Software and Operating system related Problem are taken care by CTS Staff

Standalone Systems Maintenance Policy

Other than lab systems are maintained by CTS staff, notably like Deans, Directors, Secretary, Departments, Smart rooms and Auditoriums systems.

Escalation methods:

- CMS ticketing systems
- Email
- Phone call via Extn.
- Direct Mobile
- Official Letters
- Meeting in-person

General problem:

- Power connections
- Booting problem
- Network problem
- Software installation /uninstallation
- Hardware troubleshoots
- Hardware replacement

Clearing the Junks and cache through CCleaner

Network & Surveillance Maintenance:

- Network switch
- Network switch, Wireless Access points, CCTV, Biometric and Digital Medias
- Network switches are configured and installed in required locations
- VLAN creations based on lab and Dept.
- Port security
- Increasing the switch on demand.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Wireless Access points

Access points are placed in staffrooms, smart rooms & Auditoriums and on demand places

Creations of SSID for faculty and common use.

- Channelizing based on users
- Widening the Access points depends on signal coverage.
- Access points are deployed temporarily on demand basis.
- DHCP used to bring the Laptops into the Network
- Internet are provided by binding the MAC address.
- Internet Policy varies depending upon the functionality of the users.
- **Surveillance**

✓ CCTV cameras are erected in the important location in Buildings, Hostels and Roadside.
✓ CCTV configured and installed in the required locations
✓ Bullet and Doom CCTV are used based on the places
✓ Faulty CCTV are serviced and installed.
✓ The video datas are stored for 1 month.
✓ The footage is given on demand by Security team, supported by CTS
✓ The Playback and administration are done by Monitoring software of the Brand.

Policy for online meetings

Any Department / School who needs online meeting facility, need to send a request to Centre for Technical Support department (CTS), well in advance to schedule the meeting and to facilitate online meetings. However, on demand request is also accepted based on the availability of slots. The meetings are facilitated through MS Teams, Zoom & Google meet.

POLICY FOR CONDUCTING CONFERENCE / WORKSHOPS FORLARGER AUDIENCE

College/Centres are encouraged to use either Microsoft Teams Live Event (or) Zoom integrated with YouTube and Facebook to reach the larger audience. A formal official email communication will be sent to CTS department to facilitate with the approval of Deans / Directors / HODs / Section Heads.

Remote Access & Support Policy

IT support will be given to Faculty, Staff & Students using remote support tools like Any-Desk or Team Viewer.

Usage of Biometric devices during COVID'19

Biometric feature is disabled and enabled the Smart Card / Proximity Card for Access Control Systems and Attendance.

Data Backup and Restore Policy

SMMCHRI has many critical applications that will be backed up periodically so that it can be used in all cases of restore. Centre for Technical Support (CTS) is responsible for ensuring that

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

mission critical applications and data are well preserved and protected against loss and destruction. Adequate backups allow data recovery when information technology systems or information has been destroyed by systemmalfunction or by accidental/intentional action.

Backup & Restore Policy

Every critical/production server is regularly backed up. CTS stores data such as system status data, financial database, file server, production web server, production database server, domain controllers, etc. using appropriate backup methods. Systems and data should be backed up nightly during non-business hours. Copies of all backups are stored in a secure location; offline Backups should not be stored in the same building as live data or systems. Data and recovery processes must be tested frequently. Depending on the assigned daily backup window, appropriate backup methods (ie full, incremental or differential) should be used..

Verification of Backup Status

The designated member of CTS staff must check the backup status on the system first thing everymorning and report any failures to the Assistant Director - Systems. The backup software has automatic verification, which checks data transfer, reports error if occur, immediately corrects those errors and verifies backup data store.

Backup Schedules

Daily backups will be scheduled Monday through Friday outside of working hours. Production databases server will be backed up a minimum two times a day.

Retention of Backups

Backups will be kept on Storage for the following durations.

- ✓ Daily backups [Incremental Backup] 11Hrs
- ✓ Once Weekly backups [Full Backup] Every Saturday 6:00PM.
- ✓ Backup Retention period is 30 days.

Off-site Storage of Backups

All daily, weekly and monthly backups are stored in a secure location. A secure offsite is defined as a physical location far enough away from the CTS to be safe from a data center disaster. The website is protected against environmental hazards and protected against access by other persons.

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.

Replication of Disk Backup Media

Replication of the disk backup media to and from the off-site location will occur automatically based upon the backup software's best practice configuration. CTS staff will be responsible for ensuring thatany disk replication is functioning correctly at all times.

Backup Software

Backup Administrator Responsibilities

Backup administrator is responsible for the following:

- ✓ Checking if the backup has been successfully taken.
- ✓ Troubleshooting and managing backup failure.
- ✓ Maintain backup media: Check the storage for the backup whether it is disks.
- ✓ Maintaining the backup log.

Testing/Validation

CTS performs monthly testing and validation to ensure the accuracy of backups and backups. In random computer systems, small data sets are randomly selected from weekly and monthly backup media and restored in a manner that does not affect production needs. Successful data recovery indicates the correctness of the backup procedures.

Prepared by	Verified by	Approved by
IT manager	IQAC coordinator	Dean

DEAN
SRI MUTHUKUMARAN MEDICAL COLLEGE
HOSPITAL & RESEARCH INSTITUTE
Chikkarayapuram, Near Mangadu,
Chennai-600 069.