GNIOT
Group of Institutions
Since 2001

GNIOT
ENGG. INSTITUTE

4.3.1

Institution frequently updates its IT facilities and provides sufficient bandwidth for internet connection

Greater Noida Institute of Technology (Engg. Institute)

Plot No. 7, Knowledge Park II, Greater Noida
Uttar Pradesh 201310 India

GNIOT GROUP OF INSTITUTIONS

योगः कर्मसु कौशलम्

WE GROOM TALENT

GNIOT

Group of Institutions

Since 2001

GNIOT

ENGG. INSTITUTE

4.3.1

IT Policy

Greater Noida Institute of Technology (Engg. Inst.) * Greater Noida * Director

Greater Noida Institute of Technology (Engg. Institute)

Plot No. 7, Knowledge Park II, Greater Noida
Uttar Pradesh 201310 India

Information Technology (IT) Policy

(Greater Noida Institute of Technology)

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

INDEX

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

1. Introduction

It is the purpose of the Greater Noida Institute of Technology (Institute) IT policy to preserve, protect, and guarantee the legal and appropriate utilization of the information technology infrastructure that was developed by the Institute on the campus. This policy outlines Institute -wide strategies and responsibilities for protecting the confidentiality, integrity, and availability (CIA) of the information assets that are accessed, created, managed, and/or controlled by the Institute. CIA is an acronym that stands for confidentiality, integrity, and availability. The policy takes into consideration a wide variety of information assets, such as data, information systems, computers, network devices, and intellectual property.

Both educational institutions and research organizations now rely heavily on the capabilities provided by their own intranets and the Internet. In 2001, the Institute (Engineering Institute) took the initiative to develop fundamental network infrastructure within the Institute academic complex.

Not only has the number of people actively using the network facilities increased significantly over the past few decades, but also the number of people using web-based apps has grown. This is an improvement that should be made to the academic atmosphere at the Institute.

About 855 network connections are spread across Institute's four buildings, making the entire campus accessible. The Institute's internet and intranet services are both managed by the Internet Unit, which is the department that has been charged with taking on this role.

The Computer Centre is responsible for the management of the Institute network as well as the operation of the Firewall security system, DHCP, DNS, email, web, and application servers.

City line Network is providing Institute with bandwidth for its Internet connection. The total bandwidth that is available comes from Airtel at 1.0 Gigabits per second (leased line), while Tata provides a backup line with 100 Megabits per second. This dedicated line, which was offered by City line Network Communication.

During the process of developing these policies, every effort has been taken to strike a careful balance between the need for security and the users' need to be able to carry out the functions that are rightfully theirs. In addition, because of the fluid nature of information technology, information security in general as well as the regulations that govern the information security process are both fluid in their nature. They need to be looked at on a regular basis and adjusted so that they are in line with evolving technological standards, the shifting expectations of the user community of information technology, and the shifting operating procedures. The purpose of an IT policy is to establish a direction and provide information about behaviors that are permissible as well as acts that are banned or that violate policy.

Greater Noida Institute of Technology (Engg. Inst.)
Director
Greater Noida

Guidelines are developed and made available in order to assist individuals, organizations, and departments that are a member of the Institute community in gaining an understanding of how Institute policy applies to some of the most significant areas and achieving conformance with the policies that have been established.

The following categories make up the subsets of the present IT policy:
• The Policy Concerning IT Services
• A policy for backing up data applicable to faculty, staff, and students
• The Installation Protocol for IT Hardware
• Guidelines for the Acquisition and Activation of Software Licenses
• The helpdesk policy for IT Services
• Guidelines for the Use of Networks (Including the Internet and Intranet)
• The Acceptable Use Policy for Email Accounts
• The Hosting Policy for Websites
• Guidelines for the Use of the Institute Database
• A Policy for the Use of CCTV Surveillance
• Power Backup protocol for information technology hardware
• Protection of Privacy and Data in Cyberspace
Conducting Policy Evaluations and Changes

In addition, the policy will be implemented in two different levels:
1. Groups of End Users (including Teachers, Students, Senior Administrators, Officers, and Other Staff Members)
2. Administrators of Computer Networks

It should be brought to your attention that the Institute IT Policy applies to

1. The technological infrastructure that is managed either centralized by the Institute or locally by each department
2. The information services that are supplied by the Institute administration, or by the separate departments, or by individuals who are a part of the Institute community, or by authorized residents or non-residents who are using their own hardware to connect to the Institute network are referred to as "information services."
3. The resources that are managed by the central administrative departments, such as libraries, computer centers, laboratories, offices of Institute-recognized associations and unions, or hostels and guest homes, or dwellings located in areas where the Institute provides the network facility.

4. When connected to the campus network, computers that are owned by people or those that are held by research projects of the faculty are subject to the Do's and Don'ts outlined in the Institute IT policy. This applies whether the computer is owned by the research project or the individual.

In addition, everyone who is eligible to receive authorization to use the information technology infrastructure of the Institute, including faculty, students, staff, departments, authorized visitors/visiting faculty, and others, is required to comply with the standards. This includes both authorized visitors and visiting faculty. In the event that any Institute member is found to have violated this IT policy, the Institute authorities reserve the right to take disciplinary action against the member in question.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

2. Policy Regarding IT Services

The teachers, staff, and students all have access to a comprehensive range of computing and communication facilities thanks to IT Services. A crystal clear user focus, with the goal of "providing a high quality service," is maintained by IT Services. This focus, which

- Ensuring services fulfil user requirements
- Keeping an eye on how well the services are performing
- Providing a service that is efficient with regard to costs
- Employing a versatile method of operation that is congruent with the Institute vision
- Maintaining an open line of communication with users and ensuring that they are kept up to date
- Ensuring the contentment of the users

The services that are offered by IT will be outlined in detail as the goal of this policy. The following are examples of the services that IT manages:

1. Computing on desktops and laptops, as well as support
2. Hardware and networks at the heart of the central computer system
3. The strategy for information technology and the implementation of new systems
4. Normal daily operations of the systems that are already in place

The following provides a concise overview of the variety of services that can be obtained through IT Services.

1. Personal computer workstations and technical support
2. For the majority of users, the IT Helpline serves as their initial point of contact with IT Services. Helpline Advisers are trained to assist callers with a wide variety of standard questions and concerns and to ensure that issues are resolved. In addition to this, the Helpline handles requests for new information technology equipment and oversees contacts with all staff members regarding the availability of services for all systems.
3. Standard Hardware IT Services provide advice and recommendations for the selection of IT hardware. This covers purchases made with money obtained from outside sources or for research. In addition to this, IT Services will coordinate the ordering of any and all IT hardware and software to guarantee the most cost-efficient investment possible in IT.

4. Pay for Use of Software

The desktop software that Institute uses is licensed by Microsoft under the terms of a central license agreement. A recommended software list provides access to additional software that has undergone the appropriate testing and evaluation. Through the helpline provided by IT Services, software requests can be sent.

5. Support for desktops and laptops, including audio and video.

Help for about 855 desktop and laptop computers used by Institute. Core support includes:

- The setting up of the appropriate software
- The configuration of network connections, access to email and Internet, as well as network file space and
- Fault diagnosis
- Installation of patches for both the software and the hardware
- Hardware and networks of the central computer system

Greater Noida Institute of Technology (Engg. Inst.)
Director
Greater Noida

6. Networks is in charge of managing all of the Institute networks, which includes the mobile network for the campus and, more crucially, its connection, which links all of the other networks together.

7. Servers

The administration of the core servers that make up the Institute, which are located in data centers that have been purposely built with high levels of security and climate control. Server back-ups, upgrades, fixes, and service enhancements are some of the most important activities. These servers are responsible for hosting the primary Institute systems, as well as the systems of individual departments, websites, and network file space for students and employees.

8. Telecommunications

The Institute's telephone systems, including all cordless telephones, desk sets, and mobile phones, are managed by IT Services, which are responsible for the organization's overall IT infrastructure. Maintaining information technology security and anti-virus protection, as well as offering advice and guidance.

9. Creating and maintaining "images" of standard and specialized software for use on staff computers, open access locations, and in the computer lab for instruction purposes. Additionally, IT Services keeps a Institute wide printer strategy, which includes the deployment of MFP and Scanner devices.

10. Normal daily operations of the systems that are already in place

a. Support entails taking care of a wide variety of the university's preexisting systems by diagnosing and resolving any issues that crop up, as well as installing and testing any upgrades or patches provided by the vendor.

b. Enhancement refers to the process of working with users and suppliers to describe, build, and test modifications to already existing systems as new needs arise.

c. Institute Integration Developing and managing the integration points between existing systems Identity Management: Supporting and maintaining identity and access to systems by offering a single view of a user's identity across the Institute Integration Supporting and maintaining identity and access to systems by giving a single view of a user's identity across the Institute

11. Services Related to Operations

a. Help Desk for Computer Issues and Problem Solving

b. Access to the institute's various networks and the internet requires a new username and password.

c. a new or refurbished standard personal computer

d. Hardware that is specialized for computers

e. Mobile phone or mobile computing device

f. Software designed specifically for specialists

g. Desktop software

h. Access to the network as well as connectivity via Wi-Fi

i. Personal Storage

j. Students and faculty can use the email services.

Greater Noida Institute of Technology (Engg. Inst.)
Director
★ Greater Noida ★

First line support for staff, students, and external clients is accessible 24 hours a day, 365 days a year. This service is included in the provision of the services.

The IT team keeps track of all open incidents and reports those that cannot be handled to people and organizations that can provide assistance in resolving the issue. In the event that a problem presents itself, we will address it based on an initial evaluation performed using a severity table.

Complaints and Feedback

Feedback from Users

Please let us know as soon as possible if you are an end-user who would like to provide feedback or are not pleased with the services that we provide. This will allow us to do everything in our power to make things right. Management reads through every comments in order to assess the level of user satisfaction and ensure that our services are continuously improved. Please utilize our E Mail- itsupport@gniot.edu.in

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

3.The policy for backing up data, applicable to academics, staff, and students

The Scope of the Procedure and the Justification

The major objective of the data protection strategy is to ensure the safety of Institute's data by copying it to a secondary site that is geographically distinct from the location of the original data storage. Electronic backups are required in order to enable the recovery of data and applications in the event that anything catastrophic happens to the system, such as a natural disaster, a failure of the system disc drive, sabotage, ransomware, errors in data entry, or faults in system operations.

Utilized Technology

At this time, the data on all Institute level systems is backed up using a technology that is based on duplicate discs. In the secondary and tertiary backup data centers are where the various backup solutions are stored. The cloud storage service is used for the primary backup. A backup of the live data will be performed to our storage facility located in the primary data centre at predetermined time intervals, in accordance with the requirements outlined in a backup plan. This data is regarded to be backup data and it represents a certain point in time. The two sites consist of the live data and the backup data for the vast majority of non-critical computer systems. Using our Storage Area Network (SAN) technology, we are able to replicate data that is considered to be of mission-critical importance across many locations. This Institute grantee requires that the data be stored in at least two locations simultaneously, one as a live production mode and the other as a point-in-time backup data at the second location.

Data is replicated to the tertiary backup data centers when it is deemed necessary for the data to have an increased level of security since it is mission-critical data. Only a subset of Institute's mission-critical systems, which are more often known as Disaster Level Zero (DR0), are allowed to make use of replicated data solutions.

Availability of the Service

One of the potential options is independent backup service provision. The provision of backup services is included in the provision of storage services. The storage and backup services that are included in the package are done largely through the use of the cloud, and a secondary storage and backup option is offered in the datacenter through the use of WD4TB(2/2)

The backup service is utilize for student records, such as academic details, student login records, and admission records for students. In addition, a backup of the students' web activities is kept (this is accomplished through the use of student logins). Employee records consisting of information on the employee's job, qualifications, income records, attendance (presence, absence, leaves (used, remaining), in and out timings), and leaves (used, remaining).

Included in the faculty records are the individuals' qualifications, as well as the faculty development programmes they have attended or organized, the research work they have done (ongoing or published), and the e-learning content they have created. These records are kept under the categories of both the department and the school simultaneously.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

To keep track of the activities of administrative staff members on the web (which is accomplished with the help of the staff login), records are preserved. Additionally, the IT Team is responsible for the maintenance of access records for Institute portals such as RF campus, LMS, and INPODS.

Records of all of the academic and non-academic events, including information on the organizing committee, participants, advertising, images, videos, and financial details, are kept. These records include information on both academic and non-academic activities.

Guidelines

The establishment of the guidelines for the regulations governing the backup of electronic information is the goal of these guidelines. All personnel responsible for the installation and support of technological resources, all individuals charged with the security of technological resources, and data owners are required to adhere to these rules.

Responsibilities

When necessary modifications arise, technology resources and data owners are obligated to keep the Infrastructure Operations Security (IOS) organization informed of the situation. The responsibility for data backup, validation, and testing lies with the owners of the data as well as the technology resources. The IT Department will NOT be accountable for any data backups that are either corrupt or incomplete.

Greater Noida Institute of Technology (Engg. Inst.) * Greater Noida *
Director

4. Policy for the Installation of IT Hardware

At the Institute, the expected lifespan of any desktop computer, laptop, or peripheral device should be at least three years. In the event that a desktop computer, a laptop computer, or a peripheral device experiences a fault that cannot be rectified, then the device should be replaced, but only when it has reached the end of its minimum life. It is the job of the Information Technology team to oversee the purchase of desktop computers, laptops, and accessories for each of the departments.

It is forbidden for any member of the teaching or administrative staff to have more than one computer (desktop or portable). After getting the consent of the IT Manager, the devices whose guarantee periods have run out will be evaluated, and any necessary maintenance will be performed on them.

At the beginning of each academic year, the IT Manager evaluates and prepares the reports, as well as arranges the replacement of equipment, in collaboration with the Institute fraternity. Applications for replacements that are not part of the typical replacement cycle are sent to the IT Manager to be considered.

The following criteria will determine how the replacement applications are handled:

1. Guarantee time has come to an end.
2. a new piece of equipment or a requirement that has become more relevant in the real world.
3. Emerging technologies or standards for the workplace.
4. Multiple instances of malfunctioning.
5. There is room in the budget.

The Manager of Information Technology is responsible for evaluating specialised sales agents and consulting with them in order to select the national and worldwide brands that are the best fit for Institute in terms of quality of model, price, and efficiency.

The Manager of Information Technology is responsible for overseeing the process of purchasing and distributing desktop computers, laptops, and other auxiliary devices.

After going through the approval process with the Manager of Information Technology, each of the desktop and laptop computers comes preinstalled with an operating system that has been tailored to meet the requirements of the various colleges and departments.

Documentation is required for the procedures involving the distribution and replacement of the devices.

1. Because of the force of repulsion.
2. The relevant dean or HOD will check the slip before it is accepted.
3. It is necessary to return any outdated or broken products.

E-waste management is carried out in line with the E- Waste (Management) Rules, 2016 (amendment, 2018) [Government of India]. These rules stipulate that the authority is responsible for ensuring that electronic trash is delivered to authorized recyclers or dismantlers on an annual basis, and that this process is accompanied by the completion of the necessary documentation.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

5. Policy Regarding the Installation and Licensing of Software

The goal of this Policy is to highlight the importance of compliance with software licensing provisions and to identify particular responsibilities that are related to this compliance. This Policy also has the purpose of defining specific obligations that are related to this compliance.

The Head of Department is the one who is responsible for ensuring that all software license requirements are met.

The following are the specific responsibilities:

- You will need to keep a register in order to give confirmation that software was purchased.
- Keeping a record of the software that has been sold and then disposed of (for instance, software that was sold along with a computer).
- Keeping track of an inventory that details the locations of licensed software installations. The redistribution of software within the department needs to be monitored by this.

The Information Technology Department conducts software compliance audits on occasion in order to fulfil its responsibility of ensuring that all licensing criteria are met.

The Institute advocates the use of in order to guarantee that pupils will receive an ongoing education.

- Free and public domain software
- The ability to conduct practical exercises in a virtual environment
- LMS complier
- Software with a valid license
- Online certifications can be obtained through Coursera.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

6. Rules for the helpdesk provided by IT Services

The IT Team offers a wide range of different types of technical support to students, professors, and staff in order to improve education by utilizing various forms of technology. The hours that the help desk for information technology is open are as follows: Monday through Saturday, 9:00 AM to 5:00 PM (excluding on holidays).

Campus Support Request

- Get Support through ERP

The user can file the complaint by using the option that is provided in the ERP system that Institute has, which involves entering in with an authorized ID and password, and then providing the completed details of the problem or issue that was encountered. It is strongly recommended that the complainant provide accurate contact information, particularly their mobile phone number.

- You can get support through e-mail.

The user can send an email to our helpdesk requesting assistance with the following information: Please include your name, email address (if different), phone number, and a brief explanation of the issue.

- Call Us, If you are unable to access your email or the internet, you can get in touch with the information technology help desk at.
- Visit Computer Centre

You have the option of physically going to the Computer to file the complaint there.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

7. Use Guidelines for the Network (Including Intranet and the Internet)

The Institute commits to taking all precautions, both reasonable and suitable, to prevent unauthorized access to or disclosure of any information that is shared with it. The Institute makes every effort to put in place safety protocols that prevent the data it collects from being lost, misused, or corrupted in any way. The Institute is responsible for the administration of a computer security policy.

The Information Technology Manager is accountable for ensuring that all information that is stored on computer systems is protected in a manner that is compliant with government regulations. It is generally accepted that Institute (Engineering Institute) owns all of the information that is stored on the computers that it maintains. Only users who have been authorized by Institute are permitted to access the organization's computer systems. The individuals who are responsible for the institution's data are the ones who decide who can use administrative applications.

Authorized users are accountable for the following:

- Ensuring that the confidentiality of their passwords is preserved.
- Ensuring that any removable media that may contain private or vital information are kept in storage units with locks when they are not in use, or that they are kept in areas that are locked when they are not in use;

- Backing up crucial data maintained on their Computers' hard disks.
- Making certain that only approved software is installed on any computer system belonging to a Institute. PC software packages that have been developed, approved, or installed by the Office of Information Technology are considered to be authorized. Authorized PC software packages can also be bought from trustworthy vendors that guarantee their products. Use of unauthorized computer software and programmes, such as software obtained via unauthorized computer bulletin boards, friends, other employees, etc., is strictly prohibited. This includes software used on personal computers.

- Preventing viruses from infecting Institute PCs by utilizing legitimate anti-virus software and scanning discs.
- Making certain that no unlawful copies are made of software that has been installed on Institute systems.
- Creating documentation for confidential or mission-critical computer programmes that were designed for departmental usage and are utilized to conduct Institute business.
- Ensuring that the privacy of every record is protected at all times, as stipulated by the relevant Institute policy as well as the federal and state laws.
- Preventing access by either logging out of all computer systems or utilizing a screen saver that includes a password protection feature. When utilizing a screen saver that requires a password in order to be activated, this password should only be known by the person who is in charge of that particular workstation.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

Arrangements Regarding Safety:

The Firewall – Nebro was utilized to ensure the safety of the network that is utilized by the Institute.

Cyberoam's product range offers network security (Firewall and UTM appliances), Cyberoam network security appliances include multiple features like Firewall – VPN (SSL VPN & IPsec), Gateway Anti-Virus, Anti-Spyware & Anti-Spam, Intrusion Prevention System (IPS), Content &Application Filtering, Web Application Firewall, Application Visibility & Control, Bandwidth Management, Multiple Link Management for Load Balancing and Gateway Fail over, over a single platform.

Greater Noida Institute of Technology (Engg. Inst.) * Greater Noida *
Director

8. Use Guidelines for Your Email Account

It is suggested to use the Institute's e-mail services, for formal Institute communication as well as for academic and other official purposes, in order to boost the efficiency with which important information is disseminated to all of the faculty, employees, and students, as well as the administrators of the Institute. This will help increase the effectiveness with which important information is communicated.

The use of email for official communications will make it easier to distribute messages and documents to different user groups and people, as well as to the university as a whole and its surrounding areas. The Institute sends out official messages to its academics, employees, and students as well as the other way around in what are known as formal Institute communications. These emails may contain administrative content such as information pertaining to human resources, policy messages, general Institute messages, formal notifications, and other similar topics.

It is imperative that the e-mail address be maintained active by utilizing it on a consistent basis if one want to receive these reminders. In order for academics, staff, and students to access this feature, they will need to log-in on a Gmail-based domain using the email id and password associated with their Institute accounts. The user is responsible for contacting the HR office or data centre and submitting an application in a required Performa format in order to get the Institute's user email id.

It's possible that users are aware that by using the email service, they are agreeing to comply by the policies listed in the following paragraphs:

- The facility should be utilized primarily for scholarly and official objectives, with personal uses being permitted only to a restricted degree.
- It is a direct violation of the policy of the Institute to use the facility for illegal or commercial reasons, and doing so may result in the facility's withdrawal from use. The illegal usage includes, but is not limited to, the unlicensed copying or distribution of software, the sending of unsolicited bulk e-mail messages, and the generating of threatening, harassing, abusive, obscene, or fraudulent communications or pictures. Moreover, the sending of unsolicited bulk e-mail messages is against the law.
- Before a user sends huge attachments to other people, the user should check that the recipient's email account has the capability to accept such large attachments and is able to handle them.
- The user should keep the mail box used space within roughly 80% of the threshold for utilizations, since a' mailbox full' or'mailbox all fullest' condition will result in the bouncing of the messages. This is especially true when the incoming mail has large attachments.
- The user should not open any attachments or emails that come from unknown or dubious sources. Before reading the message, the user should make sure they have received confirmation from the sender that it is real. This is true even if the message comes from a known source and contains an attachment that is of a questionable nature or appears to be fraudulent. Because these messages may contain viruses that have the ability to destroy the precious information that is stored on your computer, it is very important that you do this, especially from the perspective of the safety of the user's computer.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

- The user should not allow other people to use their email account, as the individual who is responsible for the account will be held personally liable for any inappropriate use of that email account.

- Users should not intercept the email accounts of other users or attempt to break into the accounts of other users since doing so violates the privacy of other users.

- When using computers that are shared by multiple users, any email account that was inadvertently left open by another user shall be promptly closed by the user who has occupied that machine for its use without peeking into the contents of the account. This rule applies even if the account was left open by accident.

According to the Institute IT security policy, assuming the identity of another individual in an email exchange will be considered a significant crime. It is ultimately the duty of each person to ensure that the email usage policy outlined by Institute is not violated through the use of their own email account.

Each user's email account has a folder labelled SPAM_MAIL that is automatically populated with any messages that are identified as spam. Users are urged to open these folders on a regular basis in order to check for any critical mail that may have been incorrectly labelled as SPAM mail and ended up in this folder. If this is the case, the user can forward that email address to so that the appropriate steps can be taken to remove it from the junk mail folder. It is strongly suggested that you clear up the contents of this folder as regularly as you can.
The policies that have been outlined above are applicable in a broad sense even to the email services that are provided by other sources such as Yahoo.com, Hotmail.com, etc., as long as they are being used from the campus network of the Institute, or by making use of the resources that the Institute has made available to the individual for official use even when they are away from the campus.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

9. Policy Regarding Website Hosting

The Official Website of the Institute

On the main website of the Engineering Institute, the Institute Intranet Channel allows departments, and associations of teachers, employees, and students to establish web pages. When it comes to website hosting, official websites are required to adhere to the Institute Website Creation Guidelines.

Affiliated Websites:
On the condition that suitable support and resources are made available, faculty members are permitted to host Web pages for professional organizations that are "affiliated" with the department. In order to host such pages, you are going to need to get prior consent from the appropriate administrative body. The individual units retain the right to terminate the service at any time, provided that they give the connected organization adequate notice in advance of their decision.

ELearning Websites (Web Pages)
The standards for web pages for eLearning that are created as a result of the teaching and learning process are the subject of this policy.
The faculty may post course materials (such as syllabi, course materials, resource materials, and so on) on the web, with links to those pages coming from the pages of the relevant departments.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

10. Use of the Institute Database Policy

This Policy applies to the databases that are managed by the Institute administration as part of the Institute's electronic government.

When it comes to delivering information that is helpful, Institute's data is a resource that is both crucial and important. Even if the data themselves are not considered confidential, the use of it still needs to be secured. Institute has its own set of policies governing the development of databases and access to information, in addition to a more general policy on how data can be accessed. These policies, when taken together, provide an overview of the Institute's methodology for the access and usage of this Institute resource.

Database Ownership: The Institute (Engineering Institute) is the data owner for all of the Institute's Institutional data that is generated within the Institute.

Data Custodians: Different sections or divisions of Institute are responsible for producing different parts of the database that Institute maintains. It is possible that they are responsible for the custodianship of certain sections of such data.

Data Administrators: The data Custodian may choose to delegate some of the data administration responsibilities described above to one or more of the faculties working in that department.

Components of the ERP System The ERP System of the Institute can, for the sake of governance, generally be broken down into seven different categories. These include:

- A management system for the information of employees
- The information and management system for students
- System for the Management of Financial Information
- An information and management system for assets
- The information and tracking system for projects
- Computerized library cataloguing and filing system
- A system for the administration of documents and the retrieval of information
- System for the Management and Information of Examinations
- Attendance management information system
- Student admission management system
- Student placement management system
- A database management system for alumni information

Guidelines and parameters for general policy use, applicable to departments and other administrative unit data users:

1. The data policies of the Institute do not permit the sharing of data that could be used to identify a person who is not affiliated with the Institute.
2. Data obtained from the Institute Database, including data acquired by specific departments or members of the faculty and staff, may only be used for reasons that are internal to the Institute.
3. The data resources required to carry out one's official responsibilities and rights are determined, in large part, by the job and function that one plays in the organization. The Institute makes information and data accessible in accordance with those obligations and rights through the data access policies it has established.
4. Data that can be used to directly identify a person as well as his or her personal information are not allowed to be transmitted in any form to individuals or organizations from the outside, including any and all government agencies as well as surveys and other requests for data. Any and all inquiries of this nature are to be transmitted to the Office of the Institute Registrar.

5. The Registrar Office of the Institute is responsible for processing information requests from any courts, attorneys, or other entities, and departments should never react to demands for information. For the purpose of providing a response, the Office of the Institute Registrar is responsible for receiving and processing all requests from law enforcement agencies.
6. Under no circumstances should any information, including that which is referred to as "Directory Information," be shared with any outside organization for the purposes of marketing, solicitation, commerce, or any other purpose. This comprises organizations and businesses that have the potential to operate as agents for the Institute or any of its divisions.
7. The Registrar of the Institute is responsible for preparing, compiling, and submitting all of the reports that are required by the UGC, MHRD, and any other government organizations.
8. Users of the database who repackage data for others in their unit are required to advise the recipients of the data about the difficulties discussed above regarding data access.
9. A violation of the IT policy has occurred when the database was tampered with by either the department or an individual user. Examples of tampering include, but are not limited to the following:
a. Making changes to or deleting the data items or software components through the use of unauthorized access methods.
b. Changing or deleting the data items or software components intentionally and dishonestly, even when done so by authorized individuals or departments.
c. causing a crash in a database, piece of hardware, or the operating system software, thereby obliterating all or part of the database on purpose for unethical reasons and carried out by any anyone.
d. Making an attempt to penetrate the database server's security.

Any member of the Institute or a member from the outside who is found to have tampered with the data in this manner shall be subject to disciplinary action taken by the Institute authorities. In the event that the situation involves the commission of illegal acts, law enforcement may become involved.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

11. Surveillance Policy for CCTV Cameras

The system includes monitors; multiplexers; digital recorders and public information signs. The cameras in the system are either fixed in position or have the ability to pan, tilt, and zoom.

It is planned to install surveillance cameras at key locations across the campus, namely at the points of entry and exit for buildings and sites. There will be no cameras that are hidden from view, and it will be impossible for any of them to focus on the frontages or rear regions of private accommodations.

Signs will be clearly posted at strategic areas and at access and departure points of the campus to warn staff, students, visitors, and members of the public that a CCTV/IP Camera system is in use. These signs will also be placed outside of the school.

Despite the fact that every possible measure has been taken to guarantee the system's highest possible level of efficiency. There is no way to provide a guarantee that the system will be able to identify each and every occurrence that takes place inside the coverage region.

The reason why the system exists

Institute installed the system with the primary goal of lowering the threat of crime in general, securing the premises of the Institute, and assisting to secure the safety of all staff members, students, and visitors while still respecting the people' right to privacy. By monitoring the system in order to fulfil these goals, we will be able to:

- Identify those who have the intent to commit a crime
- Contribute to the suppression of criminal activity and the identification of criminals
- Assist in the locating, arresting, and prosecuting of criminals in connection with maintaining public order and preventing further criminal activity
- Assist in giving evidence to management and/or to a member of staff or student against whom disciplinary or other action is being taken or is threatening to be taken, and facilitate the identification of any activities or events that would warrant disciplinary proceedings being taken against staff or students. • Facilitate the identification of any activities or events that might warrant disciplinary proceedings being taken against staff or students.
- In the case of the security staff, to supply management with information regarding employee compliance with employment contracts.

The following will not be done using the system:

- To supply photographs that have been recorded for use on the internet.
- To engage in sound recording in a manner that is not in conformity with the covert recording policy.
- For the purpose of making any decisions automatically.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

Secretly recorded material

Under the following conditions, cameras may be utilized with the prior written authorization or request of the senior officer, Registrar, and only after the Head of Security and Facilities Services as well as the Data Protection Officer have conducted an evaluation of the situation.

- That alerting the individual(s) concerned that recording was taking place would pose a significant risk to the achievement of the goal of making the recording; and
- That there is grounds to suspect that an unauthorised or unlawful conduct is taking place or is likely to take place and that this suspicion is supported by reasonable evidence.

Any such covert processing shall only be carried out for a limited and reasonable amount of time in accordance with the goals of producing the recording, and will only pertain to the precise unauthorised action that is alleged to have occurred.

The Command and Control Centre for Security

The Security Control Room will be responsible for monitoring and recording any images that are captured by the system. Throughout the course of an entire year, "The Control Room" will be staffed twenty-four hours a day. The monitors cannot be seen from anywhere other than the control room.

At no point in time will unauthorised entry into the Control Room be tolerated under any circumstances. Access will be rigorously restricted to the duty controllers, authorized members of senior management, law enforcement officers, and anybody else who is granted entrance rights by statute.

On a case-by-case basis, access to the Control Room may be allowed to staff members, students, or guests; however, this must be done only after receiving written authorization from the Registrar. In the event of an emergency and where it would be impossible to get previous authorization in a reasonable amount of time. Those who have valid reasons to enter the Control Room may be granted access to do so.

The employees will verify the identification of any visitor and ensure that the visitor has the proper authorization before allowing the visitor to enter the Control Room. Each visitor will be asked to fill out and sign the visitors' log, which will include information such as their name, the department or organization they represent, the person who authorized their visit, as well as the times at which they entered and exited the facility. A comparable log will be kept of any visitors who are permitted emergency access as well as any staff members who are on duty in the Security Control Room.

Administration and Operating Procedures of the Security Control Room

The specifics of the administrative processes that are applicable to the Control Room will be outlined in a Procedures Manual. A copy of this manual can be inspected if an appointment is made in advance and the requester provides an explanation of the motivation behind the inquiry.

Images of living people who can be identified are covered by the provisions of the Act Governing the Protection of Personally Identifiable Information. It is the responsibility of the Control Room Supervisor to ensure that the Act is followed in a day-to-day manner. This policy, as well as the processes outlined in the processes Manual, will be adhered to extremely closely when dealing with any and all recordings.

Staff

The delicate nature of working with CCTV/IP Camera images and recordings shall be stressed to every member of staff that is assigned to work in the Security Control Room. The Control Room Supervisor is responsible for ensuring that all staff members receive thorough briefings and training in regard to the tasks, both operational and administrative, that are a result of the deployment of CCTV/IP Cameras.

Recording

Digital recordings are made utilizing digital video recorders operating in time lapse mode. It is possible to record incidents as they happen in real time. Images will typically be kept for ten days from the day they were recorded, after which they will be overwritten automatically and the Log will be updated accordingly. When a hard drive has served its purpose and is no longer needed, it will be wiped clean before being discarded, and the Log will be updated to reflect this change.

Greater Noida Institute of Technology (Engg. Inst.) * Greater Noida *
Director

The hard drives and recorders will continue to be Institute's property up until the point that they are discarded or destroyed.

The ability to view images According to the instructions in the Procedures Manual, the Access Log will keep a record of every time photos are accessed. Only those members of staff who are required to have access to the photographs in order to fulfil the system's objectives will be granted access to them.

The ability of third parties to access images

Disclosure of recorded content will only be disclosed to third parties in strict line with the aims of the system, and such disclosure will be confined to the following authorities only:

- Law enforcement agencies when the recording of photographs might be useful in the course of a criminal investigation and/or in the fight against terrorism and disturbance.
- Departments of Public Prosecution
- Relevant legal representatives
- The media, in cases when the help of the general public is required in identifying either a victim of a crime or a perpetrator of a crime.
- Individuals whose photos have been captured and saved, unless disclosing such information to that person could compromise an investigation into criminal activity or legal processes.
- The involvement of emergency services in the process of conducting an accident inquiry.

Subject access to a collection of images

If a person can be identified in a digital image captured by a CCTV or IP camera, the image is considered personal data and falls under the purview of the Data Protection Act. Anyone who has reason to suspect that they have been videotaped by a CCTV or IP camera has the legal right to request a copy of the data, provided that they do not fall under one of the exceptions listed in the Act. They do not have the right to access information immediately.

In order to gain access to the data, a person whose image has been recorded and stored and who wants to do so must submit a request in writing to the Head Security Officer. Subject Access Request Forms can be obtained at the Security Office Monday through Friday between the hours of 9:00 AM and 12:35 PM and 1:00 PM and 5:00 PM, with the exception of times when Institute is officially closed.

After that, the Chief Security Officer will make arrangements for the applicant to receive a copy of the data that has been copied and supplied to them. The applicant is not allowed to ask any other member of the staff to show them the data or to get a copy of the data from any other individual. Any and all communications are required to go via the Head Security Officer of the Institute. After obtaining the necessary fee and information, a response will be sent as soon as possible and, in any case, no later than forty days after that.

The Data Protection Act provides the Head Security Officer with the authority to deny a request for a copy of the data, particularly in situations in which providing such access could compromise efforts to prevent or identify criminal activity, or to apprehend or prosecute those responsible for such activity.

Any and all inquiries of this nature will be forwarded to the Supervisor of the Security Control Room or to the Head Security Officer.

If it is considered that a data subject access request should be denied, the grounds for doing so will be thoroughly documented, and the data subject will be informed in writing, stating the reasons, as to why the request was denied.

Greater Noida Institute of Technology (Engg. Inst.)
Director
★ Greater Noida ★

Request to prevent processing

A person has the legal right to submit a request for the prevention of processing when it is likely that the processing will cause significant and unnecessary damage or distress to either that person or another person.

All requests of this nature should be directed in the first instance to the Head Security Officer or the Supervisor of the Security Control Room. That individual will review the request and submit a written response within 21 days of receiving it, in which they will detail their decision regarding the request. Both the request and the response will be saved in their respective formats.

Complaints

It is understood that people outside of Institute, as well as members of Institute, may have concerns or complaints regarding the functioning of the system. Any grievance needs to be brought to the attention of the supervisor in charge of the Security Control Room right away. If, after going through all of the procedures that were outlined, the complaint still stands, unresolved; the complaint has the option of invoking Universities Centralized Complaints Procedure by acquiring a Institute Complaints Form and a copy of the procedure and then filling both out in their entirety. Both the Security Office and the Registrar's Office have paperwork available for filing complaints that can be picked up there. These rights do not change the existing rights of members of Institute or anyone else under any relevant grievance or disciplinary procedures. Inquiries or concerns relating to the terms of the current Data Protection Act can be sent to the Head Security Officer.

Compliance monitoring:

The Security Office will serve as the point of contact for individuals who are members of Institute or members of the general public who desire to inquire about the system. The Security Office will be open from 10:20 to 1400 and from 14:30 to 1800 Monday through Friday, with the exception of the times when Institute is officially closed. Enquirers shall be given the following information in response to their requests: • A description of this statement of policy • An access request form if necessary or requested • A topic access request form if necessary or requested • A copy of the Institute central complaints processes Every documented procedure will be scrutinized on a consistent basis, and the Estates Management Committee will get updates on its status at regular intervals.

The efficiency with which the system accomplishes its goals will be monitored constantly, and the Estates Management Committee will receive updates on a regular basis.

Greater Noida Institute of Technology (Engg. Inst.)
Director
★ Greater Noida ★

12. An Overview of Data Recovery Procedures in the Event of a Catastrophe

Units are required to participate in disaster recovery planning activities in order to enable the recovery and restoration of Institute information technology systems, which are essential to the organization's operation.

Planning for disaster recovery is the ongoing process of developing, implementing, and testing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption, regardless of the source of the interruption. This is done in order to ensure that critical functions can be resumed in a timely manner in the event of an unscheduled interruption.

Participating in disaster recovery planning ensures that system dependencies have been identified and taken into account when designing the order of recovery, setting recovery time and recovery point objectives, and documenting the roles of supporting individuals. This is done so that the order of recovery can be developed.

In addition, the act of regularly backing up one's data is an essential part of any disaster recovery plan. In the event of a physical disaster, database corruption, and error propagation in robust systems, failure of hardware or software, or any other incident that may lead to the loss of data, data backup safeguards against the loss of data. The requirements for backups that are outlined in this document will make it possible for Institute business processes, teaching and learning activities, and research projects to be resumed in a fair length of time, based on the importance of the data, with a minimal quantity of data being lost.

Scope

• Information technology systems that either process or store data deemed essential to the mission are handled by the Institute. This is determined by the unit that is responsible for the system's maintenance. Desktop computers and workstations are notably excluded from this definition because they are not required to have disaster recovery plans but may require data backup.

• The activities, policies, and procedures that are involved in making preparations for the restoration or continuation of an organization's essential technological infrastructure, systems, and applications after a catastrophic event has taken place.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

The Parts Played and Duties Shouldered

• Information Assurance (IA) is responsible for the maintenance and publication of Institute's disaster recovery planning templates and procedures.

o Departments or research projects that are responsible for the maintenance of information technology systems (the owner of the system or the business) o Identify systems that are mission vital.

o Ensure that there is sufficient infrastructure resiliency, as well as data backup and restoration mechanisms, for all mission-critical data and the information technology systems that are assigned to it.

o You must first devise, put into action, document, and maintain your disaster recovery plans.

o Every two years, they must provide an update on the status of their DR planning to IA.

• The Leader of the Information Technology Unit and/or the Security Unit Liaison

o Coordinate the operations of the unit in order to successfully carry out or accomplish the obligations outlined above.

o Collaborate with the IT department of the unit to conduct a review of the unit's disaster recovery plans at least once a year, or if there are substantial changes to the system architecture or people.

· Provide the leadership of the unit with an update on the status of the DR efforts and the requirements for resources.

o Unit or Executive Leadership of the Institute (Deans, Directors, and Members of the Institute Office of Research)

We make it a point to guarantee that adequate financial, manpower, and other resources are at our disposal at all times to ensure that the development and continuous maintenance of unit DR plans goes off without a hitch.

Definitions

Critical to the Mission: The failure or interruption of mission-critical information technology systems and applications, which provide important information technology functions and access to data, will have an immediate and major negative effect on the General Network Infrastructure Operations Team (Institute) and campus units. If a system or application satisfies one or more of the characteristics listed below, it may be considered to be of mission-critical importance.

● Danger to both humans and study subjects.

• A significant influence on the research, learning and teaching, and administrative activities carried out by the Institute.

• Significant legal, regulatory or financial costs.

• A significant barrier that prevents a campus unit from performing its essential business tasks during the first 48 hours after an occurrence (48 hours Recovery Time Objective – RTO).

• Loss of access to data with established availability criteria. • Loss of particular systems or applications that may have been initially evaluated as not being mission-critical; but, they may become more mission-critical over an extended time of being unavailable.

Critical Business Functions Critical operational and/or business support functions that cannot be interrupted or unavailable for longer than a mandated or predetermined timeframe without seriously jeopardizing Institute operations. These functions are known as "critical business functions."

Recovery Time Objective (RTO) is the amount of time within which a business process needs to be restored and a stated service level attained after a disruption in order to avoid undesirable consequences associated with a break in service. This timeframe is measured in minutes.

Recovery Point Objective (RPO) is the maximum amount of time that it is acceptable for data to be lost from an information technology system or service as a result of a significant incident. In the following table, Table 1, you will find a listing of the RTO and RPO deadlines for each criticality level.

Planning for disaster recovery refers to the process, policies, and processes involved in making preparations for the restoration or continuation of an organization's essential technological infrastructure, systems, and applications in the event of a catastrophe or outage.

Business Continuity Planning: Business continuity planning, as opposed to disaster recovery planning, is the process of developing detailed plans, processes, and strategies that will enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption and fully recover as quickly as possible. This differs from disaster recovery planning, which is the process of developing disaster recovery plans. Business continuity planning is the process of developing these plans, processes, and strategies.

Standard

The following is a list of the essential components that must be included in every strategy for an information technology disaster:

Critical Systems: All departments and research programmes that are responsible for the upkeep of critical information technology systems will be required to create disaster recovery plans for those systems, put those plans into action, and put those plans through regular testing (exercises).

Example of a Plan for Recovering from a Disaster: Plans for disaster recovery must to adhere to the overall content as well as the principles.

Review and Testing of the Disaster Recovery Plan Disaster recovery plans need to be reviewed on an annual basis and revised whenever there is a significant change to the system design, the system dependencies, or the recovery personnel. It is recommended that at the very least, an annual tabletop exercise or something comparable be carried out. This exercise should replicate the unexpected and sudden loss of vital functions.

Evaluation of New Systems: New applications or systems will be examined; evaluation of a disaster recovery plan is required for systems that are deemed critical, and this plan must be recorded and tested before the system can go live.

Risk Assessment: Environments that have been deemed to be mission critical are required to have a risk assessment carried out on them at least once every four years or in accordance with the legal requirements of the system. Plans for disaster recovery need to incorporate strategies to reduce the likelihood of potentially damaging effects on systems that are essential to the operation of the organization.

Data Backup: Backups are the result of copying or archiving files with the intention of restoring them to a specific point-in-time or in the event of data loss as a consequence of computer viruses, hardware failures, file corruption, unintentional or intentional destruction, etc. Backups are the result of copying or archiving files with the intention of restoring them to a specific point-in-time. In the event that the primary copy of the data becomes corrupted or is lost in some other way, backups ensure that the integrity of the data is maintained.

Data Backup Requirements

The process of backing up and restoring data should contain a written procedure for data recovery. This procedure should also take into account any data dependencies or relationships, such as situations in which data from several systems must be in sync or share similar data elements.

In addition to the requirements for the criticality of the system, data backups must meet the following criteria: • They must be required for all systems that are mission critical as well as for every system or machine that generates, processes, maintains, or stores data that is categorized as restricted or high.

• Highly recommended for data of Moderate quality and for data that cannot be replicated in a period that is acceptable to the owner of the data.

• This feature is completely optional for any other systems or data.

System resiliency is a desired goal, but it is not a substitute for, nor does it remove the necessity to perform data backups and have a disaster recovery strategy. This does not mean that increasing system robustness is not a desirable objective.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

The following table should be used to evaluate the disaster recovery and backup needs for mission important systems regardless of data categorization. This includes systems or machines that create, process, manage, or store Restricted, High, or Moderate data. Where data can be classified into more than one of the categories stated below (or an RTO classification/criticality level), the requirements for the classification that has the most stringent data backup requirements must be met.

Data Classification Data Backup Using Encryption for Data Backups Essential Components of a Disaster Recovery Plan

Restricted Required - While at rest or travelling Depending on the Classification of the Recovery Time

High Required - While at rest or travelling Depending on the Classification of the Recovery Time

Moderate Required Recommendation Supplied Subject to the Classification of Recovery Time

Low Recommended Optional Requirements Varies Based on the Classification of Recovery Time

Infractions as well as Sanctions

When faculty members violate this policy, they run the risk of receiving appropriate sanctions or disciplinary action that is in line with the procedures that are relevant for Institute. In the event that it is suggested that competent faculty members be demoted or fired, the situation will be discussed in accordance with the procedures that are outlined in. If an individual engages in illegal behavior in connection with applicable federal and state legislation, they may be personally subject to criminal or civil prosecution as well as sanctions, in addition to the disciplinary procedures that may be taken against them.

Any department or unit that is determined to have broken this Standard may be held liable for the financial fines, legal expenses, and other remedial costs that are associated with an information security incident and other regulatory non-compliance that was caused as a result of the violation.

The responsibility for the implementation, maintenance, and interpretation of this Standard falls on the shoulders of the Implementation Information Assurance team.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

13. Power Backup policy for information technology equipment

The Institute is currently in the process of having its power back up unit (generators) rated at 380 KVA which will provide sufficient back up energy for approximately 10 hours for the full load. As soon as the generators kicked on, all of the electrical loads that were supposed to be protected were immediately switched over to the secondary power supply.

The uninterruptible power supply (UPS) is used for IT-enabled applications that are considered vital. All of the academic buildings have centralized UPS systems that are equipped with redundancy. The data centre has its own uninterruptible power supply (UPS). It is decided to construct a substation that will draw power from the national grid and scale it down to 25of 10 KVA. It is available around the clock. The continuity of the power supply will be ensured, and the generators will begin operating on their own.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

14. Cybersecurity and the Protection of Private Information

In order to prevent unauthorised access to or disclosure of the information you have provided to Institute, we shall take all precautions that are both reasonable and suitable. The Institute makes every effort to put in place safety protocols that prevent the data it collects from being lost, misused, or corrupted in any way. The Institute is responsible for the administration of a computer security policy.

The IT Manager is accountable for ensuring that all information that is stored on computer systems is protected in a manner that is compliant with the regulations of the State Agency. It is generally accepted that Institute (Engineering Institute) owns all of the information that is stored on the computers that it maintains. Only users who have been authorized by Institute are permitted to access the organization's computer systems. The individuals who are responsible for the institution's data are the ones who decide who can use administrative applications.

Authorized users of computing facilities are responsible for the following: • Keeping the security of their passwords; • ensuring that removable media containing sensitive or critical data are placed into locking storage when they are not in use or maintained in areas that are locked when they are not in use; • backing up critical data that is maintained on the hard discs of their micro computers; • ensuring that only authorized software is loaded onto any computer system.

• Ensuring that software installed on Institute computers is not copied illegally; • Documenting sensitive or critical PC applications developed for departmental use and used to perform Institute business; • Keeping the confidentiality of all records as required by applicable Institute policy, federal, state, and local law. • Protecting Institute computers from viruses by using authorized virus protection software and scanning discs.

• Any workstation (terminal, personal computer, etc.) that is left unattended for more than fifteen minutes must be safeguarded from unauthorised access by either: • Using a screen saver with password protection to restrict access, or Logging off from all computer systems. • If a screen saver with password protection is not available, the workstation must be logged off from all computer systems. When utilizing a screen saver that requires a password in order to be activated, this password should only be known by the person who is in charge of that particular workstation.

Greater Noida Institute of Technology (Engg. Inst.)
Director
* Greater Noida *

15. Policy for Evaluating and Making Changes

There is a provision in Institute that allows for the review and revision of this policy. In light of this, the members of the Institute fraternity that are listed below will serve as the committee members for the get-togethers that will take place at the beginning of each new academic year for the aforementioned reason. The members of the committee have the authority to make adjustments in response to factors such as: newly enacted or revised laws or acts of government; newly added or removed end-users; newly revised Institute rules.

- The requirement for the infrastructure of the Institute

Members of the committee will include the vice Director, chief executive officer, registrar, chief proctor, deans, manager of information technology, head of security, and five student representatives (two from the master's programme and three from the bachelor's programme).