POORNIMA

INSTITUTE OF ENGINEERING & TECHNOLOGY

IT Policy

ISI-2, RIICO INSTITUTIONALAREA, SITAPURA, JAIPUR-302022 (RAJASTHAN), INDIA

INDEX

Chapter-1

About the IT policy:

The Poornima Institute of Engineering & Technology, Jaipur recognizes the crucial role that information technology plays in the institute's missions and related administrative activities, as well as the importance of safeguarding data in all forms within an academic environment. With the increasing utilization and sharing of data in a digital format by students, faculty, and staff, both within and outside the College, a heightened effort is necessary to protect the information and the technological resources that facilitate its use.

IT Hardware Installation Policy:

Adhering to specific precautions during the installation of computers or peripherals is crucial for reducing service disruptions caused by hardware failures. By carefully following installation instructions, maintaining a clean environment, handling components with care, taking electrostatic discharge precautions, and keeping hardware up to date, the institute's network user community can ensure a reliable and uninterrupted network experience.

Primary User:

A person in whose room the computer is introduced and is basically utilized by him/her, is considered to be “primary” client. In case a computer has different clients, none of whom are considered the "essential" client, the division Head ought to make a course of action and make an individual capable for compliance.

a) File and Print Sharing Facilities:

File and print sharing capabilities on a computer network should only be installed when absolutely necessary. In the event that files are shared across the network, it is imperative to safeguard them with passwords and restrict access to read-only permissions.

b) Shifting Computer from One Location to another

The relocation of a computer system to a different location requires prior written notification to the INTERNET UNIT. This is necessary as the INTERNET UNIT keeps a record of computer identification names and their corresponding IP addresses. The computer identification names are structured in a way that includes an abbreviation of the building name and the room number. In the event that any computer system deviates from the list maintained by the INTERNET UNIT, the network connection will be disabled. The user will be notified of this through email or phone if their identity can be determined.

c) Maintenance of Computer Systems

The Computer Maintenance Cell (COMPUTER CENTER) of the institute will address any maintenance-related issues for all the computers that were centrally purchased by the college and distributed.

d) Internet Unit/Computer Center Interface

The computer fails to meet the necessary standards and is causing disruptions to the

network. The Internet Unit will promptly notify the responsible person for the system and request them to resolve the issue. This notification will be communicated via email or telephone, and a copy of it will also be sent to the Computer Center. The Internet Unit will provide the required support to ensure that the individual achieves compliance.

Software Installation and Licensing Policy

It is imperative for individual departments/projects to ensure that any computer purchases they make include licensed software, such as the operating system, antivirus software, and necessary application software. The College IT policy strictly prohibits the installation of pirated or unauthorized software on college-owned computers and computers connected to the college campus network. In the event of any unauthorized software installations, the institute will hold the department/individual personally accountable for any pirated software found on the computers within their department/individuals' rooms.

Operating System and its Updating

- It is crucial for individual users to ensure that their computer systems are regularly updated with the latest operating system (OS) service packs and patches via the Internet. This is especially vital for MS Windows based computers, including both PCs and Servers. By updating their OS, users can effectively address any bugs or vulnerabilities that have been identified by Microsoft and subsequently resolved through patches and service packs.
- As part of its policy, the institute strongly promotes the adoption of open source software like Linux and Open Office within the user community. This encourages users to utilize these software options on their systems, fostering a more open and collaborative environment.

Antivirus Software and its updating

- It is imperative for the college's computer systems to have active anti-virus software installed at all times. The primary user of a computer system bears the responsibility of ensuring compliance with this virus protection policy.
- Each individual user must ensure that their respective computer systems are equipped with up-to-date virus protection software and that it is functioning properly. It is worth noting that any antivirus software running on a computer that is not updated or renewed after its warranty period is essentially useless. If these responsibilities exceed the technical capabilities of the end user, it is their responsibility to seek assistance from a service-providing agency.

Backups of Data

It is crucial for individual users to regularly back up their important data. Data on an individual's computer can be easily destroyed by virus infections. Without adequate backups, it may become impossible to recover the lost files.

Chapter-2

Network (Intranet & Internet) Use Policy

The institute's network connectivity is governed by the institute's IT Policy when accessed via an authenticated network connection. The responsibility for maintaining and supporting the Network, excluding local applications, lies with the Communication & Information Services (INTERNET UNIT). If there are any problems with the College's network, they should be promptly reported to the INTERNET UNIT.

IP Address Allocation

The INTERNET UNIT is responsible for assigning IP addresses to any computer (PC/Server) that will be connected to the college network. The allocation of IP addresses for each building is determined, ensuring that any computer connected to the network from a specific building will only receive an IP address from the designated address pool. Additionally, each network port in the room where the computer is connected will be internally bound to that IP address, preventing unauthorized usage of the IP address from any other location.

Dial-up/Broadband Connections

The utilization of computer systems within the College's campus-wide network, regardless of whether they are owned by the college or individuals, should refrain from being employed for dial-up/broadband connections. This practice violates the college's security measures by circumventing the firewalls and other network monitoring servers. Failure to comply with this policy may lead to the withdrawal of the IP address assigned to the respective computer system.

Wireless Local Area Networks

- The entirety of this policy is applicable to the wireless local area networks of the School, department, or division. Alongside complying with this policy, it is mandatory for the school, departments, or divisions to register every wireless access point with the INTERNET UNIT, providing Point of Contact information.
- Wireless local area networks operated by departments, offices, or cells must not have unrestricted access. Network access should be limited through authentication or MAC/IP address restrictions. Encryption of passwords and data is also required.

Email Account Use Policy

To enhance the efficient dissemination of vital information to all members of the college community, including faculty, staff, students, and administrators, it is recommended that the college's email services be utilized for official college communication and academic or other authorized purposes.

Utilizing email for formal communication will streamline the delivery of messages and documents to both the campus and extended communities, as well as to specific user groups and individuals. Official college communications encompass important notices from the

college to faculty, staff, and students. These communications may consist of administrative content, such as human resources information, policy updates, general college messages, official announcements, and more.

Staff and faculty members can access the email facility using their unique User ID and password. To obtain a college email account, users can contact the INTERNET UNIT and submit an application in the prescribed Performa to receive their email account and default password.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies.

- The primary use of the facility should be for academic and official purposes, with personal use being limited.
- Engaging in illegal or commercial activities using the facility is a direct violation of the college's IT policy and may result in the withdrawal of access to the facility.
- When using shared computers, it is important to promptly close any accidentally left open email accounts without accessing their contents. This responsibility falls on the user who is currently using the computer.
- Impersonating someone else's email account will be considered a serious offense according to the college's IT security policy.
- Each individual is ultimately responsible for ensuring that their email account adheres to the college's email usage policy and remains free from any violations.

Chapter-3

Web Site Hosting Policy

Official Pages

Poornima Institute of Engineering & Technology, Jaipur allows schools, departments, and Teachers/ Employees/ Students to have their own pages on the Intranet Channel of the official Web page. However, it is important to note that these pages must adhere to the College Web Site Creation Guidelines for Web site hosting. Currently, the college's webmaster is solely responsible for maintaining the official web site of the college, which can be accessed at http://www.piet.poornima.org/.

Personal Pages:

The institute possesses a finite resource in the form of its computer and network infrastructure. It is acknowledged that every faculty member will have distinct needs for their respective pages.

Web Pages for eLearning (LMS)

The institute offers an e-learning platform for the Teaching/Learning process. The faculty members have the option to upload class materials such as syllabi, course materials, resource materials, etc. on the Web, which are then accessible through the respective department's pages.

Servers:

It is advisable to upload pages on the student information server. However, pages created for classes can also be uploaded on departmental servers or the main campus server designated for eLearning.

Maintenance:

If the pages are published on the eLearning information server, they will be subject to the default rules for personal eLearning pages. The instructor will be responsible for maintaining pages that are published on departmental servers or the main campus server designated for eLearning purposes.

Class Information:

The class-generated site's homepage will feature the class name, student's name, date, and a hyperlink to the class home page.

Policies for Maintaining Web Pages

Pages should be aligned with the mission of the College. It is mandatory for the creators of official POORNIMA and affiliated pages (excluding those generated by classes or personal pages) to inform the webmaster about their online presence by sending an announcement to the designated E-Mail Folder on the POORNIMA official website.

The announcement should include:

- The website address.
- A concise description of the content or objective of the webpages (e.g., webpages for an administrative or academic department, etc.).

College Database (of e-Governance) Use Policy

This Policy relates to the databases maintained by the college administration under the college's e-Governance. Data is a vital and important College resource for providing useful information. Its use must be protected even when the data may not be confidential.

PIET has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the college's approach to both the access and use of this college resource.

Database Ownership:

The ownership of all institutional data generated within the college lies with Poornima Institute of Engineering & Technology, Jaipur.

- **Data Ownership:** The institutional data generated within the college is under the ownership of Poornima Institute of Engineering & Technology, Jaipur. Various schools or departments within the institute may have custodianship responsibilities for specific portions of this data.
- **Delegated Responsibilities:** The data custodian may delegate certain data administration activities to officers within their respective departments. These officers act as data administrators and assist in managing the institute's database..

Chapter-4 RESPONSIBILITIES

RESPONSIBILITIES OF INTERNET UNIT

Campus Network Backbone Operations

- The administration, maintenance, and control of the campus network backbone and its active components are under the purview of INTERNET UNIT.
- INTERNET UNIT ensures that the campus network backbone operates in accordance with the service level requirements of the College Sections, departments, and divisions it serves, while adhering to operational best practices.

Physical Demarcation of Campus Buildings' Network

- Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of INTERNET UNIT.
- Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of INTERNET UNIT. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the INTERNET UNIT. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of INTERNET UNIT.
- It is not the policy of the institute to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the institute's Internet links.

Network Expansion

The INTERNET UNIT is responsible for overseeing substantial network growth as well. Annually, the INTERNET UNIT evaluates the existing networking infrastructure and evaluates whether there is a need for potential expansion. In the event that the college provides the required funding, the INTERNET UNIT will proceed with expanding the network.

Network Policy and Technology Standards Implementation

INTERNET UNIT has been granted the authority to undertake any necessary measures to ensure adherence to this policy, as well as other network-related policies aimed at safeguarding the integrity and security of the campus network backbone.

Receiving Complaints

During the process of addressing end-user computer system complaints, the COMPUTER CENTER may report any network-related issues they come across to the INTERNET UNIT. These complaints should be communicated via email or phone.

Disconnect Authorization

INTERNET UNIT is obligated to disconnect any Section, department, or division from the campus network backbone if their traffic violates the practices outlined in this policy or any other network-related policy. In situations where the regular traffic flow is significantly disrupted by a machine or network belonging to a Section, department, or division, INTERNET UNIT strives to address the issue in a way that minimizes the negative impact on other network members. If a Section, department, or division is disconnected, INTERNET UNIT establishes the requirements that must be fulfilled for reconnection to occur.

Responsibilities of College Computer Center

Maintenance of Computer Hardware & Peripherals

COMPUTER CENTER is responsible for maintenance of the college owned computer systems and peripherals that are either under warranty or annual

maintenance contract, and whose responsibility has officially been entrusted to this Cell.

Receiving Complaints

- If any of the specific computer systems are causing network issues, the INTERNET UNIT may file complaints with the COMPUTER CENTER.
- Users may report complaints to the COMPUTER CENTER if any of the computer systems or peripherals that are being maintained by them encounter any problems.
- The assigned individual at the COMPUTER CENTER handles complaints from users/INTERNET UNIT regarding these computer systems and collaborates with the service engineers of the respective computer system brands to resolve the issue within a reasonable timeframe.

Scope of Service

The COMPUTER CENTER's responsibility lies solely in resolving hardware issues, as well as any problems related to the operating system or application software that have been legally acquired by the college and installed by the company.

Installation of Un-authorized Software

The service engineers at the COMPUTER CENTER should avoid promoting the installation of unauthorized software on users' computer systems. It is crucial for them to firmly decline any requests of this nature.

Reporting IT Policy Violation Incidents

If the COMPUTER CENTER or its service technician encounters any applications that are causing disruptions to the network operations or violating the IT policies of the college, it is important to report such incidents to the INTERNET UNIT and the institute authorities.

Reporting incidents related to Network Operations

If the network port of a specific computer system is disabled due to a virus or any other activity that is impacting the network's performance, the COMPUTER CENTER will be notified by the INTERNET UNIT. Once the necessary steps have been taken to address the issue, the COMPUTER CENTER or service engineers should inform the INTERNET UNIT, allowing them to reactivate the port.

Coordination with INTERNET UNIT

In cases where uncertainty arises regarding a specific issue on a computer connected to the network, whether it is related to the network itself, the installed software, or a malfunctioning hardware, the COMPUTER CENTER/service technician can collaborate with the INTERNET UNIT staff to address the problem collectively. It is crucial to avoid leaving this task solely to the individual user.

Setting up of Wireless Local Area Networks/Broadband Connectivity

- This policy is applicable to wireless local area networks/broadband connectivity within the academic complex for schools, departments, or divisions. Along with complying with this policy, schools, departments, or divisions are required to register each wireless access point with the INTERNET UNIT, providing Point of Contact information.
- The use of broadband connections and switching between computers on the broadband and the college campus-wide network is a direct violation of the college's

IT Policy. The IT Policy strictly prohibits broadband connections within the academic complex.

- Prior to implementing wireless local area networks, schools, departments, or divisions must obtain permission from the INTERNET UNIT for the use of radio spectrum.

1. It is imperative that schools, departments, or divisions refrain from operating wireless local area networks without any limitations on access. To ensure security, network access should be restricted through authentication or MAC/IP address restrictions. Additionally, passwords and data must be encrypted for enhanced protection.
2. The establishment of inter-building wireless networks should not be initiated by the Schools/Centers without informing the INTERNET UNIT, as these networks are also subject to the regulations outlined in the College IT Policy.

A. Security

When connecting to the network backbone, departments, cells, or offices must adhere to the Network Usage Policy as outlined in the College IT Security Policy. Any network security issues will be addressed by coordinating with a designated Point of Contact (POC) within the respective department. If a POC cannot be reached, the security incident will be resolved by disconnecting the offending computer from the network until the user or POC complies with the policy.

B. Preservation of Network Equipment and Accessories

The institute owns and maintains various equipment such as routers, switches, fiber optic cabling, UTP cabling, connecting inlets to the network, racks, UPS, and their batteries. These items are installed at different locations by the institute and are under the responsibility of the INTERNET UNIT.

Responsibilities of the Administrative Units

The INTERNET UNIT requires up-to-date information from the various Administrative Units of the College in order to offer network and other IT services to new members of the college, as well as to terminate these services for those who are leaving. The information needed can be categorized into the following types:

- Details regarding Recent Appointments/Promotions.
- Notification regarding Cancellation/End of Services.
- Updates on Fresh Enrollments.
- Notice on Studentship Expiration/Removal from College Records.
- College Authorities' Measures Affecting Ineligibility for Network Access.

Chapter-5 Guidelines

Guidelines

To ensure efficient network troubleshooting and prompt service delivery, it is crucial to swiftly identify computers connected to the campus network. All computer names within the campus network must adhere to the standard conventions set by the College. Failure to comply with these naming conventions may result in the removal of non-compliant computers from the network, as determined by the INTERNET UNIT.

Video Surveillance Policy

The system

- The system is composed of: stationary cameras; cameras with pan, tilt, and zoom capabilities; monitors; multiplexers; digital recorders; and SAN/NAS storage. Additionally, public information signs are included.
- Cameras will be strategically positioned throughout the campus, primarily at the entrances and exits of sites and buildings. None of the cameras will be concealed, and they will be restricted from focusing on the front or rear areas of private accommodations.
- Prominent signs will be placed strategically at various points on the campus, as well as at the entrance and exit points, to notify staff, students, visitors, and the general public about the presence of a CCTV/IP Camera system.
- While extensive efforts have been made to ensure the system's maximum effectiveness, it cannot be guaranteed that every incident within the coverage area will be detected.