



GURU NANAK EDUCATION TRUST



GURU NANAK INSTITUTE OF PHARMACEUTICAL SCIENCE AND TECHNOLOGY

(GNIPST)

*A JIS Group Institution | Approved by PCI | Accredited by NAAC & NBA | Affiliated to
Maulana Abul Kalam Azad University of Technology, West Bengal (MAKAUT)
157/F, Nilgunj Road, Sahid Colony, Panihati, Kolkata – 700114, West Bengal*

INSTITUTIONAL POLICY DOCUMENT IT POLICY AND CYBER SECURITY GUIDELINES

Document Control

Document Title	IT Policy and Cyber Security Guidelines
Applicable To	All students, faculty, staff, departments, visitors and service providers using GNIPST IT resources
Custodian	IT Committee / IT Cell (System Administrator)
Approving Authority	Governing Body, GNIPST
Version	1.0
Effective Date	To be notified upon Governing Body approval
Review Cycle	Once every three (3) years, or as required

Table of Contents

1. Preamble	
2. Objectives of the Policy	
3. Legal and Regulatory Framework.....	
4. Definitions	
5. Scope and Applicability	
6. Institutional Mechanism – IT Committee and IT Cell	
7. IT Infrastructure and Services	
8. User Accounts and Access Control.....	
9. Acceptable Use of IT Resources	
10. E-mail and Official Communication.....	
11. Internet and Wi-Fi Usage	
12. Software Licensing and Installation	
13. Hardware Procurement, Maintenance and Disposal	
14. Cyber Security Guidelines	
15. Data Protection, Privacy and Backup	
16. Institute Website and Social Media	
17. Cyber Security Incident Reporting and Response	
18. Logging and Monitoring	
19. Awareness and Training	
20. Non-Compliance and Disciplinary Provisions.....	
21. Amendment and Review of Policy	
22. Approval	
Annexure I – IT Account and Access Request Form	
Annexure II – Cyber Security Incident Report Form.....	
Annexure III – IT Asset Issue and Return Form	

1. Preamble

Guru Nanak Institute of Pharmaceutical Science and Technology (GNIPST), established in 2005 under the aegis of the Guru Nanak Education Trust and nurtured within the JIS Group, relies on information technology for teaching and learning, research, examinations, administration, communication and student services. The Institute's computers, network, software, data and online services are valuable institutional assets that must be used responsibly and protected against misuse, loss and cyber threats.

This IT Policy and Cyber Security Guidelines document has been framed in line with the Information Technology Act, 2000 (as amended), the directions of the Indian Computer Emergency Response Team (CERT-In), the Digital Personal Data Protection Act, 2023, the Pharmacy Council of India (PCI) and the affiliating University (MAKAUT), the norms of NAAC and NBA, and accepted good practices in information security, so as to provide a clear and secure framework for the use of IT resources at GNIPST.

2. Objectives of the Policy

The specific objectives of this policy are to:

- Provide reliable, secure and equitable access to IT resources for academic, research and administrative purposes.
- Define the responsibilities of users, the IT Cell and departments in the use and management of IT resources.
- Establish rules for acceptable use and prevent the misuse of IT resources.
- Protect the confidentiality, integrity and availability of the Institute's information and systems against cyber threats.
- Protect the personal data of students, employees and other stakeholders in accordance with applicable law.
- Ensure timely detection, reporting and response to cyber security incidents, including mandatory reporting to CERT-In.
- Promote awareness of cyber hygiene, digital ethics and safe online behaviour.

3. Legal and Regulatory Framework

This policy is framed in accordance with, and shall be read together with, the following:

- The Information Technology Act, 2000 (as amended) and the Rules made thereunder.
- The directions issued by CERT-In under Section 70B of the IT Act, including the directions of April 2022 relating to information security practices, procedure, prevention, response and reporting of cyber incidents.
- The Digital Personal Data Protection Act, 2023 and the Rules made thereunder, as and when in force.
- The Copyright Act, 1957, in respect of software, digital content and licensed resources.
- The E-Waste (Management) Rules, 2022, in respect of the disposal of IT equipment.
- Applicable guidelines of UGC, PCI and MAKAUT, and the Institute's other policies, including the Gender Sensitization and POSH Policy.

In the event of any conflict between this policy and the applicable law, the law shall prevail.

4. Definitions

"Institute" means Guru Nanak Institute of Pharmaceutical Science and Technology (GNIPST).

"IT Resources" means all computing and communication facilities owned, leased or managed by the Institute, including computers, laptops, servers, printers, scanners, projectors, smart boards, network and Wi-Fi infrastructure, internet connectivity, software, cloud services, e-mail, websites, portals, databases, CCTV and biometric systems, and the data stored in them.

"User" means any student, faculty member, staff member, research scholar, guest, visitor, vendor or service provider authorised to use the Institute's IT Resources.

"IT Committee" means the committee constituted under Section 6 of this policy.

"IT Cell / System Administrator" means the unit and personnel responsible for the management and maintenance of the Institute's IT Resources.

"Cyber Security Incident" means any real or suspected adverse event that compromises or threatens the confidentiality, integrity or availability of the Institute's IT Resources or data, including malware or ransomware infection, unauthorised access, data breach, phishing, website defacement, denial of service and identity theft.

"Personal Data" means any data about an individual who is identifiable by or in relation to such data, as defined under the Digital Personal Data Protection Act, 2023.

"Competent Authority" means the Director/Principal of the Institute, or the Governing Body where specified.

5. Scope and Applicability

This policy applies to all Users and to all IT Resources of the Institute, whether used on campus, in hostels or remotely, and to personal devices when connected to the Institute's network or used to access Institute systems or data. It covers the provision, use, security and disposal of IT Resources, and the handling of the Institute's digital information in any form.

6. Institutional Mechanism – IT Committee and IT Cell

An IT Committee shall be constituted by the Director, as follows:

- **Chairperson:** Director / Principal, GNIPST
- **Convenor:** Senior faculty member nominated by the Director as IT Coordinator
- **Members:** System Administrator / In-charge of the IT Cell, one faculty representative from each department, the Librarian, the Examination Controller/Officer-in-charge, and a representative of the Finance & Accounts Office

The IT Committee shall be responsible for:

- Framing, implementing and reviewing IT policies and security guidelines.
- Planning IT infrastructure, and recommending the annual IT budget, procurement and upgrades.
- Reviewing cyber security status, incidents and audit findings.
- Meeting at least twice in each academic year, with minutes duly recorded.

The IT Cell, headed by the System Administrator, shall be responsible for the day-to-day management of IT Resources, including user accounts, network and server administration, security controls, backups, maintenance, helpdesk support, asset records and incident response. The System Administrator shall act as the point of contact for CERT-In and shall ensure that the Institute's contact details are registered with CERT-In as required.

7. IT Infrastructure and Services

The Institute shall provide and maintain the following IT Resources, as available from time to time:

- Campus-wide wired and wireless network with internet connectivity.
- Computer laboratories, the digital library, and computers and peripherals in departments and offices.
- Official e-mail accounts on the Institute domain for faculty, staff and, where provided, students.
- The Institute website, and ERP, learning management, library management, examination and other application systems.
- Licensed software for academic, research and administrative use, including pharmaceutical and statistical software where available.

- ICT-enabled classrooms and seminar halls, CCTV surveillance and biometric attendance systems.

Requests for new services, equipment or software shall be made through the Head of Department to the IT Cell, and shall be considered by the IT Committee within the budget and technical feasibility.

8. User Accounts and Access Control

1. Access to IT Resources shall be granted only to authorised Users, on submission of the IT Account and Access Request Form (Annexure I), duly approved by the Head of Department/Section.
2. Each User shall be given a unique user ID. Accounts shall not be shared, and the User shall be responsible for all activity carried out through their account.
3. Access to administrative, financial, examination and other sensitive systems shall be granted on a need-to-know and least-privilege basis, and shall be reviewed at least once a year by the IT Cell with the concerned section heads.
4. Administrative (privileged) access to computers, servers and network devices shall be restricted to authorised IT Cell personnel.
5. Accounts of employees who leave the Institute shall be disabled on their relieving date; accounts of students shall be disabled on completion of the programme or after a notified grace period. Official data in such accounts shall be handed over to the Head of Department before exit.
6. Guest and vendor access shall be temporary, limited to the required systems, and shall expire automatically at the end of the approved period.

9. Acceptable Use of IT Resources

9.1 Permitted Use

IT Resources are provided primarily for teaching, learning, research, administration and other official purposes of the Institute. Limited incidental personal use is permitted, provided it does not interfere with official work, consume excessive resources, or violate this policy or any law.

9.2 Prohibited Use

Users shall not use IT Resources to:

- Access, create, store or transmit obscene, pornographic, defamatory, hateful, harassing, threatening or unlawful material.
- Engage in cyberbullying, stalking, sexual harassment or impersonation of any person, including through social media or messaging groups.
- Gain or attempt unauthorised access to any system, account or data, or circumvent security controls such as firewalls, content filters and authentication.
- Install or run hacking tools, network scanners, packet sniffers, cryptocurrency miners, proxies or VPNs to bypass Institute controls, except as authorised in writing for academic purposes in a controlled environment.
- Knowingly introduce viruses, malware or other harmful code.
- Download, store or share pirated software, movies, music or other copyrighted material, or use peer-to-peer file-sharing for such purposes.
- Use IT Resources for commercial activity, private business, political campaigning or gambling.
- Send spam, chain messages, or unsolicited bulk e-mail.
- Tamper with, damage, remove or relocate IT equipment, cables or configurations without authorisation.
- Use generative AI or other online tools in a manner that violates academic integrity rules, or upload confidential Institute data, examination material or personal data to external AI tools or public platforms.

10. E-mail and Official Communication

- Official communication shall be carried out using the Institute e-mail account. Personal e-mail accounts shall not be used for official work involving confidential information.
- Users shall not forward official e-mail automatically to personal accounts, and shall not share their e-mail password with anyone.
- Circulars and official announcements may be sent to groups only by authorised persons.
- E-mail attachments and links from unknown or suspicious senders shall not be opened. Suspected phishing e-mails shall be reported to the IT Cell.
- Official messaging groups (such as departmental or class groups) shall be used responsibly and with the same standards of conduct as other official communication.
- The Institute reserves the right to access official e-mail accounts, in accordance with Section 18, in the event of a security incident, legal requirement, or with the approval of the Competent Authority.

11. Internet and Wi-Fi Usage

- Internet and Wi-Fi access shall be provided through authenticated login. Users shall not share their Wi-Fi credentials.
- The Institute may apply content filtering, bandwidth management and access restrictions to ensure fair use and security.
- Users shall not set up personal wireless routers, access points or hotspots that interfere with the Institute network, or extend the network without permission.
- Hostel internet access, where provided, shall be subject to the same rules and to such additional time or bandwidth restrictions as may be notified.

12. Software Licensing and Installation

- Only licensed, open-source or freeware software that is legally obtained shall be installed on Institute computers.
- Software shall be installed only by, or with the approval of, the IT Cell. Users shall not install software on laboratory or office computers on their own.
- Departments requiring new software shall submit a request with justification through the Head of Department. Licences shall be procured in the name of the Institute and recorded by the IT Cell.
- Licence terms, including the number of installations and permitted users, shall be strictly followed. Institute-licensed software shall not be copied for personal use unless the licence permits it.
- Outdated or unsupported software and operating systems shall be phased out as early as feasible.

13. Hardware Procurement, Maintenance and Disposal

- IT equipment shall be procured according to the Institute's purchase procedure, on the technical recommendation of the IT Cell, with attention to warranty, security features, energy efficiency and compatibility.
- The IT Cell shall maintain an up-to-date register of all IT assets, including their configuration, location, user and warranty or maintenance contract status.
- Equipment issued to individuals (such as laptops) shall be recorded using the IT Asset Issue and Return Form (Annexure III). The individual shall be responsible for its care and shall return it on transfer or exit.
- Faults shall be reported to the IT Cell, which shall arrange repair through in-house staff or authorised vendors. Storage media shall be removed or securely wiped before equipment is sent outside for repair, where feasible.

- Obsolete or unserviceable equipment shall be written off with the approval of the Competent Authority. All data on storage media shall be securely erased or the media physically destroyed before disposal, and e-waste shall be handed over only to authorised recyclers in accordance with the E-Waste (Management) Rules, 2022.

14. Cyber Security Guidelines

14.1 Password and Authentication

Users shall follow the password rules given below. Multi-factor authentication shall be enabled for e-mail, administrative, financial and examination systems wherever supported.

Parameter	Requirement
Minimum length	At least 8 characters (12 or more recommended; longer passphrases encouraged)
Complexity	A mix of upper-case and lower-case letters, numbers and special characters
Reuse	Not the same as the last few passwords, and not used for personal accounts
Change	Immediately if compromise is suspected, and periodically for privileged accounts
Account lockout	After a limited number of consecutive failed login attempts, as configured by the IT Cell
Default passwords	To be changed at first login and on all new devices and systems

Note: Parameters are indicative and may be revised by the IT Committee in line with current good practice.

Passwords shall never be written down in visible places, shared, or sent by e-mail or message. The IT Cell shall never ask a User for their password.

14.2 Endpoint Protection

- All Institute computers shall have licensed and updated anti-malware protection, enabled firewalls, and automatic screen locking after a period of inactivity.
- Operating systems, browsers and applications shall be kept up to date with security patches. Critical patches shall be applied as early as possible.
- USB storage devices shall be scanned before use. The IT Cell may restrict the use of removable media on sensitive systems.

14.3 Network and Server Security

- The Institute network shall be protected by a firewall, with separate network segments for administrative systems, academic laboratories, guest Wi-Fi and CCTV/IoT devices, where feasible.
- Servers and network devices shall be hardened, with unused services and ports disabled, and administrative access restricted and logged.
- System clocks of all servers and network devices shall be synchronised with the Network Time Protocol (NTP) servers of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or with servers traceable to them, as required by CERT-In.
- Remote access to Institute systems shall be permitted only through secure, approved methods, and only for authorised Users.
- Periodic vulnerability assessment of critical systems, and a security audit of the website and key applications by a CERT-In empanelled auditor or other qualified agency, shall be carried out where required or feasible.

14.4 Phishing and Social Engineering

Users shall be alert to phishing e-mails, messages and calls that ask for passwords, OTPs, payments or personal details, or that urge immediate action. Requests for payments or changes to bank details, even if they appear to come from senior officials or vendors, shall be verified by phone or in person through a known contact before any action is taken.

14.5 Personal Devices (BYOD)

- Personal devices connecting to the Institute network shall have an updated operating system and security software, and a screen lock.
- Institute confidential data, examination material and personal data of students or employees shall not be stored on personal devices, except where specifically authorised and protected.
- The Institute may deny network access to any device that poses a security risk.

14.6 Physical Security

- The server room and network racks shall be kept locked, with access restricted to authorised IT Cell personnel and an access register maintained.
- Server rooms shall be provided with power backup (UPS), fire safety equipment and suitable environmental conditions.
- Users shall lock or log out of their computers when leaving them unattended, and shall not leave confidential documents on printers.

15. Data Protection, Privacy and Backup

- Personal data of students, employees and other stakeholders shall be collected only for specified lawful purposes, limited to what is necessary, kept accurate, protected with reasonable security safeguards, and retained only as long as required, in accordance with the Digital Personal Data Protection Act, 2023 and the Rules made thereunder.
- Access to personal data (such as admission records, marks, health information, bank details and identity documents) shall be restricted to authorised personnel on a need-to-know basis.
- Personal data shall not be displayed publicly or shared on messaging groups or social media except as required by law or with consent. Result lists and notices shall disclose only the minimum information necessary.
- Any personal data breach shall be treated as a cyber security incident and reported as per Section 17, including notification to the Data Protection Board and affected individuals where required by law.
- Examination papers, results and other confidential data shall be handled using secure systems and encrypted storage or transfer where feasible.

15.1 Backup

The IT Cell shall back up critical data as follows:

Data / System	Indicative Frequency	Retention
ERP, finance, admission and examination databases	Daily	As per statutory and Institute record-retention requirements
Website and application servers	Weekly and before every major change	At least the last three versions
Departmental shared drives / official files	Weekly	As decided by the IT Committee
System and security logs	Continuous	At least 180 days (see Section 18)

Note: Frequencies are indicative. At least one copy of critical backups shall be kept offline or offsite (or in a secure cloud) to protect against ransomware, and restoration shall be tested periodically.

16. Institute Website and Social Media

- The Institute website shall be the official online source of information about the Institute, and shall be maintained with accurate and up-to-date content, including mandatory disclosures required by AICTE, PCI, NAAC, NBA and other bodies.
- Content for the website shall be approved by the Head of Department/Section and published by the authorised website team. The website shall be secured with HTTPS, regular updates and periodic security checks.
- Official social media accounts of the Institute shall be created and managed only by persons authorised by the Competent Authority, with credentials held by the IT Cell.
- Users shall not create accounts, pages or groups that purport to be official Institute accounts, or use the Institute's name, logo or letterhead online without authorisation.
- Users shall not post confidential Institute information, or photographs and videos of students, employees or events that violate privacy or dignity, on social media.

17. Cyber Security Incident Reporting and Response

1. **Reporting by Users:** Any User who notices or suspects a cyber security incident (such as a malware infection, suspicious login, phishing attempt, data leak, lost or stolen device, or website defacement) shall report it immediately to the IT Cell, using the Cyber Security Incident Report Form (Annexure II) or by any quick means followed by the form.
2. **Containment:** The IT Cell shall immediately take steps to contain the incident, such as isolating affected systems, disabling compromised accounts and blocking malicious addresses, while preserving evidence.
3. **Reporting to CERT-In:** Incidents of the types specified by CERT-In shall be reported to CERT-In within six (6) hours of being noticed, in the prescribed manner, by the System Administrator with the knowledge of the Competent Authority.
4. **Other Reporting:** Where required, the incident shall also be reported to the police or the National Cyber Crime Reporting Portal (cybercrime.gov.in / helpline 1930), and personal data breaches to the Data Protection Board and affected individuals as required by law.
5. **Recovery:** Affected systems shall be cleaned or rebuilt, and data restored from verified backups.
6. **Review:** A post-incident review shall be carried out, and the report, including the root cause and preventive measures, shall be placed before the IT Committee.

18. Logging and Monitoring

- The Institute shall maintain logs of its systems, including firewall, network, server, authentication, e-mail and application logs, securely within India for a rolling period of at least 180 days, or such other period as may be prescribed by CERT-In, and shall provide them to CERT-In or other authorities when lawfully required.
- The IT Cell may monitor network traffic and system usage for security, performance, fault management and compliance purposes. Users should have no expectation of privacy in the use of Institute IT Resources, subject to applicable law.
- Access to the content of an individual User's files or communications shall be carried out only in connection with a security incident, a legal requirement, or an inquiry, and with the written approval of the Competent Authority. The information obtained shall be kept confidential and used only for that purpose.

19. Awareness and Training

The IT Cell, in coordination with the IT Committee, shall conduct regular awareness programmes on cyber hygiene, password security, phishing, safe use of social media, online fraud, data privacy and digital ethics for students, faculty and staff, including orientation for new entrants. Staff handling examinations, finance and personal data shall receive specific training. Users shall be encouraged to use national resources such as the Cyber Swachhta Kendra and the cyber awareness material of CERT-In and the Indian Cyber Crime Coordination Centre (I4C).

20. Non-Compliance and Disciplinary Provisions

Any violation of this policy, including misuse of IT Resources, unauthorised access, sharing of credentials, installation of unauthorised software, breach of data confidentiality, or failure to report a known incident, may result in one or more of the following, in addition to any action under the IT Act and other applicable laws:

- Written warning.
- Temporary or permanent suspension of access to IT Resources.
- Recovery of the cost of damage or loss caused to the Institute.
- Disciplinary action under the Institute's student disciplinary rules or service rules, as applicable.
- Referral to law enforcement authorities where the act constitutes an offence.

21. Amendment and Review of Policy

This policy shall be reviewed once every three years, or earlier if required by changes in the IT Act, CERT-In directions, data protection law, UGC/AICTE/PCI/MAKAUT guidelines, technology, or Institute needs. Technical standards and operational procedures under this policy (such as password parameters and backup schedules) may be updated by the IT Committee with the approval of the Competent Authority. Any other amendment shall require the approval of the Governing Body of GNIPST and shall be communicated to all Users through official circulars.

22. Approval

This IT Policy and Cyber Security Guidelines document has been recommended by the IT Committee and is placed for approval before the Governing Body of Guru Nanak Institute of Pharmaceutical Science and Technology.

Prepared by
(IT Coordinator)

Date:

Recommended by
(Director / Principal)

Date:

Approved by
(Chairperson, Governing Body)

Date:

Annexure I – IT Account and Access Request Form

1. Name of User	
2. Category (Student / Faculty / Staff / Guest / Vendor)	
3. Department / Section	
4. Enrolment No. / Employee ID	
5. Contact Number & Personal E-mail (for recovery)	
6. Services Requested (E-mail / Wi-Fi / ERP / LMS / Lab Systems / Other)	
7. Level of Access Required and Justification	
8. Period of Access (for guests and vendors)	
9. Undertaking: I have read the IT Policy and Cyber Security Guidelines and agree to abide by them. Signature of User & Date	
10. Approval of Head of Department / Section	
11. User ID Created and Access Granted by (IT Cell) & Date	

Annexure II – Cyber Security Incident Report Form

1. Name, Department & Contact Number of Person Reporting	
2. Date and Time the Incident was Noticed	
3. Type of Incident (Malware / Phishing / Unauthorised Access / Data Leak / Lost Device / Website Defacement / Other)	
4. Systems, Accounts or Data Affected	
5. Description of the Incident	
6. Immediate Action Taken by the User	
7. Received by IT Cell (Name, Date & Time)	
8. Containment and Recovery Actions Taken	
9. Reported to CERT-In / Police / Other Authority (Yes / No, Date & Time, Reference No.)	
10. Root Cause and Preventive Measures	
11. Signature of System Administrator & Date	
12. Remarks of IT Coordinator / Competent Authority	

Annexure III – IT Asset Issue and Return Form

1. Name of Employee / User	
2. Department & Employee ID	
3. Asset Description (Type, Make, Model)	
4. Asset Tag No. / Serial No.	
5. Accessories Issued (Charger, Bag, Other)	
6. Purpose of Issue	
7. Date of Issue & Signature of User	
8. Signature of IT Cell (Issued by)	
9. Date of Return & Condition of Asset at Return	
10. Data Wiped / Accounts Removed (Yes / No)	
11. Signature of IT Cell (Received by) & Remarks	