B. P. PODDAR INSTITUTE OF MANAGEMENT & TECHNOLOGY

Approved by AICTE, New Delhi & Affiliated to MAKAUT, W. B.

137, V. I. P. Road, Poddar Vihar, Kolkata-700052, West Bengal, India

IT POLICIES AND GUIDELINES

About the Institute

Established in 1999, B. P. Poddar Institute of Management & Technology (BPPIMT) stands as a tribute to Late B. P. Poddar, a visionary philanthropist, educationist, and the founding father of the B. P. Poddar Group. The Institute was founded with the mission to uphold his legacy of promoting excellence in education and social development.

Supported by the B. P. Poddar Foundation for Education, a trust devoted to enhancing the quality of technical education in India, BPPIMT is affiliated to the Maulana Abul Kalam Azad University of Technology (MAKAUT), West Bengal, and approved by the All India Council for Technical Education (AICTE).

The Institute strives to elevate society through transformative education, guided by a unique learning culture that emphasizes collaboration, communication, and innovation. Its dedicated and experienced faculty, drawn from diverse academic and professional backgrounds, nurture students to become competent professionals and responsible citizens.

Vision of the Institute

To emerge as a progressive and premier Institute for Engineering and Technology education with ethical values for creative engineering solutions commensurate with global changes.

Mission of the Institute

- Offer quality education through modern accessible, comprehensive and research oriented teaching-learning process.
- Create opportunities for students and faculty members in acquiring knowledge through research and development.
- Providing effective interface with industry by strengthening Industry-Institute interaction and developing entrepreneurial skills.
- Meet ever-changing needs for the nation through rational evolution towards sustainable and environment friendly technologies.

Table of Contents

Preamble

Undoubtedly, Intranet & Internet services have become the most important resources in educational institutions. Realizing the importance of these services, BPPIMT took the initiative way back in 2000 and established basic network infrastructure in the academic complex of the institute.

Over the past few years, the number of active users utilizing network facilities has grown significantly, along with a substantial rise in web-based applications. This development has positively influenced the institute's academic environment. In response to this progress, the institution's decision-makers have been encouraged to further enhance and expand the network infrastructure within the academic complex.

At present, the institute maintains approximately 2,500 network connections distributed across three buildings on the campus including Wi-Fi connectivity. The Computer Centre (CC) is responsible for operating and maintaining the institute's intranet and Internet services. It manages key network services, including firewall security, proxy, DHCP, DNS, email, web, and application servers, while also overseeing the overall network infrastructure of the institute.

BPPIMT is getting its Internet leased line (dedicated 1:1 ILL) from reputed service provider with sufficient bandwidth. In addition to these there are some broadband connections.

While educational institutions are providing access to the Internet to their faculty, students, staff and visitors connected to the institute, they face certain constraints:

- Limited Internet bandwidth.
- Limited infrastructure like computers, computer laboratories,
- Limited financial resources in which faculty, students and staff should **be provided** with the network facilities, and
- Limited technical manpower needed for network management.

On one hand, resources are not easily available for expansion to accommodate the continuous rise in Internet needs, on the other hand, uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes nor governance of the institute.

At the outset, we need to recognize the problems related to uncontrolled surfing by the users:

- Prolonged or intermittent surfing like social networks, chatting, etc., affecting quality of work.
- Heavy downloads like movies, songs etc. that lead to choking of available bandwidth.
- Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.

- Confidential information being made public.

With the extensive use of the Internet, network performance suffers in three ways:

- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.
- When users are given free access to the Internet like social network and chatting, non-critical downloads like movies and songs may choke the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users who are on the high-speed LANs trying to access Internet resources through a limited bandwidth definitely create stress on the Internet bandwidth available. Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Emails, unsafe downloads, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network. They can slow down or even bring the network to a halt.

Containing a virus associated with the downloaded file spreads through the network; removal of such a virus is not an easy task. Plenty of man-hours and possibly data are lost in making the network safe once more. So, preventing it at the earliest is crucial. Hence, in order to securing the network, CC has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing on the freedom of users.

As IT users are aware, all the reputed educational institutions of India have IT policies implemented in their respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily aligned with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies, formulated with due diligence are often necessary in the event of an IT audit or litigation. Policies also serve as blueprints that help the institution to implement security measures.

An effective security policy provides the essential framework for a resilient information security program. Hence, BPPIMT is also proposing to have its own IT Policy that works as guidelines for using the Institution's computing facilities, including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT) Infrastructure". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this institute. Further, this document is prepared after consulting different documents published by the academic institutes of national importance like JNU, IITs and others.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of Information Technology, Information security in general and therefore policies that govern the information security process, are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community and operating procedures.

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help the organization, departments and individuals who are part of the institute community to understand policy applies to some of the significant areas and brings conformance with stated policies. IT policies may be classified into the following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Social Media Usage Policy

Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, senior administrators, staff members and visitors)
- Network Administrators

It may be noted that the institute's IT Policy applies to technology administered by the institute centrally or by the individual departments, to information services provided by the institute's administration, or by the individual departments, or by individuals of the institute community or by authorized visitors on their own hardware connected to the institutional network. This IT policy also applies to the resources administered by the central administrative departments such as the Library, Computer Centers, Placement Cell, etc., of the institute wherever the network facility was provided by the institute. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to the campus network, are subjected to the Do's and Don'ts detailed in the institutional IT policy.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the Institute's information technology infrastructure must comply with the guidelines. Certain violations of IT policy laid down by the institution by any institutional member may even result in disciplinary action against the offender by the institutional authorities. If the matter involves illegal action, law enforcement agencies may become involved.

IT Hardware Installation Policy

Institution network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. Who is the Primary User

An individual in whose room the computer is installed and is primarily used by him/her is considered to be the “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. What are End-User Computer Systems

Apart from the client PCs used by the users, the institute will consider servers not directly administered by CC, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet, even if registered with the CC, are still considered under this policy as "end-user" computers.

C. Warranty & Maintenance

Computers purchased by the Computer Centre/Department/Project should preferably be with a 3-year on- site comprehensive warranty. After the expiry of the warranty/ the expiry of the tenure of the project, the computer/instrument will be the property of the institute and the computers / INSTRUMENTS should be under the maintenance of the computer center. Such maintenance should include OS reinstallation and checking hardware-related problems. Power Connection to Computers and Peripherals.

All the computers and peripherals should be connected to the electrical point through UPS. Power supply to the UPS should never be switched off, as a continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

D. Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

E. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when

it is absolutely required. When files are shared through network, they should be protected with password and also with read only access mode.

F. Shifting Computer from One Location to Another

Computer system may be moved from one location to another with prior written intimation to the CC and the office of the Registrar, as CC maintains a record of computer identification names, corresponding IP address and central stock.

G. Maintenance of Computer Systems Provided by the Institution

For all the computers that were purchased by the institute centrally and distributed by the office of the Registrar through Computer Centre (CC) who also attend the complaints related to any maintenance related problems.

H. Noncompliance

BPPIMT faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole institution. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

I. Maintenance of Logbooks for Instruments

A log book for usage of each computer/equipment to be maintained in each laboratory. The entry and logout from the instrument / laboratory must be recorded into the logbook by each user. A separate logbook must be maintained for each costly equipment such as GPU Servers for proper usage of high value equipment.

J. Computer Centre (CC) Interface

The individual user of a non-compliant computer affecting the network must ensure that his/her computer gets necessary compliance. The CC will provide guidance as needed for the individual to gain compliance.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, utilities, antivirus software and necessary application software) or open source software installed.

Respecting the anti-piracy laws of the country, Institute IT policy does not allow any pirated/unauthorized software installation on the institute owned computers and the computers connected to the institute campus network. In case of any such instances, institute will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers).
2. Checking for updates and updating of the OS should be performed at least once in a week or so. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users' responsibility to make sure that the updates are being done properly.
3. Institute as a policy encourages user community to go for open source software such as Linux. Open office to be used on their systems wherever possible.

B. Antivirus Software and its updating

1. Computer systems used in the institute should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly.

C. Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool

proof solution. Apart from this, users should keep their valuable data either on Pen drive or CD or other storage devices.

D. Noncompliance

Institute faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity, risk of spread of infection to others confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole Institute. Hence, it is critical to bring all computers into compliance as soon as they are recognized not to be.

E. Computer Centre Interface

CC upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the CC and Registrar's Department, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The CC will provide guidance as needed for the individual to gain compliance.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the Institute, referred to hereafter as "the Network", either through an authenticated network access connection or a Broad Band connection, is governed under the Institute IT Policy. The Computer Centre (CC) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to CC.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the institute network, should have an IP address assigned by the CC. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorizedly from any other location.

As and when a new computer is installed in any location, the concerned user can apply to avail internet for the purpose of IP address allocation and get the IP address from the CC. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports.

B. DHCP and Proxy Configuration by Individual Departments / Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the institute.

Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by CC. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running Network Services on the Servers

Individual departments/individuals connecting to the institute network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the CC in writing and after meeting the requirements of the institute IT policy for running such services. Non-compliance with this policy is a direct violation of the institute IT policy, and will result in termination of their connection to the Network.

CC takes no responsibility for the content of machines connected to the Network, regardless of those machines being Institute or personal property.

CC will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Access to remote networks using an Institute's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the institute Network connects. Institute network and computer resources are not to be used for personal commercial purposes.

Network traffic will be monitored for security and for performance reasons at CC. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

D. Broadband Connections

Except the machines connected with MHRD BSNL broad band internet connectivity, computer systems that are part of the Institute's campus -wide network, whether institute's property or personal property, should not be used for broadband connections, as it violates the institute's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies, in its entirety, to all students, faculties and staff members of the institute to use wireless local area network. In addition to the requirements of this policy, all user must register each wireless access point with CC including Point of Contact information.
2. All users must inform CC for the use of radio spectrum, prior to use of wireless local area networks.
3. Users must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions.
4. If individual department wants to have their own wireless network, prior to installation of such network, it should obtain permission from the institute authorities whose application may be routed through the Principal.

F. Browsing Restrictions

There are many reasons why it may be necessary to limit or restrict internet access in educational institutions. By regulating access to the Internet, it is possible to improve the

institute's functionality on several different levels; gaining productivity, using the internet principally for professional purposes, reducing the risk of virus attacks and faster internet connection. Sometime users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users but these regulations are to make users responsible web surfers. In view of above, institute impose bar to browse the social networking sites, audio and video downloading sites, abusive sites and other sensitive sites. Monitoring is to be enabled on all users, will be logged and maintained for certain period. Certain violations of browsing policy laid down by the institution by any institutional member may even result in disciplinary action against the offender by the institutional authorities.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties and the Institute's administrators, it is recommended to utilize the institute's e-mail services, for formal communication and for academic and other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal communications are official notices from the Institute to faculties. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on gmail.com with their User ID and password. For obtaining the institute's email account, user may contact CC for email account and default password by submitting an application.

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

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as ‘mail box full’ or ‘mailbox all most full’ situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
6. Users should configure messaging software (Outlook Express/Netscape messaging client/Gmail etc.) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the

disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

7. User should not share his/her credential of email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
8. User should refrain from intercepting or trying to break credentials of others email accounts, as it is infringing on the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.
12. Any Spam mail received by the user into INBOX should be forwarded to spam.
13. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to INBOX for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Gmail, Hotmail, Yahoo etc., as long as they are being used from the institute's campus network, or by using the resources provided by the institute to the individual for official use even from outside.

Social Media Use Policy

Cyber safety is the safe and responsible use of information from internet particularly during the use of social media. The user of social media will be solely responsible for any damage or misconduct in social media.

Circulation of strange message from your email id and social media account should not be done. Each user of computer and network devices must be careful about impersonation attack, Cyber bullying, Cyber trolls etc. No user of communication device is allowed to do such activity from the institute.

Circulation of any office related messages from the administration, HoDs or from any officials and stake holder of the institute through WhatsApp will be treated as official communication.

The institute will adhere to the IT ACT 2000, Amended IT ACT 2008, Information Technology Intermediatory Guidelines (Amended) Rules 2018, and other related GOs of Government of India. Any IT related misconduct will be governed by the law of the land based on IT ACT and IT Guideline rules.

Responsibilities of Computer Center (CC) Related to Network

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by CC.
2. CC operates the campus network backbone such that service levels are maintained as required by the departments, and sections served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of CC.
2. Physical demarcation of the "backbone" is the responsibility of CC. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the CC. 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 CC.
3. CC will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. 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.

C. Network Expansion

Major network expansion is also the responsibility of CC. Every 3 to 5 years, CC reviews the existing networking facilities and need for possible expansion. Network expansion will be carried out by CC when the institute makes the necessary funds available.

D. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations CC considers providing network connection through wireless connectivity.
2. CC is authorized to consider the applications of departments and section for the use of radio spectrum from CC prior to implementation of wireless local area networks.
3. CC is authorized to restrict network access to the departments or sections through wireless local area networks either via authentication or MAC/IP address restrictions.

E. Electronic Logs

Electronic logs that are created because of the monitoring of network traffic be retained until the administrative need for them ends, at which time they should be destroyed.

F. Global Naming & IP Addressing

CC is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. CC monitors the network to ensure that such services are used properly.

G. Providing Net Access IDs and email Accounts

CC provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the institute upon receiving the requests from the individuals in consultation with Principal.

H. Network Operation Centre

CC is responsible for the operation of a centralized Network Operation Control Centre. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilization are reported to the CC technical staff for problem resolution.

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the CC. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, CC will analyse the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

CC is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

J. Receiving Complaints

CC may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call to CC.

The designated person in CC receives complaints from the users and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

CC will be responsible only for solving the network related problems or services related to the network.

L. Disconnect Authorization

CC will be constrained to disconnect any connection in consultation with administration from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded machine or network, CC endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a department or section is disconnected, CC provides the conditions that must be met to be reconnected.

Related to Software and Hardware

A. Maintenance of Computer Hardware & Peripherals

CC is responsible for maintenance of the institute owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints

CC may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in CC receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. Scope of Service

CC will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the institute and was loaded by the company.

D. Installation of Unauthorised Software

CC or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If CC or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the institute, such incidents should be brought to the notice of the CC and institute authorities.

F. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

Further, before reformatting the hard disk, dump of only the data files should be taken by the user for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

Responsibilities of Departments or Sections

A. User Account

Any department or section or other entity can connect to the Institute network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the institute. The user account will be provided by CC.

Once a user account is allocated for accessing the institute's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the institute for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID) to prevent unauthorized use of their user account by others.

As a member of BPPIMT, when using the institute's network facilities and its user account, it becomes user's duty to respect the Institute's reputation in all his/her electronic dealings within as well as outside the Institute.

It is the duty of the user to know the IT policy of the institute and follow the guidelines to make proper use of the institute's technology and information resources.

B. Security

In connecting to the network backbone, a department or section agrees to abide by this Network Usage Policy under the institute IT Security Policy. Any network security incidents are resolved by coordination with a Head of the Department (HOD) in the originating department. If a HOD is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/HOD.

C. Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the institute are the property of the institute and are maintained by CC. Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

1. Removal of network inlet box
2. Removal of UTP cable from the room
3. Opening the rack and changing the connections of the ports either at jack panel level or switch level

4. Taking away the UPS or batteries from the room.
5. Disturbing the existing network infrastructure as a part of renovation of the location

CC will not take any responsibility of getting them rectified and such tampering may result in disconnection of the network to that segment or the individual, until the compliance is met.

D. Additions to the Existing Network

Any addition to the existing network done by department or individual user should strictly adhere to the institute network policy and with prior permission from the competent authority and information to CC. Institute Network policy requires following procedures to be followed for any network expansions:

1. All the internal network cabling should be as on date of CAT 5 UTP/ CAT 6 UTP
2. UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.
3. UTP cables should be properly terminated at both ends following the structured cabling standards.
4. If any IP address allocation is required, then the same can be obtained from CC on request.

E. Campus Network Services Use Agreement

The "Campus Network Services Use Agreement" should be read by all members of the institute who seek network access through the institute campus network backbone. All provisions of this policy are considered to be a part of the Agreement. Any Department or Section or individual who is using the campus network facility, is considered to be accepting the institute IT policy. It is user's responsibility to be aware of the Institute IT policy. Ignorance of existence of institute IT policy is not an excuse for any user's infractions.

F. Installation of Unauthorised Software

HOD should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

G. Reporting IT Policy Violation Incidents

If any HOD come across any applications that are interfering with the network operations or with the IT policies of the institute, such incidents should be brought to the notice of the CC and institute authorities.

H. Enforcement

CC periodically scans the Institute network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

Responsibilities of the Administration

CC needs latest information from the different Administrative Units of the Institute for providing network and other IT facilities to the new members of the institute and for withdrawal of these facilities from those who are leaving the institute and also for keeping the BPPIMT web site up-to-date in respect of its contents. The information that is required could be broadly of the following nature:

A. Information about New Appointments/ Promotions

B. Information about Superannuation/ Termination of Services

C. Information of New Enrolments

D. Any action by the institute authorities that makes an individual ineligible for using the institute's network facilities

E. Information on Important Events/ Developments/ Achievements

F. Information on different notice/ Rules, Procedures, Facilities

Information related items nos. A to F should reach System in-charge well in-time. Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on a floppy or CD or by email) should be sent to CC, so as to reach the above- designated persons.

Guidelines for Desktop Users

These guidelines are meant for all members of the BPPIMT Network User Community and users of the Institute network. Due to the increase in hacker activity on campus, Institute IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1. Don't use any unauthorised software in the PCs. It is absolutely against the IT Policy of the institute and may lead to punishment as per the law of the land. The user will be the sole responsible for the act.
2. All desktop computers should have the latest version of antivirus and should retain the setting that schedules regular updates of virus definitions from the central server.
3. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis.
4. All Windows desktops should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
5. The password should be difficult to break.
6. The guest account should be disabled.
7. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks) when the hard disk of the PC is formatted, the OS and all the application software should be installed from the original source of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.
8. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
9. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.
10. In addition to the above suggestions, CC recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.
11. If a machine is compromised, CC will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.
12. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, CC technical personnel can scan the servers for vulnerabilities upon request.

Concluding Note

As a concluding note, it is explicitly emphasized that though the policies focus on issues related to the technology and information usage, it may be understood that they derive broader meaning and significance from not only fundamental rights but also basic rules and responsibilities that apply to all aspects of the Institute's community. If something is not specified explicitly in the policy or guidelines as illegal or unauthorized, it may still be infraction of the institute rules, if it violates the basic rules of the institute and responsibilities of the institution community. In all such cases the decision of the institutional authority will be final. So, it is essential and important to use one's own wisdom and critical thinking in evaluating any such new situations.

-:-