

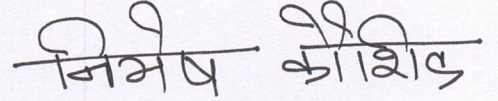
नं. 26(1)/2023-INST

दिनांक: 20.02.2023

### कार्यालय आदेश / OFFICE ORDER

सक्षम प्राधिकारी द्वारा संस्थान की सूचना प्रौद्योगिकी नीति एवं दिशानिर्देश (वर्शन १.०) को अनुमोदित किया गया है। सभी से इसका पालन अपेक्षित है।

An IT Policy and Guidelines (Version 1.0) of the Institute has been approved by competent authority for circulation. All are requested to comply with the same.



मुख्य वित्त एवं प्रशासनिक अधिकारी  
Chief Finance and Administrative Officer

संलग्नक : आई.एन.एस.टी. सूचना प्रौद्योगिकी नीति एवं दिशानिर्देश (वर्शन १.०)

Enclosure : INST IT Policy and Guidelines (Version 1:0)

#### प्रसार / Circulation:

1. सामान्य / General
2. निदेशक कार्यालय / Office of Director, INST
3. कार्यालय आदेश फोल्डर / Office Order Folder



# **INSTITUTE OF NANO SCIENCE AND TECHNOLOGY**

## **IT Policy & Guidelines (Version 1.0)**

## Policy Objectives

The Institute of Nano Science & Technology (INST) provides IT resources to support the academic, research, and administrative activities of the Institute and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well-informed and carry out their functions in an efficient and effective manner. This document establishes specific requirements for the use of all IT resources at INST. This policy applies to all users of computing resources owned or managed by INST. Individuals covered by the policy include (but are not limited to) INST faculty and visiting faculty (permanent/adjunct/visiting/guest/fellow), staff, students, guests, and external individuals. For the purpose of this policy, the term 'IT Resources' includes all Institute-owned, licensed, or managed hardware and software, and use of the Institute network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network. Misuse of these resources can result in unwanted risks and liabilities for the Institute. It is, therefore, expected that these resources are used primarily for Institute related purposes and in a lawful and ethical way.

## E-mail Account Management

### 1. Creation of E-mail Addresses:

The following rules will apply creation of email account for Faculty (permanent/adjunct/visiting/guest/fellow), Students and Staff (Permanent & Temporary).

- a. Email ID will be created for all individuals who join the institute for more than 6 months.
- b. An e-mail account will be created upon filling out the online form by the concerned faculty/ administrative officer on behalf of the newly joined student/staff. The link is available on the INST website's internal user section (<https://inst.ac.in/internalUsers/52>).
- c. It is compulsory to mention the alternative email id (Non-INST) when filling out the online form because all the communication regarding the email id creation shall be forwarded to the alternative email id.
- d. An E-mail ID will be created within 48 working hours after receiving the filled online form. If there is any issue in obtaining the email ID, the concerned person can contact the IT personnel.
- e. No route other than via the academic section will be entertained for the creation of an email account.
- f. All administrative officials (e.g. CFAO, FO, Deans, and Heads) will be allocated a dedicated role-attached email address in addition to their individual email ID. This email address is expected to be used only for the intended official correspondence. Once the tenure of the concerned individual in any of these posts ends, it has to be handed over to the new appointee for that post. The data within these email addresses should be strictly retained across the appointments.
- g. With prior permission from the parent institution, email ID can be provided to adjunct and guest faculty if they stay at INST at least for 6months. This email ID should be used as a secondary address while the primary email address is active with the parent organization. The INST email ID should not be used for professional activities such as the submission of manuscripts and grant applications.
- h. Individuals with short visiting appointments who do not require a stay at INST for at least 6 months will not be provided with an INST email ID. However, with necessary

approvals in place, temporary access to INST internet will be provided during the period of the visit.

- i. Email ID after being assigned will not be reallocated to a second person even after the exit of the first person who handled it. This is to maintain the privacy and security of the concerned.

## 2. E-Mail Data Backup

Each user is responsible for the individual emails and data stored in the relevant webmail folders. IT Department will not be responsible for any accidental user deletion of e-mails/data.

## 3. E-Mail Security

Google G-suite email services by default provide Spam filters and anti-virus filters. These filters are there to protect the e-mail setup from viruses and unsolicited e-mails. Whilst these filters are constantly updated by Google, the IT Department cannot guarantee that it shall provide 100% protection against all viruses and spam. Hence users are advised to mark the suspicious email as Junk or SPAM using this option available in the email application, if they consider so, any mail received in their mailbox may forward to the IT department for further necessary action.

## 4. Deactivation of E-mail Accounts

To get the No Dues Sign-off signature, one needs to fill and submit IT No Dues online form, which is available on the website under internal user forms.

### **Email ID suspension policy for faculty, staff, and students**

- a) **Faculty** – The email ID of the permanent faculty member will get suspended after **six months** from the last working date at INST. An extension with approval from competent authority will be on a case-to-case basis.
- b) **Adjunct / Guest / Visiting Faculty** - Email ID will get suspended after **Three Months** from the last working date at INST. An extension with approval from competent authority will be on a case-to-case basis.
- c) **Faculty fellow (INSPIRE/Ramalingaswamy etc)** - Email ID will get suspended after **Three Months** from the last working date at INST. An extension with approval from competent authority will be on a case-to-case basis.
- d) **Staff** – The email ID of the Permanent/Temporary Staff member will get suspended immediately from the last working date at INST.
- e) **Ph.D. Students**- Email ID of the Ph.D. Students will get suspended after **one month** from the last working date at INST. An extension with approval from competent authority will be on a case to case basis in concurrence with a supervisor.
- f) **PDF Students** - Email ID of the PDF Students will get suspended after **one month** from the last working date at INST. An extension with approval from competent authority will be on a case-to-case basis in concurrence with a supervisor.
- g) **Project Students** – The email ID of the Project Students will get suspended immediately from the last working date at INST.

### **NOTE –**

- 1) All the Suspended Email accounts will get permanently deleted from the email server after One Year from the date of suspension.

- 2) Suspended email accounts will not be activated again without proper approval from the competent authority.
- 3) Any account which is found not signed in or inactive for a period of 90 days will be deactivated by the IT Department. The user ID along with the data will be removed from the e-mail server system after a period of 180 days if no request for activation is received during this period. Once deleted, in case of rejoining of the concerned person, a fresh request and associated formalities should be completed for the reopening of the said account.
- 4) After a no-dues certificate is submitted by a user, the institute will not be responsible for any misuse or security of data in her/his account till it is suspended.

## 5. Recommended Best Practices:

Users are advised to adopt the following best practices for the safe usage of e-mail services:

- a) Users are strongly recommended to change their passwords on a periodic basis
- b) Users must log out from their email accounts whenever they leave the computer unattended for a considerable period of time. The user should log out from web-based services like web email before closing the browser session.
- c) Users should disregard any email that requests details like login ID and password and should refrain from sharing such details over mail or otherwise with anyone
- d) Emails identified as SPAM are delivered in the “Probably Spam” folder that exists in the user’s mailbox. Hence, users are advised to check the “Probably Spam” folder on a daily basis.

## 6. Handling email address suspension

The allowed period during which an individual’s email address stays active after her/his exit is strictly to take back up of the data and for required arrangements to inform all the concerned personal and professional contacts of the individual’s change of email ID. All professional bodies such as publishers, societies, etc allow the updation of contact details from time to time. It is important that the individual including faculty, students, and staff should plan well ahead of their expected exit date, to secure any valuable information prior to suspension of the account.

## Website Management

1. **Content uploading Policy:** For content updation, an individual should send an email to [webteam@inst.ac.in](mailto:webteam@inst.ac.in). Verbal requests will not be entertained.
2. All the changes within the faculty group profile will be done by the concerned faculty and she/he will take full responsibility for its contents.
3. **Website Security:** INST website is hosted by the Govt. organization STPI (Software Technology Park of India) and they are responsible for website server security and data backup. Any loss of data can be recovered easily from STPI data backup.

## Network (Intranet & Internet) Use Policy

Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the Institute IT Policy. IT Department is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute’s network should be reported to IT Department.

1. **IP Address Allocation:** Any computer that will be connected to the institute network should have an IP address assigned by the IT Department. Departments should follow a

systematic approach, the range of IP addresses that will be allocated to each building / V LAN as decided. So, any computer connected to the network from that building will be allocated an IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have a binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

## **2. Network Infrastructure**

INST Network is secured Using Fortinet Firewall which is installed in the Server Rack and the NKN / NIC Leas line with 100 Mbps speed is routed through the Firewall to L3 Level switches and then to other L2 Level Local Switches on Each Floor/building in Local Area Network throughout the campus.

## **3. Threat and vulnerability management**

Threat and vulnerability management in a firewall is used to test new threats and malware automatically. The test of these new threats and malware is tested by Firewall and then at the user end by an Antivirus Program installed on every computer with updated definitions so that all new threats can be detected and deleted before any damage to infrastructure.

IT Department will be constrained to disconnect user machines where potentially damaging software is found to exist. A user machine may also be disconnected if the client's activity adversely affects the Network's performance.

## **4. Mobility and Wireless Devices**

To the extent possible, users are expected to connect only to the official INST WiFi network for wireless access. Setting up of unsecured Wi-Fi systems on the Institute network is prohibited. Mobile and wireless Device connections will get safe by using internet access by password. Currently, all the Access Points are configured through the Fortinet Firewall Wireless controller in the internal Network and connected to local switches to provide Internet connections to wireless devices.

## **Security Measures**

### **1. Security of Server Room, Data Centre / Firewall / Switch Rack**

INST Security office takes care of the CCTV recording and all security breach issues. No individual person will contact the IT department for CCTV footage regarding any issue. IT section will only provide technical support for CCTV infrastructure for fixing nonfunctional cameras and hardware, whenever required.

### **2. Computer Security**

- a) For the security of individual computers, all Windows OS computers have an Antivirus program that is getting updated on daily basis automatically to get rid of the virus, malicious spam websites, and malicious, torrent, and illegal websites & contents are also blocked by the firewall.
- b) Individuals should not use their computers for any illegal activities, chain letters (electronic mail spam), or discriminatory communication. The individual person is responsible for their computer's health and security.
- c) Employees cannot copy, retrieve, or modify copyrighted materials without the permission of the copyright holder. Violation of this policy can lead to copyright law enforcement for both the individual and the company.
- d) As per DST guidelines, any computer can be audited at any time, so an individual person should maintain the system as per the instructions.