Narula Institute of Technology

81, Nilgunj Road,
Agarpara,
Kolkata-700109, WB

IT Policy
Version: 1.0
(2015-16)

Approved by BOG
Dated on 12/03/2016
Under Agenda No. 16

Ref. No: NIT/IT Policy/ 2015-16 / 01 Date of Issue: 19/03/2016	Compiled By: System Admin, Narula Institute of Technology	Checked By: HOD, IT, Narula Institute of Technology	Approved By: Principal, Narula Institute of Technology

Policy for Information Technology – ver 1.0

Table of Contents

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

Approved by BOG
Dated on 12/03/2016
Under Agenda No. 16

Policy for Information Technology – ver 1.0

1. Intent:

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

2. Purpose:

NiT recognizes the vital role information technology plays in effecting institutional activities, academic purpose as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by NiT'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 NiT and hence this Policy.

Since a limited amount of personal use of these facilities is permitted by NiT 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 institutional activities, academic purpose 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 NiT's Information Technology facilities.

3. Reference:

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

3.1. Information Technology Resources:

Information Technology Resources for purposes of this Policy include, but are not limited to, NiT owned or those used under license or contract or those devices which are connected to NiT-owned Information Technology Resources such as computer hardware, printers, software, E-mail and Internet and intranet access.

3.2. User:

Anyone who has access to NiT's Information Technology Resources, including but not limited to, all teaching and non-teaching staffs.

3.3. 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

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

- The Helpdesk Process

4. Policy:

The use of the Information Technology Resources of NiT in connection with institutional activities 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 NiT's Information Technology resources efficiently, effectively, securely and responsibly.

By accessing NiT's Information Technology Resources, the user agrees to comply with this Policy. Users also agree to comply with the applicable Cyber laws and licenses and to refrain from engaging in any activity that would subject to NiT to any liability. NiT reserves the right to amend these policies and practices at any time without prior notice. Any action that may expose NiT to risks of unauthorized, unauthenticated access to data, disclosure of information, legal liability, or other potential system failure is strictly 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, wants to access NiT's Information Technology Resources and it shall be the responsibility of Departmental Heads, System Admin to ensure that this policy is clearly communicated, understood and followed by all users.

This Policy also applies to those who providing services to NiT that bring them into contact with NiT's Information Technology resources. The Admin department who contracts for these services shall be responsible to provide a copy of this Policy before any access is given to them.

These policies cover the usage of all of the Information Technology and Communication Resources of the institute, whether they are owned by the institute or are under the institute's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, wireless computing devices, telecomm equipment, networks, databases, printers, scanners, servers and computers connected through internet and intranet in the campus, and all networks and hardware to which this equipment is connected.

- All electronic communications equipment, including telephones, voice- mail, E-mail, wired or wireless communications devices and services, Internet and Intranet and other on-line services.

- All software including purchased or licensed software applications, NiT written applications, computer operating systems, firmware, and any other software residing on NiT –owned equipment.

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

6. General standards for acceptable use of NiT Information Technology Resources require:

- Responsible behavior with respect to the electronic information environment at all times.
- Compliance with all applicable laws, regulations and NiT'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.

7. General Information Technology Usage Policy

7.1. Passwords

- Individual password security is the responsibility of each user.
- Passwords are an essential component of NiT's computers and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single 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 and combination of letters (uppercase and lowercase), numbers and special symbols. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change passwords in regular interval. 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 in readable form in computers without access control systems, or in other 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 the necessary approval from the concerned System Admin 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 NiT shall initiate appropriate disciplinary proceedings against the said user.

Principal
Narula Institute of Technology
81, Nilganj Road, Agarpara
Kolkata-700 109

7.2. Access Control

- All in-bound connections to computers of NiT 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 NiT after receiving the written approval of the System Admin 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 system of NiT anonymously. To prevent unauthorized and unauthenticated access, all supplied default passwords must be changed before NiT's use.

- Access to the server room should be restricted with RFID lock and only recognized IT staff or someone with due authorization from System Admin 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 admin in mail. Users must clearly state why the changes in privileges are necessary.

- In response to feedback from Admin department of NiT, any privileges no longer needed by users will be revoked. After receiving information from Admin department, all system access privileges will be terminated within 24 hours when a user leaves the institute.

- Management of NiT reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of NiT information systems, which adversely affects the ability of others to use these information systems, 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 NiT's owned computers and printers, to or from any network of NiT.

- With the exception of emergency situations, all changes to Information Technology Systems and networks of NiT must be documented, and approved in advance by the System admin.

- Only persons who have been authorized by the System Admin can make emergency changes to any computer system or network of NiT.

7.5. Security (Access Control and Cyber Security)

- Users are forbidden from circumventing 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 NiT'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 mail system of NiT on a real-time basis, can do so through the Internet.

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

- Unless the prior approval of the System Admin has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to systems and information of NiT. These connections include the establishment of multi-computer file systems, Internet web pages & FTP servers.

- Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the System Admin. Incidents involving the following will be considered serious violations of NiT's IT as well as Cyber Security policies and will be dealt with stringently, leading to (but not limited to) criminal proceedings, fine (amounting to monetary loss incurred due to loss of company data plus taxes), and/or sacking:

  - unapproved system cracking (hacking)
  - password cracking (guessing)
  - file decryption
  - software copying
  - unauthorized copying and replication/duplication of job responsibilities from respective allotted PC/devices
  - changing of computer configuration or similar unauthorized attempts to compromise security measures
  - attempts to bypass system security measures
  - installation of unauthorized software application
  - patch updates and system updates installation
  - unauthorized use of USB devices without prior Virus/malware scanning
  - non-reporting of phishing attacks and loss of personal devices like cellphones, laptop/notebooks, IPads, any smart devices
  - sharing of company information/data, without authorization, in social media/online/public platforms

8. Software Licensing Policy

- Devices of NiT only use licensed softwares (both system softwares and application software) and strictly follow the NASSCOMs advisory on usage and distribution of properly purchased and licensed software. The entire institute is bound by Microsoft Campus Agreement and maintains proper PO, challans relating to software purchases.

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

- For all software including purchased or licensed software applications, NiT – written applications, employee and supplier-written applications, computer operating systems, firmware and any other software residing on NiT -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 Admin. In case any such software is found on any system of the institute which is not allocated to the individual user, it shall be the responsibility of the user to inform the same to the System Admin, in cases the same is not installed by the said user otherwise NiT shall initiate appropriate disciplinary proceedings against the said user.

- All necessary softwares are pre-installed on all systems of NiT for day-to-day office needs. Request for any additional needs to be addressed to the System Admin for approval.

- Use of network resources of NiT 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 Cyber law or by the owner of the copyright.

9. Internet and Intranet Usage Policy

- Access to the internet and its resources is provided for the purposes of conducting institutional activities, academic purpose on behalf of NiT. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out by the Sonicwall/Cyberoam/Fortigate Firewall/UTM.

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

- The System Admin has 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 institutional activities of NiT. The approval for the same needs to be obtained by the Department Head from the System Admin.

- Similarly, to protect NiT'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 network of NiT or the internet or bypass security features.

10. E-mail Usage Policy

- All authorized users of NiT are provided with an E-mail account, which is either individual to the specific user or generic E-mail 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 institutional activities, academic 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 NiT's operations. Incase any individual is found using E-mail service, which is objectionable by any means, the access can be terminated without any prior information, however the same may be re-instated with the approval from the Principle and the System Admin.

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

- E-mail 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 the System Admin.

- 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 Cyber law or regulation of the country or which brings the institute into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via E-mail.

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

- Security regarding access to the E-mail system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their E-mail addresses to external parties, especially mailing lists.

- Users transferring or receiving files or attachments from external sources should note that the system of NiT 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 Admin immediately for inspection and action.

- E-mail users of NiT are required to use this communication tool in a responsible fashion and to observe the related guidelines. NiT provides the E-mail system for the purposes of conducting institutional activities and it may not be used for personal gain or activities unrelated to NiT's operations. Users must not use the system to promote an external cause without prior permission from the System Admin.

- Reasonable personal use of the E-mail system is permitted. Personal use of the E-mail service must not interfere with NiT's operations, involve cost implications for NiT or take precedence over the user's job accountabilities.

- Where it is considered that there has been a breach in the use of the E-mail system, the service of the user will be terminated without any prior information.

11. Helpdesk Process

- All help and support pertaining to the system/user/network/back-end shall be provided by the NiT IT helpdesk executives. In case any user finds any problem with the IT systems or need any help, they can send in their request to NiT IT helpdesk via E-mail to it_helpdesk@nit.ac.in.

- NiT IT helpdesk team shall be constituted from its staff members. The group shall be headed by the System Admin and should consists of those staffs who are conversant with basic IT troubleshooting and protocols and must possess technical acumen and problem-solving skills.

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

- All calls to the IT helpdesk, via email or phone call, should be resolved within a timeframe of 2 to 3 working days, depending on the nature of call logged.

- The IT helpdesk team should conduct a meeting at the end of each week to review the present week's performances and plan for the coming week. All unresolved calls must be thoroughly reviewed and further plans to resolve the issues shall have to be communicated with the call- logging department's head.

- All troubleshooting calls should be properly documented with the following:
    - SL No of the call
    - Date
    - Time of call logging
    - Source (dept name)
    - Name of the person logging the call
    - Description of the problem
    - Name of the person attending the call
    - Time of resolution of the call
    - Date of resolution of the call

- The IT helpdesk team shall be responsible in enforcing and maintaining Cyber Security rules and protocols and conducting periodic checks to find any gaps/violation of the said rules with proper reporting of the same to the System Admin.

12. Data Backup

In order to prevent loss of information by destruction of the backup tapes/HDDs/network drives in which all departmental backed-up data is stored, a periodic backup procedure/process is to be carried out. The responsibility for backing up the information located in shared access servers is with the System Admin/IT Helpdesk team. Periodic backups should be performed either manually or through automatic configurations. The type and amount of data that is to be backed up is to be selected and chosen by the individual department. Since both HDDs and magnetic tapes are quite prone to errors that destroy their contents and are inclined to fail, greater importance is to be given to cloud/network backups with failsafe mechanisms.

- **General Rule:** Presently all backups happen in adhoc basis. A fixed timeline is maintained for overwriting the old with the new backups. Central systematic periodic backups are being planned for future implementation.

- **Data Backup in File Servers:** The Systems Management backs up all the information in the file servers through an automated procedure.

- **Data Backup in Database Servers:** The Systems Management backs up 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.

Principal
Narula Institute of Technology
81, Nilgunj Road, Agarpara
Kolkata-700 109

Approved by BOG
Dated on 12/03/2016
Under Agenda No. 16