GURU NANAK INSTITUTE OF TECHNOLOGY

IT Policy

Guru Nanak Institute of Technology
157/F, Nilgunj Road, Panihati
Kolkata-700114

Ref. Number	Compiled & Checked by:	Approved by:
GNIT/IQAC/PRIN/2016/101	HOD, CSE Sig..... Date 14/07/2016	Principal Sig..... Date 14/07/16

Ms. Srabani Kundu
Head of the Department
Department of Computer Science & Engg.
Gurunanak Institute of Technology

Principal
Gurunanak Institute of Technology

Guru Nanak Institute of Technology

Information Technology Policy

Table of Contents

1. Intent:

Increased protection of Information Technology Resources to assure the usability and availability of those resources to all users of Guru Nanak Institute of Technology (GNIT) is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access GNIT's Information Technology Resources.

2. Purpose:

Guru Nanak Institute of Technology recognizes the vital role information technology plays in effecting Institution as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by GNIT's IT resources authorized users , the need for an increased effort to protect the information and the technology resources that support it is felt by Guru Nanak Institute of Technology and hence this Policy.

Since a limited amount of personal use of these facilities is permitted by Guru Nanak Institute of Technology to users, including computers, printers, e-mail and Internet access, therefore, it is essential that these facilities are used responsibly by users, as any abuse has the potential to disrupt institution business and interfere with the work and/or rights of other users. It is therefore expected of all users to exercise responsible and ethical behavior while using GNIT's Information Technology facilities.

3. Reference:

In this Policy, a reference to the following word(s) shall have the following meanings assigned to it.

Information Technology Resources:

Information Technology Resources for purposes of this Policy include, but are not limited to, Guru Nanak Institute of Technology owned or those used under license or contract or those devices not owned by GNIT but intentionally connected to Guru Nanak Institute of Technology -owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and Internet and intranet access.

User:

Anyone who has access to Guru Nanak Institute of Technology's Information Technology Resources, including but not limited to, all employees, temporary employees, probationers, contractors, vendors and suppliers.

Policy:

This Policy includes within its purview the following referred Policies

- The General Information Technology Usage Policy
- The Software Licensing Policy
- The Internet and Intranet Usage Policy
- The E-mail Usage Policy
- The Helpdesk Process
- The Business Continuity Planning and Disaster Recovery

4. Policy:

The use of the GNIT's information technology resources in connection with GNIT's business and limited personal use is a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the Users of GNIT's Information Technology resources efficiently and responsibly.

By accessing GNIT's Information Technology Resources, the user agrees to comply with this Policy. Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject GNIT to any liability. GNIT reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose GNIT to risks of unauthorized access to data, disclosure of information, legal liability, or other potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

5. Scope

This policy applies to everyone who, in India, has access to GNIT's Information Technology Resources and it shall be the responsibility of all Head of the Departments and System Administrator at the institution to ensure that this policy is clearly communicated, understood and followed by all users.

This Policy also applies to all contracted staff and vendors/suppliers providing services to GNIT that bring them into contact with GNIT's Information Technology resources. The HR / Admin department and the respective System Administrator who contracts for these services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy before any access is given to them.

These policies cover the usage of all of the Institution's Information Technology and communication resources, whether they are owned or leased by the institution or are under the institution's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.
- All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services.
- All software including purchased or licensed business software applications, GNIT -written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on GNIT –owned equipment.
- All intellectual property and other data stored on GNIT's Information Technology equipment.
- These policies also apply to all users, whether on Institution property or otherwise, connected from remote connections via any networked connection, or using Institution equipment.

6. General standards for acceptable use of GNIT Information Technology resources:

- Responsible behavior with respect to the electronic information environment at all times.
- Compliance with all applicable laws, regulations and GNIT's policies
- Respect for the rights and property of others including intellectual property rights
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.

7. General Information Technology Usage Policy

7.1 Passwords

- Individual password security is the responsibility of each user.
- Passwords are an essential component of GNIT's computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. Hence passwords must not be easy to guess like Name/Phone Number/ Date of birth etc. It also should not be a common word found in the dictionary or some other part of speech.
- To make guessing more difficult, passwords should also be at least eight characters long. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change passwords every 60 days. Password history would be maintained for

previous three passwords. This applies to the Systems Logon (windows password) and Mail Passwords.

- Passwords must not be stored automatic log-in scripts, or in locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.

  Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be changed by the user to ensure confidentiality of all information.

- Under no circumstances, Users shall use another user's account or password without proper authorization.

- Under no circumstances, the user must share his/her password(s) with other user(s), unless the said user has obtained from the concerned System Administrator the necessary approval in this regard. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.

- In cases where no prior approval had been obtained for sharing of password(s) with other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this Policy and GNIT shall initiate appropriate disciplinary proceedings against the said user.

7.2. Access Control

- All GNIT computers that are connected to the internal computer networks must have a password-based access control system. Irrespective of the network connections, all computers handling private information must also employ proper password-based access control systems.

- All in-bound connections to GNIT computers from external networks must be protected with an approved password or ID access control system. Modems, Wi-Fi models, routers/USB devices may only be used at GNIT after receiving the written approval of the System Administrator and must be turned off when not in use.

- All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user. Users are prohibited from logging into any GNIT system anonymously. To prevent unauthorized access all vendor-supplied default passwords must be changed before use.
  Access to the server room should be restricted with RFID lock and only recognized IT staff or someone with due authorization from System Administrator is permitted to enter the room.

- Users shall not make copies of system configuration files (e.g. Passwords, etc.) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

7.3. Managing System Privileges

- Requests for new user-IDs and changes in privileges must be made to the System and Network administrator department in Mail. Users must clearly state why the changes in privileges are necessary.
- In response to feedback from the Human Resources Department, the System and Network administrator department will revoke any privileges no longer needed by users. After receiving information from HR / Admin department all system access privileges will be terminated within 24 hours when a user leaves GNIT.
- GNIT administration reserves the right to withdraw the system privileges of any user at any time. Conduct that affects the normal and proper operation of GNIT Information Technology resources, or which is harmful or offensive to others will not be permitted.

7.4. Changes to Systems

- No user must physically connect or disconnect any equipment, including GNIT owned computers and printers, to or from any GNIT network.
- With the exception of emergency situations, all changes to GNIT information technology systems and networks must be documented, and approved in advance by the System Administrator.
- Only persons who have been authorized by the System Administrator can make emergency changes to a GNIT computer system or network.

7.5. Security (Access Control)

- Users are forbidden from avoiding security measures.
- Users are strictly prohibited from establishing dial-up connections, using modems/routers/Wi-Fi Adaptors/Hotspots/USB devices or other such apparatus, from within any GNIT's premises.
- Users who have been given mobile/portable laptop / palmtop or any other device and duly authorized for such remote access, which connects to GNIT's mail system on a real-time basis, can do so through the Internet.
- Unless the prior approval of the System Administrator has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to GNIT systems and information. These connections include the

establishment of multi-computer file systems, Internet web pages & FTP servers.

- Users must not test, or try to access computer or communication system security measures unless specifically permitted in advance and in writing by the System Administrator. Incidents involving hacking, password guessing, file decryption, software copying, computer configuration changing or similar unauthorized attempts to change security measures will be considered grave violations of GNIT policy. Similarly, attempt to avoid system security measures is absolutely forbidden.

8. Software Licensing Policy

- For all software including purchased or licensed business software applications, GNIT -written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on GNIT -owned equipment, all users must comply with the software licensing policy and must not use/install/download any software for their individual use or even for business purpose without prior approval of the System Administrator at corporate office. In case any such software is found on any GNIT system which is not allocated to the individual user, it shall be the responsibility of the user to inform the same to the System and Network administrator department, in cases the same is not installed by the said user otherwise GNIT shall initiate appropriate disciplinary proceedings against the said user.

- All necessary software's are pre-installed on all GNIT systems for day-to-day office needs. Request for any additional needs to be addressed to the System Administrator for approval.

- Use of GNIT network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

9. Internet and Intranet Usage Policy

- Internet software may only be installed / used by or with the approval of the System Administrator. Software patches or updates may only be downloaded, subject to approval and ensuring strict adherence to the vendor's security and usage guidelines.

- Access to the internet and its resources is provided for the purposes of conducting business on behalf of GNIT. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out by the Cyberoam UTM 500 iNG Firewall.

- The System and Network administrator department reserves the right to block access to any Internet resource without any prior notice, in case anyone required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for official purpose and conducting GNIT business. The approval for the same needs to be

obtained by the Department Head from the System Administrator.

- Similarly, to protect GNIT's IT systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted.

- Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the GNIT network or the internet or bypass security features.

10. Email Usage Policy

- All authorized users of GNIT are provided with an E-mail account, which is either individual to the specific user or generic Email ID and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose; however personal mail can also be exchanged to a limited quantum provided that such exchange does not amount to breach of this IT policy or otherwise materially affects GNIT's operations. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by System and Network administrator department without any prior information, however the same may be re-instated with the approval from the Principal and System Administrator at the corporate office.

- Email users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence exchange of information should be limited to reliable sites. Users are prohibited to use their names/e-mail ids/mail domain in public domain without prior authorization from System Administrator.

- Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation of the country or which brings the organization into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via email.

- All material contained on the email system belongs to the GNIT and users should consider messages produced/received by them on GNIT account to be secure. The confidentiality of email data should be maintained by the individual user.

- Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of

providing their email addresses to external parties, especially mailing lists.

- Users transferring or receiving files or attachments from external sources should note that the GNIT system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the System and Network administrator department immediately for inspection and action.
- GNIT email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. GNIT provides the email system for the purposes of conducting official business and it may not be used for personal gain or business activities unrelated to GNIT's operations. Users must not use the system to promote an external cause without prior permission from the System Administrator.
- Reasonable personal use of the email system is permitted. Personal use of the e-mail service must not interfere with GNIT's operations, involve cost implications for GNIT or take precedence over the user's job accountabilities.
- Where it is considered that there has been a breach in the use of the email system, the service of the user will be terminated without any prior information.

11. Help deskProcess

All help and support pertaining to the system/user/network/back-end shall be provided by the System Administrator. In case any user finds any problem with the IT systems or need any help, they can send in their request to the System Administrator via e-mail to gnit.digital@gnit.ac.in, with a cc to the System Administrator, sysadmin@jisgroup.org.

12. Data Backup

In order to prevent loss of information by damage of the secondary memory in which it is stored, a periodic backup procedure is carried out in Google Cloud and Microsoft Azure Cloud storage. The responsibility for backing up the data is of the System Administrator's.

- **General Rule**: Periodic backup of on every fortnight is maintained for overwriting the old data with the new backup. Central systematic periodic backups are being planned for future implementation.
- **Data Backup in File Servers**: The Systems Management does back up of all the information in the file servers through an automated procedure.
- **Data Backup in Database Servers**: The Systems Management does back up of all the information in the databases through an automated procedure.
- **Data Backup in Desktop PC and Notebook**: This task is the responsibility of the user to whom the computer has been assigned.

Ammended & Approved By BOG
Dated.....6/10/2020.....
Under Agenda Number.....15.....

Revision of IT Policy (2020)

Updated and approved by BoG on 06/10/2020 Agenda no 15.

The IT Policy has been amended in Agenda No. 15 which is to be read as:

- **Cyber security measures to be enhanced to reduce exploitable weakness and attacks:**

Most software vendors work diligently to develop patches for identified vulnerabilities. But even after patches and updates have been released, many systems remain vulnerable because organizations are either unaware of or choose to not implement these fixes. System Administrator should ensure periodical updates of Operating System and Application Software for secured operation of the systems.

- **Develop and Enforce Policies on Mobile Devices:**

The proliferation of laptops, tablets, smartphones, and other mobile devices in the workplace presents significant security challenges. The mobile nature of these devices means they are potentially exposed to external compromised applications and networks and malicious actors.
Therefore, it's important to develop policies on the reasonable limits of mobile devices in GNIT's networks. Devices should also be password protected to ensure that only authorized users can log-in. Otherwise, an unauthorized user can gain access to restricted networks and files using an authorized user's device. Similarly, employees should avoid or be cautious about using devices that do not belong to them as they cannot be sure these are properly protected or comply with established policy. Such devices may actually be infected, and using them could put the information and networks access at risk.

- **Implement an Employee Cyber security Training Program:**

When employees aren't involved in cyber security, not only can vulnerabilities and threats go unnoticed but the employees themselves can become conduits through which attacks are executed. Therefore, employees should receive initial and periodic cyber security training, helping to maintain the security of the organization as a whole.

- **Enhancement of Internet Bandwidth:**

To support Online Mode of Education, Internet speed has been increased up to 500 MBPS.