PAAVAI
ENGINEERING COLLEGE
(AUTONOMOUS)
NH-44, Paavai Nagar, Pachal, Namakkal - 637 018.
(Approved by AICTE Government of India | Affiliated to Anna University, Chennai)

PROSPER EXCEL CONQUER

IT POLICY
JUNE 2024

Institution Vision

To strive to be a globally model Institution all set for taking 'lead-role' in grooming the younger generation socially responsible and professionally competent to face the challenges ahead.

Institution Mission

- To provide goal – oriented, quality – based and value – added education through state – of – the – art technology on a par with international standards.

- To promote nation – building activities in science, technology, humanities and management through research

- To create and sustain a community of learning that sticks on to social, ethical, ecological, cultural and economic upliftment.

TABLE OF CONTENTS

ABOUT THE COLLEGE

Paavai Engineering College was established by Pavai Varam Educational Trust in the year 2001. It has been managed by the Board of Trustees with Shri.CA.N.V.Natarajan as its Chairman. The college is an autonomous institution and approved by AICTE, New Delhi and Anna University, Chennai. The college was granted Autonomous status under UGC Scheme for Autonomous Colleges with effect from the academic year 2015-2016 and accredited by NBA – AICTE. The college has been included under 2f section of UGC. At present the college offers 21 undergraduate programs leading to B.E/B.Tech., degree, seven postgraduate programs in engineering leading to M.E. degree and also MBA/MCA program and five Ph.D programmes. Institute in nearly two decades of its journey offering quality technical education to the aspirants of the rural area like Pachal (Namakkal District of TamilNadu), has crossed several mile-stones. To name a few, Accreditation by NAAC, accreditation by NBA and Conferment of autonomy.

Situated at Namakkal, nearest railway station of 7kms distance and located on NH-44 highway and is well connected by road and rail. It is spread over 15.75 acres of clean, Green and serene area.

The college provides various academic amenities so as to attain Bachelors and Masters Degree in the field of Engineering, Information Technology, Computer Applications, Management etc., and also Ph. D studies. The college not only ensures academic development of the students but also provides them with opportunities to prove themselves by means of Curricular, Co-Curricular activities and extension activities. Counselling, Career Guidance, Internship Training, Industrial Visits, Guest Lecturers, Workshops, Seminars, Conferences, Implant Training, Project Guidance, are firmly established that made PEC a "contemporary" and "Progressive" education Institution.

IT POLICY CLASSIFICATION

Need for IT Policy

- IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Directors, Dean, Principal, Students, faculty, Staff, Management and visiting Guests.

- Due to the policy initiative and academic drives, IT resource utilization in the Campus has grown by leaps and bounds during the last decade.

Now, Paavai Engineering College (PEC) has network connections to every computer system across the campus and hostel. IT Support Team is the department that has been given the responsibility of running the institute's internet services. The Team is running the Firewall security, email, web application and managing the network of the institute.

PEC is getting its Internet bandwidth from Infonet Comm Enterprises Pvt Ltd, Namakkal. Total bandwidth availability from Infonet Comm Enterprises Pvt Ltd source is 1 Gbps (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 LAN's 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. Hence, in order to securing the network, IT Support Team has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

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, Computer Centers, Laboratories, Offices of the institute, or hostels and guest houses, or residences wherever the network facility was provided by the institute.

All the faculty members, students, staff, departments, authorized visitors/visiting faculty
and others who may be granted permission to use the College information technology infrastructure,

must comply with the Guidelines. Such notification will be done via email/telephone and a copy of the notification will be sent to the IT Support.

Applicable to

- Directors, Deans & Principal
- Faculty Members
- Administrative Staff (Non-Technical / Technical)
- Lab assistants
- Guests
- Students: UG, PG, Research

Resources

A. Desktop computing facility
B. Network Devices
C. Printer and Scanner Facility
D. Internet Access
E. Power Backup Facility
F. Web Hosting
G. Email Services

A. Desktop Computing Facility

Computers purchased by any department should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers should be under maintained by internal System Maintenance Team (SMT). Such maintenance should include OS re-installation and checking virus related problems also. All computer names on the campus network must use the PEC standard conventions. Computers which are not following standard naming conventions may be removed from the network at the discretion of Network Maintenance Team (NMT). All the computers should follow the standard naming convention

B. Network Devices

LAN is used to connect computing resources, typically inside one building. The computing resources can be computers, printers, servers. Connections between the workstations are physical, with cables, and all the office resources are shared and distributed between the network workstations. The most common type of LAN is that of Ethernet. This is a family of frame-based computer networking technologies for LANs. You must first identify which services you need to

provide locally on the LAN. Computers are connected to a switch with Ethernet cables. Each device has a unique IP address.

C. Printers and Scanner Facility

Except for perhaps disk drives, the most commonly shared device on small networks is almost certainly the printer. This makes sense because almost everyone needs to print something sometime, to attach both a laser printer and an ink-jet printer to every computer. It's just so much easier to share one of each type of printer on the network so that everyone can use them.

Digitizing just your active files is great way to cut costs and be more productive. Document scanning is particularly useful to facilitate the smooth-running, among its uses are:

- Improved organization, Safeguarding documents through electronic filing.
- Translating paper files into backed up, digital formats, reducing paper storage within organizations.
- Saving time by referencing and accessing electronic files on internal systems
- Sophisticated printers with integrated scanners offer an ideal solution for quick and convenient document scanning. Depending on the manufacturer and model you choose, many printers are available with print, scan, copy and fax built in.

D. Internet Access

User Access control provides control over web applications and Internet access by creating rules based on personalized policies (appendix I). This ensures multilevel access to network resources and allows for the distribution of bandwidth among various applications and services. The Internet access control feature can also apply security settings automatically to specific users and network infrastructure facilities. Network traffic will be monitored for security and for performance reasons by **Network Maintenance Team (NMT).**

E. Power Backup Facility

A UPS, at its most basic, is a battery backup power system that supplies power long enough for equipment to properly shut down when utility power fails. It helps prevent loss of data and minimizes the stress a hard shutdown causes on your electronic equipment. The UPS is also a surge protector that protects connected devices from power problems, like surges or abnormal voltages, which can damage, reduce lifespan, or affect performance of electronic equipment and devices. All the computers and peripherals should be connected to the electrical point strictly through UPS Maintained by **Backup Power Team (BPT)**.

F. Website Hosting

A website that containing all details about the Institution, department, faculty and events. A staff want to upload a document duly submit a signed copy of proforma from Higher officials of the Institutions. Web Development Team (WDT) will manage all the content uploads, hosting and maintain data, related to website official pages. No staff/faculty or students permit to upload the data to official website personally. If anyone violate the Institutions rule policy may ready to face Institution decision.

G. Email Services

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 Institution communications are official notices from the Institution to faculty, staff and students (appendix IV). These communications may include administrative content, such as human resources information, policy messages, general messages, official announcements, etc.

IT Policy Classification

1. Computing Policy (Hardware & Software)
2. Network Policy (Internet & Sharing)
3. Backup Policy
4. Password Policy
5. Security Policy
6. Service and Troubleshoot Policy
7. Wi-Fi Policy
8. E-mail & Web Site Policy

1. COMPUTING POLICY

A.   Hardware Installation

For all the computers that were purchased by the PVET centrally and distributed by the IT Support Team, PEC the SMT will attend the complaints related to any maintenance related problems.

PEC 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.

Apart from the client PCs used by the users, the PEC will consider servers not directly administered by NMT, 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 Internet though registered with the NMT, are still considered under this policy as "end- users" computers.

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

Such computer identification names follow the convention that it comprises Department name abbreviation and Lab Name. As and when any deviation (from the list maintained by SMT) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs SMT in writing/by email, connection will be restored.

B. Software Installation

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 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. Checking for updates and updating of the OS should be performed at least once ina week or so.

As a policy encourages user community to go for open-source software such as Linux, office to be used on their systems wherever possible. Any MS Windows OS based computer that is connected to the network should access the web site for free updates. Such updating should be done at least once in a Month. Even if the systems are configured for automatic updates, it is users' responsibility to make sure that the updates a being done properly.

- Computer systems used in the PEC 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 any service-providing agency.

2. NETWORK POLICY

A. Physical Infrastructure

It essentially means exactly at which location the Cat6 & fiber optic -based backbone terminates in the buildings will be decided by the NMT. The manner in which the building is to be connected to the campus network is also the responsibility of NMT. NMT will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network.

B. Structured Networking

All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans for LAN as a part of the building layout Plan.

Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the PEC are the property of the PEC and are maintained by NMT.

Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

- Removal of network inlet box.

- Removal of UTP cable from the room.

- Opening the rack and changing the connections of the ports either at jack panel level or switch level.

- Taking away the UPS or batteries from the switch room.

- All the internal network cabling should be as on date of CAT 6 UTP.

- UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.

- 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 Managed and unmanaged switch, the network connection to that switch will be disconnected, till compliance is met by the user/department.

- As managed switches require IP address allocation, the same can be obtained from NMT on request.

C. IP Address Allocation

Any computer (PC/Server) that will be connected to the PEC network, should have an IP address assigned by the NMT. 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.

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. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

D. Internet Usage

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

- Information about New Appointments/Promotions.
- Information of New Enrolments.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy should be sent to NMT so as to reach the above designated persons.

Internet bandwidth acquired by any Section, department of the PEC under any research programme/project should ideally be pooled with the PEC's Internet bandwidth, and be treated as PEC's common resource. Under particular circumstances, which prevent any such pooling with the PEC Internet bandwidth, such network should be totally separated from the PEC's campus network.

All the computer systems using that network should have separate IP address scheme (private as well as public) and the PEC gateway should not be specified as alternative gateway.

All the computers' systems have limited internet bandwidth defends on the cadre of a person (appendix III) if the internet bandwidth has expired, then the faculty members have to write a requisition letter/ Email to the IT Support Team to access the internet facility then will be carried out and implemented by the IT Support Team to the dept concerned.

E. Sharing Usage

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.

3. BACKUP POLICY

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 Three volumes typically C, D and E. OS and other software should be on C drive and user's data files on the D drive, Software's and Backup files on the E 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 foolproof solution. Apart from this, users should keep their valuable data on Email or Personal Cloud Storage. NMT or SMT 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 adviceor actions of an SMT/NMT staff member in the process of helping the user in resolving their network/computer related problems.

Backup Schedules

The scheme for the scheduling, rotation, and retention of backups will be implemented by SMT.

- Weekly backups will be scheduled during each weekend outside of working hours (9.00am to 1700 pm).

- Monthly backups will be scheduled on the last day of each month outside of Working hours (9.00am to 1700 pm).

Backup procedures and policies are developed for two purposes, disaster recovery and file recovery. In the event of a catastrophe, due to a physical disaster, personnel error, or other misfortune, reliable backups must provide timely and accurate restoration of all functions of the organization. Individual file recovery may be required to restore programs, information or other data that has become corrupted or inadvertently removed.

- Backup procedures for all servers must be approved by IT. Procedures must include an appropriate time schedule, media description, storage, documentation, and testing process.

- Knowledge of the backup location and access to the site should be limited to a few key people within the organization, but at least two individuals should have access to the facility. In addition, the access should be documented and given to a senior administrator outside of the technology team.

- Servers located in an IT Collocation Facility may take advantage of the IT offsite server backup. This backup will meet all necessary physical security, storage, documentation, and testing criteria.

- An individual outside of the technology team will audit all backup procedures regularly to ensure that backups are taking place as outlined in the policy.

All the servers have the RAID Configuration. All the data from the Selected departments shell be taken has a backup in to external hard disk and its submitted to the management monthly once.

4. PASSWORD POLICY

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

The following recommendations include:

1. 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. Whenever possible, security policies should be set at the server level and applied to the desktopmachines.

2. The password should be difficult to break. Password, defined as:

    i. must be minimum of 6-8 characters in length
    ii. must include punctuation such as ! $ % & * , . ? + - =
    iii. must start and end with letters & must not include the characters # @ ' " `
    iv. must be new, not used before
    v. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No. etc.
    vi. passwords should be changed periodically and also when suspected that it is known to others.
    vii. Never use 'NOPASS' as your password & Do not leave password blank
    viii. Make it a point to change default passwords given by the software at the time of installation

3. The password for the user login should follow the same parameters outlined above.

4. The guest account should be disabled.

5. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

6. 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 CDs of the software. Only the data or document files should be copiedfrom 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.

7. 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.

8. In addition to the above suggestions, NMT 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.

9. If a machine is compromised, NMT 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.

10. The password for the Servers, Email and other administrative privileged users have been changed periodically (once in 60 days) for security purpose and the new password shell the submitted to the management by the IT Support Team.

5. SECURITY POLICY

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

All desktop computers should have the latest version of antivirus such as Microsoft Security Essential (PC), Microsoft defender or Kaspersky Internet Security / Small office security (Server) and should retain the setting that schedules regular updates of virus definitions from the central server.

I.   Limitations on the use of resources

On behalf of the PEC, NMT reserves the right to close the Net Access ID of any user who is deemed to be using of storage space or whose actions   otherwise limit the use of computing resources for other users.

II.   Computer Ethics and Etiquette

The User will not attempt to override or break the security of the PEC computers,networks, or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes.

This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening,harassing, abusive, obscene or fraudulent messages. User's Net Access ID gives him/her access to e-mail, and campus computing resources. The use of these resources must comply with PEC policy and applicable. Electronically available information

(1) may not violate PEC policy prohibiting sexual harassment,

(2) may not be used for commercial purposes,

(3) should not appear to represent the PEC without appropriate permission, or to representothers,

(4) may not appear to represent other organizations or companies,

(5) may not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,

(6) may not contain scripts or code that could cause a security breach or permit use of resources in opposition to PEC policy, and

III.   Data Backup, Security, and Disclaimer

NMT/SMT staff member in the process of helping the user in resolving their network/computer related problems. Although NMT/SMT 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, NMT makes no guarantee concerning the security or privacy of a User's electronic messages.

IV. Account Termination and Appeal Process

Accounts on PVET 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. When an account is terminated or disabled, NMT will make an attempt to contact the user at the phone number they have on file with NMT and notify them of the action and the reason for the action

V. 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.

VI. User Restriction

To build the firewall restriction: all the faculty members shell the given firewall restriction form, in which the need to mention their priorities, based on the requirement, internet application will be provided to the faculty members.

6. SERVICE AND TROUBLESHOOT POLICY

NMT may receive complaints from SMT, if any of the network related problems are noticed by them during the course of attending the end-user computer systems related complaints. Such complaints should be by email/phone/Person.

NMT 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 NMT. The designated person in NMT receives complaints from the users/SMT 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. NMT will be responsible only for solving the network related problems or services related to the network.

A. Maintenance of Computer Hardware & Peripherals

SMT is responsible for maintenance of the PEC owned computer systems and peripherals that are under warranty, and whose responsibility has officially been entrusted to this IT Support Team.

B. Receiving Complaints

SMT may receive complaints from NMT, if any of the particular computer systems are causing network related problems. SMT may receive complaints from the users if any of the computer systems orperipherals that are under maintenance through them are having any problems.

C. Scope of Service

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

C. Installation of Un-authorized Software

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

D. Reporting IT Policy Violation Incidents

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

E. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the SMT by NMT. After taking necessary corrective action SMT or service engineers should inform NMT about the same, so that the port can be turned on by them.

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.

G. Coordination with NMT

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning, IT Support Team / service engineer may coordinate with NMT staff to resolve the problem with joint effort. This task should not be left to the individual user.

7. WI-FI POLICY

A. Wireless Local Area Networks

    (1) This policy applies, in its entirety, to department or Hostel wireless local area networks. In addition to the requirements of this policy, departments or Hostel must register each wireless access point with NMT including Point of Contact information.

    (2) Departments or Hostel 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.

    (3) Where access through Fiber Optic/UTP cables is not feasible, in such locations NMT considers providing network connection through wirelessconnectivity.

B. DHCP and Proxy Configuration by Individual Departments /Users

Use of any computer at end user location as a DHCP to connect to more computers through an individual switch and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the PEC. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by NMT.

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.

8. E-MAIL AND WEB SITE POLICY

A. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the administrators, it is recommended to utilize the PEC e-mail services, for formal communication and for academic & 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 Institution communications are official notices from the PEC to faculty, staff and students. These

communications may include administrative content, such as human resources information, policy messages, general 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://outlook.office365.com/ with their User ID and password. For obtaining the PEC email account, user may contact WDT for email account and default password by submitting a signed application in a prescribed proforma (Appendix IV).

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.

- While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

- 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.

- 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.

- It is ultimately each individual's responsibility to keep their e-mail account free from violations of Institutions email usage policy.

- All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts.

- If Users getting more spam mails from their mail box the user account automatically blocked and they couldn't send messages to other mailers.

- Blocked account users contact WDT to unblock their ID's.

- Users forget their password means contact WDT for getting temporary password.

B. Web Site Hosting Policy

- **Official Pages**

A website that containing all details about the College, department, faculty and events. A staff want to upload a document duly submit a signed copy of proforma from Higher officials of the PEC. WDT will manage all the content uploads, hosting and maintain data, related to website official pages. No staff/faculty or students permit to upload the data to official website personally. If anyone violate the Institutions rule policy may ready to face Institution decision.

- **Web Pages for eLearning**

Web pages for eLearning authored as a result of Teaching/Learning process. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

Staff and faculty may use the email facility by logging on to http://moodle.paavai.edu.in/ with their User ID and password.

Staffs may involve into this platform and post their department syllabus, notes, materials, assignments and any kind of subject related documents.

Students reading notes, materials and may also submit their assignments through this eLearning platform by using their department link and they may also attend quiz related exams through this eLearning platform.

The following are the storage and content requirements for class-generated student Web pages:

Servers:

It is recommended that pages be placed on the Moodle server meant for eLearning purpose.

Maintenance:

- If the pages are published on the eLearning information server, they will be maintained under the default rules for personal eLearning pages

- The Moodle Coordinator will maintain pages that are published on Moodle server meant for eLearning purpose.

21

APPENDIX I

PAAVAI FIREWALL RESTRICTION & EXCEPTION DETAILS

○ Potentially Liable -   Drug Abuse, hacking, illegal, unethical, Proxy

○ Bandwidth Consuming -

     ○   Software Download   ○   Internet TV

     ○   Telephony – Mobile Calling, Skype, etc., ○   Torrent – high Bandwidth

     ○   Streaming Medias – Youtube, News channels, Online TV, etc.,

     ○   Security Risk – Phishing, Spam URLs, etc.,

○ General Interest – Personal

     ○   Trading & Brokerage

     ○   Domain Parking – Website buying & hosting

     ○   Entertainment – Audios, Videos, Film Download site, etc.,

     ○   Games

     ○   Health & wellness – Medicine, Tablets, etc.,

     ○   Instant Messages – bulk Message send, etc.,

     ○   Job Search – Naukri, Times job, Monster India, etc.,

     ○   Meaning Less Content

     ○   News & Media – Newspaper & TV Channels, etc.,

     ○   Blogs – Personal blogs, etc.,

     ○   Online Shopping – Shopping, Restaurant, Dinning, etc.,

     ○   Travels – bus, Train, Air-travels booking

     ○   Social Networks – Facebook, Twitter, etc.,

     ○   Sports – Cricket live scores, Video streaming, etc.,

     ○   Web Chat – Gmail, Yahoo mail - chatting etc.,

     ○   Web Based emails

         ○   Office 365 Mail   ○   Gmail   ○   Yahoo Mail

         ○   Rediffmail   ○   other mails.

○ General Interest - Business

     ○   Finance & Banking – Online Banking, fund transfer, etc.,

     ○   Government sites

○ VoIP   -   Skype, viber, line, whatsapp, Video Calling, etc.,

○ Remote Access – Remote system access

Signature of the staff   **HOD**   **IT Support**   **Principal**

COMPUTER MAINTENANCE DETAILS

Name of the department: Name of the Lab:

Name of the lab in charge: Name of the staff in charge:

Sl.No.	System details	Working	Not working	Remarks
1.	Server : CPU:			
2.	System Details : CPU : RAM : HDD :			
3.	Keyboard			
4.	Mouse			
5.	Monitor			
6.	Printer : Laser : DMP : INKJET :			
7.	UPS : Compact : Numeric :			
8.	Switch Rack : Model : Patch panel:			
9.	A/C :			
10.	Lights : CFL : Tube :			
11.	Chairs : S Type Chairs: Wheel Chairs : Plastic Chairs:			

Signature of the Staff   **HOD**   **IT Support**   **Principal**

INTERNET ACCESS FORM

Name of the staff:	
Department:	
Designation:	
Staff ID:	
Contact Number:	

Signature of the staff   **HOD**   **Principal**

Office Use Only: - User

Access ID   :

Data Limit   :

Valid Up to   :

Remarks   :

                                                                    IT Support

APPENDIX IV

EMAIL Creation FORM

Name of the staff:	
Department:	
Designation:	
Staff ID:	
Contact Number:	

Signature of the staff   **HOD**   **Principal**

Office Use Only: -

Email Address   : Remarks   :

                                                                    WDT

PAAVAI VISION

We Grow
Globally Reputed
Creating Value Added
Disciplined, High-Profile Professionals
And Make the Nation Great

PAAVAI CULTURE

We challenge the changes
We seek beyond the best
Work shall be taken not to be given
We produce value added professionals
We lead to Prosper, Excel and Conquer

PAAVAI MANTRA

Own Our Words and Deeds