

FROM CHAIRMAN'S DESK...

"It's not a faith in technology. It's faith in people." – Steve Jobs.

The information revolution led us to the age of the internet, where optical communication networks play a key role in delivering massive amounts of data. The world has experienced phenomenal network growth during the last decade, and further growth is imminent. The information revolution is a period of change that might prove significant to the lives of people. Computer technology is at the root of this change, and continuing advancements in that technology seem to ensure that this revolution would touch the lives of people. Computers are unique machines; they help to extend the brain power. Computers offer many benefits, but there are also many dangers. They could help others invade one's privacy or wage war. They might turn one into button pusher and cause massive unemployment.

This reminds us of the fact that no matter how advanced we become technologically, the ultimate outcome will always depend on how humans use the technology. As they say, humans may fail but systems don't.

Keeping these facts in mind, I, on behalf of CSC, feel ecstatic to announce maiden IT Policy of NIT Srinagar, and request the users to use the technology with the aim to benefit from it and not to harm the community. This can easily be achieved by following the IT policy of the institute in word and in spirit.



20.02.2023

Prof. (Dr.) A. H. Bhat,
Chairman,
Computer Services Center,
NIT Srinagar.

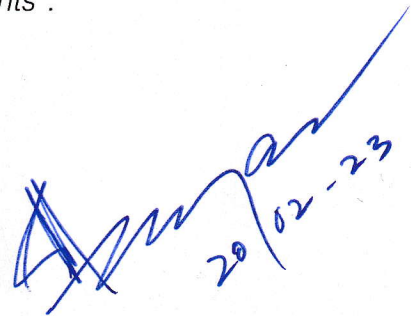
FOREWORD

A policy defines a *guide of action* to achieve an organization's goals and objectives. Policies allow for *efficient, effective, and consistent actions* to occur across an organization. Most, if not all, institutions today use computer and network technology to function. Extensive use of technology creates digital vulnerabilities for institutions that do not adhere to clear rules and guidelines regarding technology usage. Attacks on user data and technology can cause significant damage and require IT policies and procedures.

Defined IT policies and procedures provide a security framework to institutions. It not only helps to protect confidential information but also brings uniformity and control in management of IT infrastructure.

It gives me immense pleasure to document the IT policy of our institution and it shall only serve as a comprehensive guide to achieve uniformity in management and access of IT infrastructure throughout the institution.

"Discipline is the bridge between goals and accomplishments".



Er. Mustafa Zargar,
Scientific/Technical Officer,
Computer Services Center,
NIT Srinagar.

IT Policy

National Institute of Technology Srinagar

Computer Services Center

NIT Srinagar maintains certain policies regarding the use and security of its computer systems, networks and information resources. All users of these facilities, including technology developers, end users and resource administrators are expected to be familiar with these policies and the consequences of violation.

"Information technology policies ensure that everyone's use of the Institute's computing and telecommunications resources supports its educational, research and administrative mission in the best possible way."

User Responsibility

The proper use of all NIT Srinagar computer accounts and technological resources, including computers, e-mail, Internet, printers, software, servers, voice and data networks and other computer peripherals (collectively, "Computer Resources"), is the personal responsibility of everyone. Use of Computer Resources, whether by faculty, students, or staff (collectively, "Users"), must be consistent with institutional policies governing the conduct, including those regarding plagiarism, discrimination, cheating, harassment and theft.

Users must never represent or imply that the opinions that they express on or through Computer Resources are the views of NIT Srinagar. Computer Resources are made available to support the academic mission, programs and activities of NIT Srinagar. Use of Computer Resources is a privilege that is not to be abused and it can be taken away without prior notice and consent or when required by law or when a substantiated reason exists to believe that violations of law or policy have occurred. In time-sensitive cases, access may be restricted to meet critical operational



needs. Any inappropriate, illegal, unethical or immoral use constitutes a violation of this policy regardless of whether it is specifically identified herein.

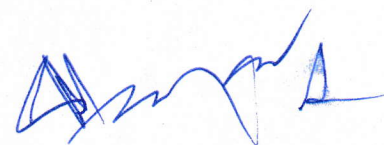
Each User is responsible for the storage of personal files created on NIT Computer Resources. Hard disks are routinely cleared of files. NIT Srinagar will not be liable, under any circumstances, for files stored on or deleted from its hard disks.

Each User is responsible for taking reasonable care for the security of his or her campus account and password. For example, one must change his or her password frequently one must not under any circumstances give his or her password to another person.

Each User must also recognize that NIT has limited means of preventing unsolicited communications from within and outside of the NIT network. Users who receive threatening or inappropriate communications must bring them to the attention of the appropriate network administrator, General Counsel, Office of Human Resources or the Office of Student Affairs.

Network Usage Policy

The Institute expects that all persons who make any use of Institute computing hardware, software, networking services or any property related or ancillary to the use of these facilities, will abide by the following policy statement: Institute information technology resources are provided in the hope that the whole institute community will use them in a spirit of cooperation. Resources are limited and must be shared. Everyone will benefit if all computer users avoid any activities which cause problems for others who use the same systems. All hardware, software and related services supplied by the Institute are for the sole purpose of supplementing and reinforcing the Institute's goals as set forth in the student and faculty handbooks and other mission statements of the Institute. It is a specific violation to give account passwords to individuals who are not the owners of such accounts or to obtain passwords to or use of accounts other than one's own. We expect that no one will use hardware, software or services without authorization to do so. Copying software is a violation of copyright law. Individuals may not extend their use of the facilities described above for any purpose beyond their intended use nor beyond those activities sanctioned in Institute policy statements. In particular, no one may use them for personal profit or gain to



harass, threaten or otherwise invade the privacy of others, to initiate or forward e-mail chain letters, to cause breaches of computer, network or telecommunications security systems, to initiate activities which unduly consume computing or network resources. Individuals who violate the aims of this policy will be subject to disciplinary action.

IT policies

- The **institute's IT infrastructure** refers to the institute network and any hardware and software services provided by the institute.

- The institute **IT infrastructure is primarily for academic use of the NIT community** and must not be used by any user for any other purposes that are in direct conflict with the role of the user without the explicit permission of the competent authority.

- Users must not use the institute **IT infrastructure for any commercial purposes** unless specifically permitted by the competent authority.

- Users must not use the institute IT infrastructure in any way so to compromise the security of any other user, system or network anywhere inside or outside the institute.

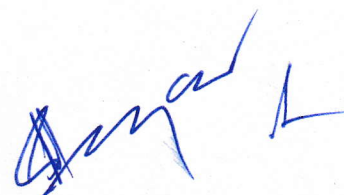
- Users must not use or communicate any information using the institute IT infrastructure that may harm, threaten, intimidate or harass others or may be otherwise considered objectionable or illegal as per law.

- Users are solely **responsible for any data stored** or sent by them using the institute IT infrastructure. Any liability arising out of any misuse is the responsibility of the user concerned.

- Users are **not allowed to extend or otherwise tamper with the institute network** in any manner without prior permission of Computer Services Center (CSC), except for any network extension made individually by faculty members or staff members inside residential quarters officially allotted to them by the institute.

- Users must use the **Email facility primarily for academic and official purposes** and to a limited extent for reasonable personal purposes.

- Users are responsible for keeping a **backup of important mails in their email accounts**. While CSC takes periodic email backups, **CSC cannot be held responsible for any loss of data in user email accounts**.



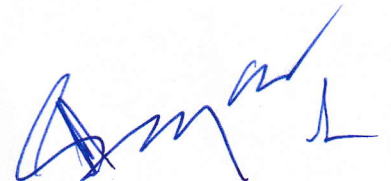
- Users must **not share their email account details with others** as the individual account holder is personally held accountable in case of any misuse of that email account.
- Users must **not attempt to break into others' email accounts**.
- User must **not open any mail or attachment that is from unknown and suspicious sources** or is of otherwise suspicious nature without confirming the authenticity of the attachment.
- Users must **not give out confidential information such as password etc.** in response to any email. CSC never asks for password information over email.
- Users **must use a strong password to protect any accounts owned by them** on the institute IT infrastructure including but not limited to email accounts. A password must be immediately changed if it is suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.
- Users aware of any breach of security in any part of the IT infrastructure must report such situations to the systems administrator or the departmental representative responsible for security in that area.
- **Users are solely responsible for understanding and following this usage policy.** Any violation of any part of this usage policy and/or any misuse of any part of the IT infrastructure by any user or using any account owned by the user is solely the responsibility of the user. Any liability or legal action arising out of any such violation/misuse will solely be the responsibility of the user and the user may be subjected to appropriate actions as decided by the authorities.

Access Control Policy

- Data capping of student internet accounts will be as follows:
 - o 3 GB/day capping for B. Tech program
 - o 5 GB/day capping for master's program.
 - o 20 GB/day capping for scholars.
- Content filtering on firewall blocks access to multiple categories of websites as per security policy. Any request to unblock a particular website (that may fall in blocked categories accidentally) must be addressed to Chairman CSC from the Head of the concerned department/center.

Software Purchase Policy

- Use of pirated software must be avoided under all circumstances.



- Software must be procured in consultation with CSC to ascertain the compatibility with the existing infrastructure of the institute.
- A client-server model of software licensing must be preferred.

Network Usage Policy

- Any service request (SR) to CSC must be placed at least 48 hours in advance. CSC will not be responsible for any pendency if the SR is made in less than 48 hours of turn-around-time (TAT).

Data Center Usage Policy

- Virtual PCs shall be given to scholars in data center. Request for the same shall be forwarded by their (scholars') respective supervisor to Chairman CSC along with the details of the required software to be installed on the Virtual PCs.

User Accounts Policy

- User IDs (Internet gateway accounts and email accounts) must be standardized. A user must have same user ID to access internet and email account.
- User IDs of students to be created immediately after admission (data to be procured from academic section).
- E-mail IDs to be deactivated 6 months after the completion of degree. Any exception to be made after due approval from competent authority. A deactivation email should be sent a week before deactivating any email
- Domain Controller (Active Directory) implementation in computer labs of the institute to ensure a centralized user account login on systems and to avoid installation of any prohibited software by students on the computers of the labs.

Website Update Policy

- Every department must nominate a faculty member as department web coordinator. A web coordinator shall look after the content management of his/her department on the institute website.

