Information and Communication Technology (ICT)

Maintenance Policy

Sreenidhi Institute of Science and Technology

Yamnampet, Ghatkesar, Hyderabad

Table of Contents

SNIST IT Policy

Information and Communication Technology (ICT) maintains the policies governing the use of SNIST computing and IT communication resources. The IT Policy process also includes an annual review of existing policies and a selection of those policies to be audited for verification of compliance within the SNIST.

Every member of the SNIST 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.

Need for IT Policy

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of the SNIST community to understand how institution policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

- **Acceptable Use Policy**
    a. Employee Acceptable Use Policy
    b. Student Acceptable Use Policy
    c. Vendor Acceptable Use Policy
    d. Network Security Policy
        i. Addressing and Domain Services
        ii. Network Connections
        iii. Wireless
        iv. External Traffic, Services and Requests
        v. Network Security
        vi. Enforcement
        vii. Monitoring and Auditing
    e. Email 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

Further, the policies will be applicable at two levels:

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

All the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the SNIST IT Infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by SNIST by any institution member may even result in disciplinary action against the offender by the institution authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

- Students: UG, PG, Research
- Employees (Permanent/Temporary/Contractual)
- Faculty
- Administrative Staff (Non-Technical /Technical)
- Higher Authorities and Officers
- Guests

Resources

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

Acceptable Use Policy

An Acceptable Use Policy is a set of rules applied by the owner, creator or administrator, Schools, Centers, Departments, internet service providers, and website owners, often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

Employee and Student Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by SNIST impose certain responsibilities and obligations and is granted subject to institution policies. Acceptable use must be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment.

Policy Statement

1. 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).

2. The use of SNIST 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 SNIST mission.

3. 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:

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

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

5. 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.

6. Although ICT deploys Windows patches for Institution issued devices, employees are responsible for keeping their computer updated with all other security patches/fixes from the appropriate software update services. This includes updating applications, such as MS Office, Adobe, iTunes, Firefox, Chrome, etc. This also includes operating system patches for non-institution devices. If your computer is not up to date, it could lead to malware infection which may result in your network access being disabled.

7. Employees are responsible for their computer, including its hardware, software, and any network traffic transmitted by it. Please contact Information and Communication Technology (ICT)) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.
8. The use of personal routers (wireless or wired) and/or DHCP servers outside of a contained lab environment is strictly prohibited. ICT will assist you if you require additional connectivity.

9. Using the institution network to provide any service that is visible off campus without prior ICT

approval, is prohibited. This applies to services such as, but not limited to, HTTP (Web), SSH, FTP, IRC, email, private VPN, etc.

10. Configuring your computer to provide Internet or SNIST network system access to anyone who is not a SNIST faculty, staff member or student is prohibited.
11. Connecting any device or system to the institution data networks without the prior review and approval of ICT is prohibited.

Vendor Acceptable Use Policy

Policy Statement

1. 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 SNIST data.

2. Vendor agrees to only use SNIST 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 SNIST.

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

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

5. Vendor agrees to use SNIST data, systems, resources, integrations and access in a manner which is consistent with the Mission of the institution.

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

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

8. The use of SNIST 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 behavior & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with SNIST mission.

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

1. Information and Communication Technology (ICT) is solely responsible for managing any and all Internet domain names related to SNIST (e.g. snist.edu.in). Individuals, academic Schools/Departments or administrative departments may not create nor support additional Internet domains without prior approval from ICT.

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

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

Network Connections

1. SNIST 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 ICT. 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 ICT.

2. 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 ICT.

3. 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 SNIST policies.

4. 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.

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

Wireless

1. Information and Communication Technology (ICT)) 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.

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

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

4. ICT 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.

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

Network Security

1. ICT may investigate any unauthorized access of computer networks, systems or devices. ICT will work with academic or administrative departments and law enforcement when appropriate.

2. All devices connecting to the network must have adequate security installed/maintained and must be configured and maintained in such a manner as to prohibit unauthorized access or misuse.

3. If a security issue is observed, it is the responsibility of all SNIST users to report the issue to the appropriate supervisor or ICT for investigation.

4. ICT reserves the right to quarantine or disconnect any system or device from the Institution network at any time.

5. 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 DHCP or DNS servers; or a computer set up to act like such a device.

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

Email Use Policy

Summary

This policy covers appropriate use of any email sent from SNIST email address and applied to all Employees, Students and Alumni.

Employees

1. 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 SNIST e-mail services, for all formal SNIST communication and for academic & other official purposes.

2. 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.

3. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://www.**gmail.com** with their User **ID** and **password**. On joining every employee gets an official SNIST e-mail ID from HR department. The e-mail ID's are created by Information and Communication Technology (ICT) on a mail communication from HR department.

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.

1. Using the facility for illegal/commercial purposes is a direct violation of the SNIST 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.

2. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

3. 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 when the incoming mail contains large attachments.

4. 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.

5. 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.

6. 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.

7. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

8. 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.

9. Impersonating email account of others will be taken as a serious offence under the SNIST IT security policy.
10. It is ultimately each individual's responsibility to keep their e-mail account free from violations of institution's email usage policy.

11. Any spam mail received by the user into INBOX should not be forwarded to anyone and could be deleted.

Students

Students are given SNIST mail ID under the domain **sreenidhi.edu.in** hosted in G-Suite with unlimited storage space. Students will be able to use all the features offered by google.

Shifting Computer from One Location to another
Computer system may be moved from one location to another with prior written intimation to the ICT, as ICT 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 ICT) 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 ICT 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, ICT Department will attend the complaints related to any maintenance related problems.

ICT/Institution Administration Interface
ICT upon finding a non-compliant computer affecting the network will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the Institution Administration, if applicable. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. ICT will provide guidance as needed for the individual to gain compliance.

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.

A. Operating System and its Updating

1. 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 Micro Soft 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.

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

3. 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.

B. Antivirus Software and its updating

1. 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.

2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

3. 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.

C. Backups of Data

Individual users should perform regular backups of their SNIST 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 foolproof solution. Apart from this, users should keep their valuable data either on Google Drive, DVD, Flash Drive or other storage devices.

Database Use
Policy

This Policy relates to the databases maintained by the institution administration under the institution's e-governance. Data is a SNISTal and important Institution resource for providing useful information. Its use must be protected even when the data may not be confidential.

SNIST has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the institution's approach to both the access and use of this institution resource.

A. **Database Ownership:** SNIST is the data owner of all the Institution's institutional data generated in the institution.

B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute Institution's database. They may have custodianship responsibilities for portions of that data.

C. **Data Administrators:** Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The institution's data policies do not allow the distribution of data that is identifiable to a person outside the institution.

2. Data from the Institution's Database including data collected by departments or individual faculty and staff, is for internal institution purposes only.

3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies the institution makes information and data available based on those responsibilities/rights.

4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the Institution Registrar.

5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the Institution and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the Institution Registrar for response Tampering of the database by the department or individual user comes under violation of IT policy.

Tampering includes, but not limited to:

- Modifying/deleting the data items or software components by using illegal access methods.
- Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/departments.
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.

Such data tampering actions by institution member or outside members will result in disciplinary action against the offender by the institution authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

Responsibilities of Information and Communication Technology (ICT)

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by ICT.
2. ICT operates the campus network backbone such that service levels are maintained as required by the Institution Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of ICT.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of ICT. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the ICT. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of ICT.
3. It is not the policy of the Institution to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the Institution's Internet links.

C. Network Expansion

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

D. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations ICT considers providing network connection through wireless connectivity.
2. ICT is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from ICT prior to implementation of wireless local area networks.
3. ICT 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.

.

E. 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.

F. Global Naming & IP Addressing

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

G. 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@SNIST.ac.in marking a copy of the e-mail to their guide. Internet is enabled only if the Institution AV installed. ICT is authorized to remove internet access at any point in time incase 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.

H. Network Operation Center

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

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the ICT. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, ICT will analyze the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

ICT is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

J. Receiving Complaints

ICT may receive complaints from departments/schools/any user, if any of the networks related problems faced by them during the course of using the infrastructure. Such complaints should be by using the ticketing system available in the intranet portal or people orbit. However, users may register their complaint using email/phone call also. ICT Technical staff coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

ICT will be responsible only for solving the Hardware/Software/network related problems or services related to the Hardware/Software/Network only.

L. Disconnect Authorization

ICT will be constrained to disconnect any Section, department, or division from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Section, department, or division machine or network, ICT endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, ICT provides the conditions that must be met to be reconnected.

Guidelines on Computer Naming Conventions

1. In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network. All computer names on the campus network must use the Institution standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of ICT.
2. All the computers should follow the standard naming convention

Guidelines for running Application or Information Servers

Running Application or Information Servers

1. Section/Departments may run an application or information server.
2. Individual faculty, staff or students on the SNIST campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the SNIST network.

Responsibilities for Those Running Application or Information Servers

Sections/Departments may run an application or information server. They are responsible for maintaining their own servers.

1. Application or information server content and services must follow content guidelines as described in Institution Guidelines for Web Presence.
2. Obtain an IP address from ICT to be used on the server
3. Get the hostname of the server entered in the DNS server for IP Address resolution. Institution IT Policy's naming convention should be followed while giving the hostnames.
4. Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.
5. Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti- spam etc.
6. Operating System and the other security software should be periodically updated.
7. Sections/Departments may run an application or information server provided they do the following:

    - Provide their own computer, software and support staff
    - Provide prior information in writing to ICT on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization web server, contact the ICT.

Guidelines for Desktop Users

These guidelines are meant for all members of the Institution Network User Community and users of the 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:

1. 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.

2. 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.

3. 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.

4. 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 to others.
    - Never use 'NOPASS' as your password. Do not leave password blank and
    - Make it a point to change default passwords given by the software at the time of installation

5. The password for the user login should follow the same parameters outlined above.

6. The guest account should be disabled.

7. New machines with Windows XP should activate the built-in firewall.

8. 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.

9. 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.

10. 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).

11. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

12. 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.

13. In addition to the above suggestions, ICT 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.

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

15. If a machine is compromised, ICT 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.

16. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, ICT technical personnel can scan the servers for vulnerabilities upon request.

Video Surveillance Policy

A. The system

1. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.
2. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
3. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
4. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

B. 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 contraICT 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

C. The Security Control Room

1. Images captured by the system will be monitored and recorded in the Security Control Room, "the control room". Monitors are not visible from outside the control room.
2. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry.
3. Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons

with a legitimate reason to enter the Control Room.

D. Security Control Room Administration and Procedures

1. 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.

2. 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.

E. 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.

F. Recording

1. Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.
2. 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.
3. All hard drives and recorders shall remain the property of institution until disposal and destruction.

G. Access to images

1. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.
2. Access to images by third parties
3. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:
   - Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
   - Prosecution agencies
   - Relevant legal represe
   - The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
   - People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
   - Emergency services in connection with the investigation of an accident.

H. 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.ystems & Network

<u>Lab System Maintenance Policy</u>

- 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 troubleshoot
    - 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 ICT Staff

Standalone systems Maintenance Policy

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

- Escalation methods:
    - Email
    - Phone call via Extn.
    - Direct Mobile
    - Official Letters
    - Meeting in-person

- General problem:
    - Power connections
    - Booting problem
    - Network problem
    - Software installation /uninstallation
    - Hardware troubleshoot
    - 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.

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. o Access points are deployed temporarily on demand basis. o 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 are given on demand by Security team, supported by ICT
- The Playback and administration are done by Monitoring software of the Brand.

SAP Maintenance Policy

SNIST is based on SAP S/4HANA which is proving to be SAP's most successful ERP system. SAP's involvement with ERP solutions dates back to 1979 when SAP R/2 was launched. In 1992, SAP R/3 was introduced and we have seen improvements as the product has evolved from SAP ERP in 2004 to SAP S/4HANA in 2015.

For implementation, SNIST choose more modern S/4HANA. There are 5 key reasons for which SNIST ERP has been deployed in SAP S/4 HANA.

1. Performance

S/4HANA runs only on SAP HANA, SAP's flagship in-memory computing database. This means that running an SAP solution such as S/4HANA naturally takes advantage of the speed of transaction processing and reporting native to SAP HANA. S/4HANA allows you to experience better performance as it relates to complex and time driven business activities such as real-time planning, execution, reporting and analytics based on live data, as well as prompt period closing and improved forecasting. It also allows you provide a better service level for customer-centric applications.

2. Agility

The end user interface of SAP S/4HANA is completely SAP Fiori driven. This makes the user-friendly rendition of real-time business insights and intelligence on any mobile device a laudable business advantage, anytime and anywhere.

3. Simplicity

SAP S/4HANA brings unparalleled simplicity to the management and administration of the complete IT landscape, and coupled with the cloud adoption potential that it brings to the fore, hardware and network resources have never been so centralized.

4. Reduced Total Cost of Ownership

The adoption of S/4HANA is a cost efficient option when you consider the fact that you are able to combine all the analytical and transactional capabilities of different systems into a single source of truth which drives acute and proactive business making.

5. Innovation

SAP S/4HANA is one of the products from SAP that is driving cloud adoption by businesses. The cloud offers a platform for different software vendors to offer innovative

products that integrates and extends the capability of S/4HANA.

SNIST has incorporated following S/4 Hana modules:

1. FICO

SAP FICO is a module used for financial reporting both externally and internally. The objective is to record all financial transactions30 that are posted by an entity and produce financial statements that are accurate at the end of the trading period. **Full form** or SAP **FICO** stands for FI (Financial Accounting) and CO (Controlling).

2. MM

SAP MM is a key area within logistics as it is tightly integrated with all the components of SAP Logistics module. The important components of SAP MM module are

§ Material Planning

§ Purchasing

§ Inventory Management

§ Vendor Valuation

§ Invoice Verification

§ Statutory Requirements

§ Information System

Procurement Process

§ One of the important process in SAP MM module is Purchasing/Procurement.

§ The purchasing process is initially started when there is a requirement of material/service for the organization.

§ If the material/service can not be obtained from company's internal resource, the responsible person of that company must find the vendor/supplier which can provide it on the required date.

§ The purchasing process is Started with creation of Purchase Requisition (PR), Purchase Order (PO), Good Receipt/Services, Invoice Verification, Payment to vendors.

3. SLCM

SAP SLCM is designed for Higher Education & Research to provide an integrated student lifecycle management and also, support business processes. SNIST is using for maintaining student records, student financials, admissions, student advising, academic structure etc. ALL these activities is available for students by using an application "FIORI".

4. HCM

SAP Human Capital Management (SAP HCM) is an important module in SAP. It is also known as SAP Human Resource Management System (SAP HRMS) or SAP Human Resource (HR). SAP HR software allows you to automate record-keeping processes. It is an ideal framework for the HR department to take advantage of the administration and payroll documents.

5. PM

SAP PM is comprised of components for the three main activities:

· Inspection, which establishes the actual condition of the systems or equipment;

· Preventive maintenance, which helps to maintain ideal conditions for the system or equipment; and

· Repair, for restoring the systems or equipment.

In SNIST all our transportation vehicles is managed by SAP PM.

6. Along with on premise SAP HANA, SNIST is using SAP Success Factors- which is a cloud based platform for managing leaves and other HR activities like new hire, promotion, transfer and new assignment, and other activities in Employee Central.