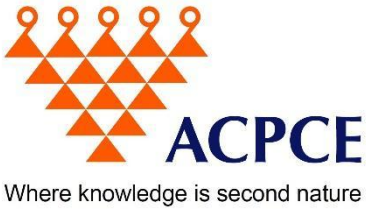

Jawahar Education Society's

A. C. Patil College of Engineering
Navi Mumbai

(Affiliated to University of Mumbai)

IT Policies & Guidelines

Table of Contents

1. Introduction IT Policy

IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, faculty, Staff and visiting Guests and Research Fellowship Members. ACPCOE has network connections to every computer system in college building. Institute network admin Team has been given the responsibility of running the institute's intranet and Internet services. Institute network admin Team looking after the Firewall security, DHCP, DNS, email, web and application servers and managing the network of the institute. ACPCOE is getting its Internet bandwidth from Vodafone Idea Limited. Total bandwidth availability from Vodafone Idea Limited source is 50 Mbps (leased line 1:1).

With the extensive use of the Internet, network performance outreach 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, non-critical downloads may clog 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 and Quality of Experience. Reducing Internet traffic is the answer.

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. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe download, 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 once it spreads through the network is not an easy job. 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, Institute network admin Team 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 the freedom of users.

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires.

Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern 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.

It may be noted that institute IT Policy applies to technology administered by the institute centrally or by the individual departments, to information services provided by the institute administration, or by the individual departments, or by individuals of the institute community, or by authorized resident or non-resident visitors on their own hardware connected to the institute network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Institute network admin Team .s, Laboratories, Offices of the institute, wherever the network facility was provided by the institute.

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 institute by any institute member may even result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

- Students: Diploma, UG, PG, Research
- Employees (Permanent/ad-hoc)
- Faculty
- Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

ACPCE maintains the Centralized IT systems and Network Resources provided to the Institute. These Centralized resources include the VPN, ERP systems, HRMS, KMS, and any other software systems, network resources etc

The enclosed policies and directives have been established in order to:

. Protect this investment

. Safeguard the information contained within these systems.

. Reduce business and legal risk.

2. Vision, mission and objectives

- IT Vision: - To provide the latest Information Technological resources for quality engineering education.
- IT Mission: - To give first priority, when it comes to IT investment & Implementations through strategic planning combined with developing a globally competitive and sustainable IT Resource Campus environment
- Policy Objectives: -
    - To provide all required IT resources as per the academic programs laid down by AICTE. Also, introduce new IT technologies which will benefit the students and research staff.
    - To effectively have an annual plan of introducing new technologies in-line with the Academia.
    - Create provision for priority up-gradation of the products
    - Create Provision for Annual Maintenance expenses to ensure maximum uptime of the products.
    - Plan and invest for redundancy at all levels.
    - To ensure that the products are updated and catered 24x7 in the campus or as per the policies lay down by the College Management.

3. IT Hardware Installation Policy

Institute 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) Primary User

An individual in whose room the computer is installed and is primarily used by him/her is considered to be “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) End User Computer Systems

Apart from the client PCs used by the users, the institute will consider servers not directly administered by Institute network admin Team ., 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 though registered with the

Institute network admin Team ., are still considered under this policy as "end- users" computers.

c) Warranty & Annual Maintenance Contract

Computers purchased by any Department/Cells should preferably be with 3 to 5-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by Institute network admin Team or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

d) Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as 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 earthling and have properly laid electrical wiring.

e) 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.

f) 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 rule.

g) Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the institute centrally and distributed by the maintenance team will attend the complaints related to any maintenance related problems.

h) Noncompliance

ACPCOE 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 affects 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.

i) Institute network admin Team Interface

Institute network admin Team finding a non-compliant computer affecting the network will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The Institute network admin Team will provide guidance as needed for the individual to gain compliance.

4. Software Installation and Licensing Policy

Any computer purchases made by the individual departments/cells should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application 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

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). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them.

b) Antivirus Software and its updating

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.

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. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from Institute network admin Team ..

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 many volumes typically C, D and so on. OS and other software should be on C drive and user's data files on the other drives (e.g. D, E). 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 foolproof solution. Apart from this, users should keep their valuable data on CD / DVD or other storage devices such as pen drives, external hard drives.

d) Noncompliance

ACPCOE 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 maintenance Center Interface

Computer maintenance Center 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/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The Institute network admin Team will provide guidance as needed for the individual to gain compliance.

5. Network (Intranet & Internet) Use Policy

Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the Institute IT Policy. The Institute network admin Team 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 Institute network admin Team monitor faculty.

a) IP Address Allocation

Any computer (PC/Server) that will be connected to the institute network should have an IP address assigned by the Institute network admin Team. Departments should follow a systematic approach, the range of IP addresses that will be allocated to each department/ session/cell.
LAN as decided. So, any computer connected to the network from that department/Session 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 unauthorized from any other location.

As and when a new computer is installed in any location, the concerned user has to take IP address allocation from Institute network admin Team .

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 /Cells/ 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 Institute network admin Team .

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 Institute network admin Team 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.

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

Institute network admin Team 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.

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 Computer server room.

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) Dial-up/Broadband Connections

Computer systems that are part of the Institute's campus-wide network, whether institute's property or personal property, should not be used for dial-up/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

This policy applies, in its entirety, department wireless local area networks. In addition to the requirements of this policy, departments must register each wireless access point with Institute network admin Team including Point of Contact information.

Departments must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

If individual department wants to have wireless network, prior to installation of such network, it should obtain permission from the institute authorities whose application may be routed through the In Charge, Institute network admin Team monitor faculty .

6. College domain Email Account Use Policy

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

Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, staff and students. 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 to https://gmail.com with their User ID (…..@acpce.ac.in) and password. For obtaining the institute's email account, user may contact Institute network admin Team for email account and default password by submitting an application in a prescribed proforma.

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

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- 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.
- 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.

- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- 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.
- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.

The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com 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.

7. Web Site Hosting Policy

a) Official Pages

Departments, Sessions, Cells, Library central facilities may have pages on ACPCOE's official Web Site. As on date, the Website maintenance team is responsible for maintaining the official web site of the institute www.acpce.org.

b) Personal Pages

It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the institute by sending a written request or mail to website maintenance team giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the institute. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the institute.

Departments, Sessions, cell, and individuals are responsible to send updated information time to time about their Web pages to Website maintenance team.

8. Institute Database Use Policy

This Policy relates to the databases maintained by the institute.

Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential.

ACPCOE 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 institute's approach to both the access and use of this institute resource.

- Database Ownership:

  ACPCOE is the data owner of the entire Institute's institutional data generated in the institute.

- Data Administrators:

  Data administration activities outlined may be delegated to some of the officers in that department.

- MIS Components:

  For the purpose of Management Information System requirements of the institute these are:

  - Employee Information Management System.
  - Students Information Management System.
  - Financial Information Management System.
  - Library Management System.
  - Document Management & Information Retrieval System.

Here are some general policy guidelines and parameters for departments, cells and administrative department data users:

1. The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.
2. Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies the institute makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.
5. Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.
6. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to :
    - Modifying/deleting the data items or software components by using illegal access methods.
    - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
    - Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
    - Trying to break security of the Database servers.

Such data tampering actions by institute member or outside members will result in disciplinary action against the offender by the institute authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

9. Wi-Fi Use Policy

- Usage of Wireless infrastructure in campus is to enhance the accessibility of internet for academic purposes and to browse exclusive online resource (licensed online journals) of the ACPCOE for student's/faculty members and staffs.

- Availability of the signal will vary from place to place. The signal strength also may vary from location to location. It is not mandatory that each and every area in each floor will have the same kind of signal strength, coverage and throughput.

- Access to Wireless internet is only an extended service and neither students nor anyone who is residing in the outside the campus can demand the service. Availability of wireless services solely depends on the discretion of the ACPCOE and it has rights to stop/interrupt the services at any given point of time, if required for any technical purpose.

- The access points provided in campus are the property of ACPCOE and any damage or loss of the equipment will be considered as a serious breach of ACPCOE's code of conduct and disciplinary action will be initiated on the student/s who are found guilty for the loss or damage of the Wireless Infrastructure or the corresponding equipment in the buildings. In the incident of any loss or damage to the wireless infrastructure, ACPCOE will assess the damage and the same will be recovered.

10. Responsibilities of Institute network admin Team

a) Campus Network Backbone Operations

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

b) Maintenance of Computer Hardware & Peripherals

Institute network admin Team is responsible for maintenance of the institute owned computer systems and peripherals that are under warranty or out of the warranty.

c) Receiving Complaints

Institute network admin Team may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them is having any problems.

The designated person in Institute network admin Team receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems (which are in warranty) to resolve the problem within a reasonable time limit. For out of warranty computer systems, problems resolved at Institute network admin Team .

Institute network admin Team may receive complaints from department/users, if any of the networks related problems are noticed by them such complaints should be made by email/phone.

Institute network admin Team 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.

The designated person in Institute network admin Team 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.

d) Scope of Service

Institute network admin Team will be responsible 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 as well as network related problems or services related to the network.

e) Installation of Un-authorized Software

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

f) Physical Demarcation of department's Network

1. Physical connectivity of department already connected to the institute network backbone is the responsibility of Institute network admin Team .
2. It essentially means exactly at which location the fiber optic based backbone terminates in the building will be decided by the Institute network admin Team. 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 Institute network admin Team .
3. Institute network admin Team 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.

g) Network Expansion

Major network expansion is also the responsibility of Institute network admin Team. Every 3 to 5 years, Institute network admin Team reviews the existing networking facilities, and need for possible expansion.

h) Wireless Local Area Networks

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

i) Electronic logs

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

j) Global Naming & IP Addressing

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

k) Providing Net Access IDs and email Accounts

Institute network admin Team 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 on prescribed proforma.

l) Disconnect Authorization

Institute network admin Team will be constrained to disconnect any Department, or cell from the institute 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 by a Department, or cell machine or network, Institute network admin Team 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 division is disconnected, Institute network admin Team provides the conditions that must be met to be reconnected.

11. Responsibilities of Department

a) User Account

Any Centre, department, or cell or other entity can connect to the Institute network using a legitimate user account (Net Access / Captive Portal ID) for the purposes of verification of affiliation with the institute. The user account will be provided by Institute network admin Team upon filling up the prescribed application form and submitting it to Institute network admin Team .

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 un-authorized use of their user account by others.

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) Supply of Information by Department, or Cell for Publishing on /updating the ACPCOE Web Site

All Departments or Cells should provide updated information concerning them periodically (at least once in a month or earlier).

Hardcopy or softcopy to be sent to the website maintenance team. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Department, or Cells.

Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the website maintenance team upon receiving the written requests. If such web pages have to be directly added into the official web site of the institute, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the In Charge, website maintenance team well in advance.

c) Security

In connecting to the network backbone, department agrees to abide by this Network Usage Policy under the Institute IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact (POC) in the originating department. If a POC 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/POC.

d) 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 Institute network admin Team and respective departments.

Tampering of these items by the department or individual user comes under violation of IT policy.

e) 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 Institute network admin Team .

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 6 UTP.
2. UTP cabling should follow structured cabling standards. No loose and dangling UTP cables are drawn to connect to the network.
3. UTP cables should be properly terminated at both ends following the structured cabling standards.
4. Only managed switches should be used. Such management module should be web enabled. Managed switches give the facility of managing them through web so that Institute network admin Team can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.
5. As managed switches require IP address allocation, the same can be obtained from Institute network admin Team on request.

f) Institute Network Services Use Agreement

The “Institute Network Services Use Agreement” should be read by all members of the institute who seek network access through the institute campus network backbone. This can be found on the institute web site. All provisions of this policy

are considered to be a part of the Agreement. Any Department or individual, who is using the Institute 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.

g) Enforcement

Institute network admin Team 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.

12. Responsibilities of the Admin Office

Institute network admin Team needs latest information from the Admin office 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 ACPCOE web site up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- Information about New Appointments.
- Information about Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Information on Important Events/ Achievements.
- Information on different Rules, Procedures, and Facilities.

13. Guidelines for Those Running Application or Information Servers

Departments may run an application or information server. They are responsible for maintaining their own servers.

1) Obtain an IP address from Institute network admin Team to be used on the server.
2) Get the hostname of the server entered in the DNS server for IP Address resolution.

3) Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.

4) Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.

5) Operating System and the other security software should be periodically updated.

14. Guidelines for Desktop Users

These guidelines are meant for all members of the ACPCOE Network User.

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) 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.

2) 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. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.

3) The password should be difficult to break.

4) The guest account should be disabled.

5) In addition to the above suggestions, Institute network admin Team 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.

15. Video Surveillance Policy

The system comprises: Fixed position cameras; Monitors; digital video recorders; Storage; Public information signs.

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

- **Purpose of the system**

  The system has been installed by institute with the primary purpose of reducing the threat of crime generally, protecting institutes premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

  - Deter those having criminal intent
  - Assist in the prevention and detection of crime
  - Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
  - Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

It is recognized that members of institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Institute network admin Team ..

CCTV footage provided by the institute (Institute network admin Team .) upon receiving the requests from the individuals on prescribed proforma.

16. Web Application Filter

Application	Management	Staff	Student	Guest
Captive portal Session	2 concurrent sessions / user			
Sites Blocked	Porn, torrents, Proxy & Hacking, Gambling, Marijuana, Criminal Activity			
YouTube	Allow	Allow	Time based	Allow
YouTube Educational	Mandatory Certificate needs to be purchased			
What's App	Allow	Allow	Time based	Allow
Facebook	Allow	Allow	Time based	Allow
Skype or Video calling	Allow	Allow	Time based	Allow
Entertainment	Allow	Time based	Time based	Allow
TV news Channel	Allow	Allow	Time based	Allow
Online Games	Deny	Deny	Deny	Deny
Windows Update	Allow	Allow	Allow	Allow

- **Default Block Category in Firewall**

  - Weapon
  - Phishing and fraud
  - Militancy and Extremist
  - Gambling
  - Pro-Suicide and self-Harm
  - Criminal Activity
  - Marijuana
  - Intellectual Piracy
  - Hunting and Fishing
  - Legal highs
  - Controlled substances
  - Anonymizers
  - Sexually Explicit
  - Nudity
  - Advertisement

Appendix I

Campus Network Services Use Agreement

Read the following important policies before applying for the user account/email account. By signing the application form for Net Access ID (user account)/email account, you agree to act in accordance with the IT policies and guidelines of ACPCOE. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of the institute. User can have a copy of the detailed document from the website & various intranet servers. A Net Access ID is the combination of a username and a password whereby you gain access to Institute computer systems, services, campus networks, and the internet.

a) Accounts and Passwords

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the Institute.

Students, staff and faculty who leave the Institute will have their Net Access ID, email id and associated files deleted.

No User will be allowed more than one Net Access ID at a time, with the exception that faculty or heads that hold more than one portfolio are entitled to have Net Access ID related to the functions of that portfolio.

b) Limitations on the use of resources

On behalf of the Institute, Institute network admin Team reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

c) Data Backup, Security, and Disclaimer

Institute network admin Team will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage

that may result from the advice or actions of Institute network admin Team staff member in the process of helping the user in resolving their network/computer related problems. Although Institute network admin Team make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, Institute network admin Team makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold Institute network admin Team , as part of ACPCOE, harmless for any such liability or expenses. ACPCOE retains the right to change and update these policies as required without notification to the User.

d) Account Termination and Appeal Process

Accounts on ACPCOE network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources.

If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may approach the In Charge, Institute network admin Team , justifying why this action is not warranted.

Appendix II

Cyber Security Guidelines

1 INTRODUCTION

Information and communication technologies (ICT) have become ubiquitous amongst government ministries and departments across the country. The increasing adoption and use of ICT has increased the attack surface and threat perception to the data of institute , due to lack of proper cyber security practices followed on the ground. In order to sensitize the employees and contractual/outsourced resources and build awareness amongst them on what to do and what not to do from a cyber security perspective, these guidelines have been compiled. By following uniform cyber security guidelines the security posture of the institute can be improved.

2 CYBER SECURITY DO'S

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Change your passwords at least once in 45 days.
3. Use multi-factor authentication, wherever available.
4. Save your data and files on the secondary drive (ex: d:\).
5. Maintain an offline backup of your critical data.
6. Keep your Operating System and BIOS firmware updated with the latest updates/patches.
7. Install enterprise antivirus client offered by the institute on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
8. Use authorized and licensed software only.
9. Ensure that proper security hardening is done on the systems. 12.When you leave your desk temporarily, always lock/log-off from your computer session.
10. When you leave office, ensure that your computer and printers are properly shutdown.
11. Keep your printer's software updated with the latest updates/patches.
12. Setup unique passcodes for shared printers.
13. Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.
14. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required. 18.Download Apps from official app stores of google (for android) and apple (for iOS).
15. Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.

16. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
17. While sending any important information or document over electronic medium, kindly encrypt the data before transmission. You can use a licensed encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password. The password for opening the protected files should be shared with the recipient through an alternative communication medium like SMS, Sandes, etc.
18. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.
19. Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
20. Report suspicious emails or any security incident to network admin team

3 CYBER SECURITY DON'TS

1. Don't use the same password in multiple services/websites/apps.
2. Don't save your passwords in the browser or in any unprotected documents.
3. Don't write down any passwords, IP addresses, network diagrams or other
    a. sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
4. Don't save your data and files on the system drive (Ex: c:\ or root).
5. Don't upload or save any internal/restricted/confidential data or files on any private cloud service.
6. Don't use obsolete or unsupported Operating Systems.
7. Don't use any 3rd party DNS Service or NTP Service.
8. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).
9. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
10. Don't install or use any pirated software (ex: cracks, keygen, etc.).
11. Don't open any links or attachments contained in the emails sent by any unknown sender.
12. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
13. Don't allow internet access to the printer.

14. Don’t allow printer to store its print history.
15. Don’t disclose any sensitive details on social media or 3rd party messaging apps.
16. Don’t plug-in any unauthorized external devices, including USB drives shared by any unknown person
17. Don’t use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin, anydesk, etc.)

Appendix III

Jawahar Education Society's

A. C. Patil College of Engineering , Navi Mumbai.

Requisition Form for College domain E-Mail Account

1. Full Name : _____

   (First Name) (Middle Name) (Last Name)

2. Designation : _____
3. Department : _____
4. Mobile No: _____
5. Existing Mail Id : _____

Date: Signature of Applicant:

……..

Approval from Principal :- Approved/Not approved

Principal

……Institute network admin Team . Use only……

The following email ID is created for Prof. /Dr. /Mr. /Ms.

_____@acpce.ac.in

Signature on Behalf of In Charge,
Institute network admin Team .

Appendix IV

Jawahar Education Society's

A. C. Patil College of Engineering , Navi Mumbai.

Application for Net Access ID Activation

1. Full Name : _____

   (First Name) (Middle Name) (Last Name)

2. Employee / Student Id (PRN) : _____

3. Department : _____

4. Mobile No: _____

5. Email Mail Id : _____

Date: Signature of Applicant:

……

Approval from Principal :- Approved/Not approved

Principal

……Institute network admin Team . Use only……

Net access ID is activated for the applicant.

Signature on Behalf of In Charge,
Institute network admin Team .

Appendix V

Jawahar Education Society's

A. C. Patil College of Engineering , Navi Mumbai.

Requisition for CCTV Footage

1. Name of Applicant : _____
2. Employee / Student Id : _____
3. Department : _____
4. Mobile No: _____
5. Email Mail Id : _____
6. Date of Footage :_____Time : From_____To_____
7. Camera Location : _____
8. Description : _____

Date: Signature of Applicant:

……

Approval from Principal :- Approved/Not approved

Principal

…….Institute network admin Team . Use only……

CCTV Footage is given to Applicant.

Signature on Behalf of In Charge,
Institute network admin Team .

Information Security Policy Document

(To Be Acknowledged by Individuals)

This form is used to acknowledge receipt of, and compliance with, the A. C. Patil College of Engineering IT Policy

Procedure

Complete the following steps:

1. Read the IT Policy and guidelines
2. Sign and Return two copies of the acknowledgement to the Institute.

Jawahar Education Society's

A. C. Patil College of Engineering , Navi Mumbai.

Acknowledgment of Information Security Policy

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Information Security Policy" and understand the same;

ii. I understand and agree that any computers, software, and storage media provided to me by ACPCE/Institute contains proprietary and confidential information about A. C. Patil College of Engineering and its customers or its vendors, and that this is remains the property of ACPCE/Institute at all times;

iii. I agree that I shall not copy, duplicate (expect for official purposes as part of my job here at A. C. Patil College of Engineering), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

iv. I agree that I will use any information downloaded from the ACPCE Server or r through the VPN , solely for the purposes of my official work and ensure that this information does not fall in the hands of a third party either during my employment at or after I leave ACPCE.

v. I agree that, if I leave A. C. Patil College of Engineering for any reason, I shall immediately return to the Institute the original and copies of any and all software, computer materials, or computer equipment that I may have received from the Institute that is either in my possession or otherwise directly or indirectly under my control.

vi. I understand the important of the ACPCE's VPN and shall ensure that I will never compromise the security of the system by either deliberately entering false information or utilizing any external floppy disks/CD/any other form of data entry; expect what has been cleared specifically by the Institute network admin Team in writing.

vii. I fully realize that if I am in default of the aforesaid conditions of the security policy I will be liable to disciplinary action of the severest form and accept the consequences as such.

Student/ Staff signature: _____

Student/Staff name : _____

PRN no./ Employee ID No:_____

Date. : _____

Department : _____