Table of Contents

1. Need for IT Policy

- The institution's IT policy is implemented to ensure the maintenance, security, and lawful use of the information technology infrastructure established on campus.
- This policy delineates the strategies and responsibilities of the institution for safeguarding the Confidentiality, Integrity, and Availability of the information assets accessed, created, managed, or controlled by the University.
- The IT policy is documented to support fair and transparent academic use of various IT resources available to students, faculty, staff, management, visiting guests, and research fellowship members.

SINCET has established network connections to every computer system across all buildings on campus and in the hostel.

The System Administrator is responsible for managing the institute's intranet and Internet services, which includes overseeing firewall security, DHCP, DNS, email, web, and application servers, as well as the overall network management.

The college previously had a 32 Mbps Internet leased line from Vodafone, which has now been upgraded to a 100 Mbps connection provided by BSNL and also Tik Fiber. Despite the increased bandwidth, network performance can be impacted in three key ways:

- Compared to the speed of the Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) can become a potential bottleneck.
- Allowing users unrestricted access to the Internet may lead to non-essential downloads that congest traffic, resulting in a poor Quality of Service for critical users and applications.
- When computer systems are interconnected, viruses that enter the LAN through the Intranet or Internet can quickly spread to all other connected computers, exploiting vulnerabilities in the operating systems.

Too many concurrent users on high-speed LANs accessing Internet resources through limited bandwidth can create significant stress on available Internet resources.

Each download increases overall traffic, raising costs and potentially degrading both Quality of Service (QoS) and Quality of Experience (QoE). Reducing internet traffic is essential.

Computer viruses can attach to files and spread rapidly, making them hard to eliminate. Some may damage files or reformat hard drives, leading to significant losses. Others simply replicate, consuming network space and slowing performance.

Significant employee time is wasted on scanning and cleaning infected workstations. Most virus attacks come from emails, unsafe downloads, file sharing, and casual web browsing. Once a virus infiltrates a network, it can spread quickly, causing extensive damage and potentially halting operations.

Containing a virus after it spreads is challenging, often resulting in lost man-hours and data loss during recovery efforts. Thus, early prevention is critical. System administrators use firewalls, access controls, and antivirus software to secure networks, but without clear IT policies, it's hard to convince users of their importance.

Users may see these restrictions as unnecessary and infringing on their freedom. Educational institutions recognize the need for IT policies to safeguard networks. Without strong management policies, security measures may lack effectiveness and alignment with organizational goals. Given the evolving nature of technology, information security policies should be dynamic and regularly updated to reflect changes in technology, user needs, and operations.

2. IT Hardware Installation Policy

The network user community at the institute should take specific precautions when installing their computers or peripherals to minimize inconvenience caused by hardware failures and service interruptions.

a) Primary User

A person who primarily uses the computer in their room is designated as the "primary" user. In cases where a computer has multiple users and no one is identified as the "primary" user, the department head should assign someone to ensure compliance.

b) End User Computer Systems

The institute classifies servers not directly managed by the Computer Center as end-user computers. If no primary user is identified, the department must take on end-user responsibilities. Servers providing services on the

Intranet/Internet, though registered with the Computer Center, are also considered end-user computers under this policy.

c) **Warranty *& Annual Maintenance Contract***

Computers purchased by any Department/ Cells should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by System Administrator or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

d) 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 required for 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.

e) 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 the computer and its peripherals are connected.

f) 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 with read only access rule.

g) Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the institute centrally and distributed by the System Administrator will attend the complaints related to any maintenance related problems.

h) Noncompliance

Faculty, staff, and students at SINCET who do not adhere to the computer hardware installation policy may expose themselves and others to network-related issues, potentially leading to damaged or lost files and inoperable computers, resulting in decreased productivity. A non-compliant computer can significantly impact individuals, groups, departments, or even

the entire institute. Therefore, it is essential to ensure that all computers are brought into compliance as soon as any issues are identified.

Computer Center Interface

If the System Administrator identifies a non-compliant computer impacting the network, they will notify the individual responsible for that system and request that it be brought into compliance. This notification will be communicated via email or phone. The individual users are expected to follow up on this notification to ensure their computer meets the necessary compliance standards. The System Administrator will offer guidance as needed to help the individual achieve compliance.

3. Software Installation and Licensing Policy

Any computer purchases made by the individual departments/cells 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, Institute IT policy does not allow any pirated/ unauthorized software installation on the institute owned computers

and the computers connected to the institute campus network. In case of any such instances, institute 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

Individual users should ensure that their computer systems have the operating system updated with the latest service packs and patches via the Internet. This is especially crucial for all MS Windows-based computers, including both PCs and servers. By updating the operating system, users can address bugs and vulnerabilities that Microsoft periodically identifies, for which it provides patches and service packs.

b) Antivirus Software and its updating

- All computer systems used in the institute must have active anti-virus software installed. The primary user of each computer is responsible for ensuring compliance with this virus protection policy.
- Individual users should verify that their computer systems have up-to-date virus protection software installed and properly maintained.

- ❖ Users should ensure that the software is functioning correctly. It is important to note that any antivirus software that is outdated or not renewed after its warranty period is essentially ineffective. If users find these responsibilities exceed their technical skills, they are responsible for seeking assistance from the System Administrator.

c) Backups of Data

Users should regularly back up essential data to prevent loss from virus infections. Without backups, recovering deleted files may be impossible. During OS installation, it's best to partition the hard drive into multiple volumes (C, D, etc.). Place the OS and software on the C drive, while storing user data on other drives (D, E). If a virus affects the system, formatting only the C volume can help protect data. However, this isn't foolproof. Users should also save important data on CDs, DVDs, or external storage devices like pen drives and hard drives.

d) Noncompliance

SINCET faculty, staff, and students who do not adhere to this computer security policy put themselves and others at risk of virus infections, which can lead to damaged or lost files, inoperable computers, and a decline in productivity. Additionally, there is a risk of spreading infections to others and exposing confidential data to unauthorized individuals. A non-compliant computer can significantly impact other individuals, groups, departments, or even the entire institute. Therefore, it is crucial to ensure that all computers are brought into compliance as soon as any issues are identified.

e) System Administrator Interface

Upon discovering a non-compliant computer, the System Administrator will notify the responsible individual and request that it be brought into compliance. This notification will be sent via email or phone. Individual users are expected to follow up on this notification to ensure their computer meets the necessary compliance standards. The System Administrator will offer guidance as needed to assist the individual in achieving compliance.

4. Network (Intranet & Internet) Use Policy

Network connectivity, whether through an authenticated network access connection or Wi-Fi, is governed by the Institute IT Policy. The System Administrator is responsible for the ongoing maintenance and support of the network, excluding local applications. Any issues related to the institute’s network should be reported to the Computer Center.

All computers (PCs/servers) that connect to the institute's network must have an IP address assigned by the Computer Center. Departments should adhere to a systematic approach regarding the allocation of IP address ranges for each building or WLAN as determined by the institute. Consequently, any computer connected to the network from a specific building will receive an IP address only from that designated address pool.

Additionally, each network port in the room where the computer connects will be internally bound to that IP address to prevent unauthorized use by others from different locations. When a new computer is installed, the concerned user must request an IP address allocation from the System Administrator for their respective department.

b) DHCP and Proxy Configuration by Individual Departments /Cells/ Users

Using any computer at the end user location as a DHCP server to connect additional computers via a switch or hub is strictly prohibited, as it violates the institute’s IP address allocation policy. Similarly, configuring proxy servers is not allowed, as it may disrupt services from the Computer Center. Non-compliance will result in the disconnection of the port connected to the non-compliant computer. The connection will be restored only after receiving written assurance of compliance from the concerned department or user.

c) Running Network Services on the Servers

The System Administrator is not responsible for the content of machines on the network, whether institute property or personal devices. If potentially damaging software is detected, the System Administrator will disconnect the client machine. A machine may also be disconnected if its activities negatively impact network performance. Institute network and computer resources must not be used for personal or commercial purposes. Network traffic will be monitored for security and performance. Impersonating an authorized user is a direct violation and will result in termination of the connection.

d) Dial-up/Broadband Connections

Computer systems connected to the Institute's campus-wide network, whether owned by the Institute or personally owned, must not be used for dial-up or broadband connections. Such usage compromises the Institute's security by bypassing firewalls and network monitoring servers. Failure to comply with this policy may result in the withdrawal of the IP address assigned to the offending computer system

e) Wireless Local Area Networks

This policy applies to all departmental and hostel wireless local area networks. In addition to adhering to this policy, departments and hostels must register each wireless access point with the System Administrator, providing relevant Point of Contact information.

5. Email Account Use Policy

To efficiently distribute critical information to faculty, staff, students, and administrators, the Institute's email services should be used for formal communications and academic purposes. Using email for official correspondence will streamline message and document delivery to campus communities and specific user groups. Formal communications include notices for faculty, staff, and students on topics like human resources information, policy updates, and general announcements.To ensure receipt of these notices, it is important to keep your email address active by using it regularly. Faculty and staff can access their email by logging into https://www.gmail.com with their username and password. For those needing to obtain an Institute email account, please contact the System Administrator to request an account and receive a default password by filling out the designated form.

6. Web Site Hosting Policy

a) Official Pages

Departments, cells, and central facilities may have pages on SINCET's official website.

As of now, the System Administrator is responsible for maintaining the Institute's official website at https://www.sincet.ac.in/.

b) Personal Pages

Each faculty member may have unique requirements for their personal pages. Therefore, faculty can request that their pages be linked to the Institute's official website by submitting a written request or email to the System Administrator, including the URL they wish to add. However, any illegal or inappropriate use will result in the termination of the hyperlink. The content of personal pages must comply with all relevant export laws and regulations, must not infringe on copyrights or trademarks, must not be used for commercial purposes or political lobbying, and must not violate any local, state, or federal laws. Additionally, personal pages may not host content for other individuals or groups.

c) Responsibilities for updating Web Pages

Departments, cells, and individuals are responsible for regularly sending updated information about their web pages to the System Administrator.

7. Institute Database Use Policy

This policy pertains to the databases maintained by the Institute. Data is a vital resource for providing valuable information, and its use must be safeguarded, even if the data is not confidential. SINCET has established specific policies regarding the creation of databases and access to information, along with a broader policy on data access. Together, these policies define the Institute's approach to accessing and utilizing this important resource.

Database Ownership:

SINCET is the data owner of all institutional data generated within the Institute.

Data Administrators:

Data administration activities may be delegated to certain officers within the department.

MIS Components:

For Management Information System requirements of the institute these are

- Employee Information Management System. - Students Information Management System.

- Financial Information Management System.

- Library Management System.

- Document Management & Information Retrieval System.

Here are some general policy guidelines and parameters for departments, cells and administrative department data users:

The Institute's data policies prohibit the distribution of personally identifiable data to individuals outside the Institute.

1. Data from the Institute's database, including information collected by departments or individual faculty and staff, is intended for internal use only.
2. An individual's role and responsibilities determine the data resources required to fulfill their official duties. The Institute's data access policies provide information and data based on these responsibilities.

3. Data that directly identifies a person, along with their personal information, may not be shared in any form with external individuals or agencies, including government entities and survey requests. All such inquiries should be directed to the Office.
4. Requests for information from courts, attorneys, or similar entities must be handled by the Office; departments should not respond to these requests, even if accompanied by a subpoena. All inquiries from law enforcement agencies should also be forwarded to the Office for proper handling.
5. Any tampering with the database by a department or individual user is considered a violation of IT policy. Tampering includes, but is not limited to:

    - Modifying or deleting data items or software components through unauthorized access.
    - Deliberately altering or deleting data items or software components with malicious intent, even by authorized personnel.
    - Intentionally causing a crash of the database, hardware, or system software to destroy all or part of the database.
    - Attempting to breach the security of the database servers.

8. Hostels Wi-Fi Use Policy

Wireless infrastructure in hostels is designed to enhance internet access for academic purposes and exclusive online resources for students, faculty, and staff.

Signal availability may vary across different locations, and coverage is not guaranteed in every area.

Access to wireless internet is an extended service; students cannot demand it, and the Institute reserves the right to suspend services for technical reasons.

The access points are Institute property, and any damage or loss will result in disciplinary action against the responsible student. If loss or damage occurs, costs will be recovered from all students on that floor, building, or hostel.

9. Video Surveillance Policy

The system includes fixed-position cameras, monitors, digital video recorders, storage devices, and public information signs.

Cameras will be installed at key locations on campus, primarily at the entrances and exits of buildings and sites. All cameras will be visible and will not focus on the front or rear of private accommodations.

Signs will be prominently displayed at strategic locations and at campus entrances and exits to inform staff, students, visitors, and the public about the presence of CCTV cameras.

Purpose of the system

The system has been installed by the Institute primarily to reduce the threat of crime, protect the premises, and ensure the safety of all staff, students, and visitors, while respecting individual privacy. These goals will be achieved through monitoring the system to:

- Deter individuals with criminal intent.
- Assist in preventing and detecting crime.
- Aid in the identification, apprehension, and prosecution of offenders related to crime and public order.
- Facilitate the identification of activities or events that may lead to disciplinary proceedings against staff or students, and provide evidence for managers or staff members in such cases. We acknowledge that members of the Institute and others may have concerns or complaints regarding the operation of the system. Any complaints should be directed initially to the Computer Center. CCTV footage will be provided by the Institute upon receiving requests from individuals using the prescribed form.

Appendix I

Campus Network Services Use Agreement

Before applying for a user account or email account, please review the following important policies. By signing the application form for a Net Access ID (user account) or email account, you agree to adhere to the IT policies and guidelines of SINCET. Non-compliance with these policies may lead to the termination of your account or IP address. This is only a summary of the key IT policies; users can obtain a copy of the detailed document from the website and various intranet servers. A Net Access ID consists of a username and password that allows you to access the Institute's computer systems, services, campus networks, and the internet.

a) Accounts and Passwords

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the Institute. Students, staff, and faculty who leave the institute will have their Net Access ID, email id and associated files deleted. No User will be allowed more than one Net Access ID at a time, with the exception that faculty or heads that hold more than one portfolio are entitled to have Net Access ID related to the functions of that portfolio.

b) Limitations on the use of resources

On behalf of the Institute, System Administrator reserves the right to close the Net Access 10 of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

c) Data Backup, Security, and Disclaimer

System Administrator will not be liable for the loss or corruption of data on the individual user's computer because of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of System Administrator staff member in the process of helping the user in resolving their network/computer related problems. Although System Administrator make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email

Account. In addition, System Administrator makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify, and hold System administrator, as part of institution, harmless for any such liability or expenses. SINCETretains the right to change and update these policies as required without notification to the User.

d) Account Termination and Appeal Process

Accounts on SINCET network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may approach the In Charge, Computer Center, justifying why this action is not warranted.

Writing an Appeal Letter

An appeal letter is something you write if you feel you've been treated unfairly in some way--you want someone to reconsider a decision they made about you.

In the letter, make sure you:

- Know where to send it
- Use a polite tone
- State what you would like to have happen
- Be factual, not emotional
- Follow up

Appendix II

SIR ISSAC NEWTON COLLEGE OF ENGINEERING AND TECHNOLOGY

System Administrator

Requisition Form for E-Mail Account

1. Full Name: _____
2. Designation: _____
3. Department: _____
4. Mobile No: _____
5. Existing Mail Id: _____

Date: Signature of Applicant:

----------SYSTEM ADMIN USE ONLY----------

The following email ID is created for Prof. /Dr. /Mr. /Ms. _____

_____

On @sincet.ac.in

Signature on Behalf of In Charge,

System Admin

Appendix III

SIR ISSAC NEWTON COLLEGE OF ENGINEERING AND TECHNOLOGY

System Administrator

Application for Net Access ID Activation

1. Full Name: _____
2. Employee ID: _____
3. Department: _____
4. Mobile No: _____
5. Email Id: _____

Date: Signature of Applicant:

----------SYSTEM ADMIN USE ONLY---------

Net access id is activated for the applicant

Signature on Behalf of In Charge,

System Admin

Appendix IV

SIR ISSAC NEWTON COLLEGE OF ENGINEERING AND TECHNOLOGY

System Administrator

Requisition for CCTV Footage

1. Full Name: _____

2. Employee/Student ID: _____

3. Department: _____

4. Mobile No: _____

5. E-Mail Id: _____

6. Date of Footage: _____ Time: From _____ To _____

7. Camera Location: _____

8. Description: _____

Date: Signature of Applicant:

-----SYSTEM ADMIN USE ONLY---

CCTV Footage is given to the applicant

Signature on Behalf of In Charge,
System Admin