E.G.S.PILLAY ENGINEERING COLLEGE,

(AUTONOMOUS)

NAGAPATTINAM – 611002

INSTITUTIONAL POLICY

INFORMATION TECHNOLOGY POLICY MANUAL

Guidelines by Technical Committee

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

INFORMATION TECHNOLOGY POLICY MANUAL

The Information Technology Policy Document is prepared to make all the faculty members, students and research scholars of E. G. S. Pillay Engineering College, Nagapattinam to aware of rules and regulations that govern their appropriate use of Information technology infrastructure established by the institute. The policy is effective from July, 2002. It is expected that said members strictly adhere to the rules and regulations spelled out in this document. The Management reserves the right to change/modify the policy as and when necessary and apply their discretion in specific cases.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

TABLE OF CONTENTS

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

Need for IT Policy

IT Policy is being documented for fair and transparent academic purpose for the use of various IT resources in the Campus for Students, Staff, Management and visiting Guests and Research Fellowship Members.

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, EGSPEC has network connections to every computer system covering more than 5 buildings across the campus and hostel.

EGSPEC is the department that has been given the responsibility of running the institute's intranet and Internet services.

Department of EGSPEC is running the Firewall security, DHCP, DNS, Email and application servers and managing the network of the institute.

EGSPEC is getting its Internet bandwidth from Clapsy Networks. Total bandwidth availability from the source is 310 Mbps (1:1 leased line).

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.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

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.

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, EGSPEC 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.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

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

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.

i) 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.

ii) End User Computer Systems

Apart from the client PCs used by the users, the institute will consider servers not directly administered by EGSPEC, 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 EGSPEC, are still considered under this policy as "end- users" computers.

iii) Warranty & Annual Maintenance Contract

Computers purchased by any Department/Cells should preferably be with 1-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by EGSPEC or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

iv) 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.

v) Network Cable Connection

While connecting the computer to the network, the connecting network cable should put be a way 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.

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: UG, PG, Research scholars
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

Resources

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

Policy Objectives

The objectives of the IT policy are as follows:

- 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 faculty.
- To effectively have an annual plan of introducing new technologies.
- Create provision for up-gradation.
- Create Provision for Annual Maintenance expenses
- 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.
- Leveraging information technology as a tool for the socio-economic development of Ser the Institute.

i) 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.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

ii) 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 hotel 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 us appear beyond the end user's technical skills, the end-user is responsible for seeking Assistance from EGSPEC.

iii) 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. 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.

iv) Non compliance

EGSPEC staff and students not complying with this computer security policy buy leave themselves and others at risk of virus infections. It could result in damaged or lost files in operable computer resulting in loss of productivity.
Risk of spread of infection to others confidential data being revealed to un authorized persons.

An individual's non-compliant computer can have significant, adverse effects on other individual groups, departments, or even whole institute. Hence it is critical to bring

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

v) 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.

vi) Maintenance of Computer Systems provided by the Institute

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

vii) Non compliance

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

viii) EGSPEC Interface

EGSPEC upon 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 wills follow-up the notification to be certain that his/her computer gains necessary compliance. The EGSPEC will provide guidance as needed for the individual to gain compliance.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

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.

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.

i) 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 to the knowledge of the EGSPEC 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.

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

EGSPEC 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 EGSPEC.

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.

ii) Wireless Local Area Networks

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

Departments or hostels 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 inter-building wireless network, prior to installation of such network, it should obtain permission from the institute authorities whose application may be routed through the Incharge, EGSPEC all computers into compliance as soon as they are recognized not to be.

iii) EGSPEC Interface

EGSPEC upon finding a non-compliant computer will notify the individual responsible bob for the system and ask that it be brought into compliance. Such notification will be done via email, phone. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The EGSPEC will provide guidance as needed for the individual to gain compliance.

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 EGSPEC 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 EGSPEC.

i) IP Address Allocation

Any computer (PC/Server) that will be connected to the institute network should have an IP address assigned by the Computer Center. Departments should follow

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

a systematic approach, the range of IP addresses that will be allocated to each building.

As and when a new computer is installed in any location, the concerned user has to take IP address allocation from Computer Center / respective department.

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.

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 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 domain mail paid with extensions EGSPEC.ac.in with their User ID and password. For obtaining the institute's email account, user may contact EGSPEC for email account and default password by submitting an application in a prescribed Performa.

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

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

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.

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.

EGSPEC 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.

Dr. S. RAMABALAN, M.E., Ph.D.
PRINCIPAL
E.G.S. Pillay Engineering College.
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

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

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.

Hostels Wi-Fi Use Policy

- Usage of Wireless infrastructure in hostels is to enhance the accessibility of internet for academic purposes and to browse exclusive online resource (licensed online journals) of the EGSPEC 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 of every block 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 hostels can demand the service. Availability of wireless services solely depends on the discretion of the EGSPEC 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 hostels are the property of EGSPEC and any damage or loss of the equipment will be considered as a serious breach of EGSPEC'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 de Infrastructure or the corresponding equipment in the hostels buildings. In the incident of any loss or damage to the wireless infrastructure, EGSPEC will assess the damage and the same will be recovered from all the students who are residing in that floor/building/hostel.

i) Electronic logs

Cathode 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.

ii) Global Naming & IP Addressing

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

iii) Providing Net Access IDs and email Accounts

SAT provides Net Access IDs and email accounts to the individual users to enable food in them to use the campus-wide network and email facilities provided by the institute upon receiving the requests from the individuals on prescribed home Performa.

iv) Disconnect Authorization

SAT will be constrained to disconnect any Department, or cell, hostel from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy.

In the event of a situation where the normal flow of traffic is severely degraded by a Department, or cell, hostel machine or network, SAT 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, SAT provide the conditions that must be met to be reconnected.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu

Responsibilities of SAT

i) Campus Network Backbone Operations

1. The campus network back bone and its active components are Administrator, maintained and controlled by SAT.

2. SAT operates the campus network backbone such that service levels are maintained as required by the Institute Departments, and hostels served by the campus network backbone within the constraints of operational best practices.

ii) Maintenance of Computer Hardware & Peripherals

SAT is responsible for maintenance of the institute owned computer systems and peripherals that are under warranty or out of the warranty.

iii) Receiving Complaints

SAT 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 SAT 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 SAT.

SAT 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.

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

The designated person in SAT 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.

iv) Scope of Service

SAT 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.

All requests from law enforcement agencies are to be forwarded to the Office for response.

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.

Responsibilities of Department

i) 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 SAT, upon filling up the prescribed application form and submitting it to SAT.

ii) Installation of Unauthorized Software

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

iii) Physical Demarcation of Campus Building's Network

1. Physical connectivity of campus buildings already connected to the Campus network backbone is the responsibility of SAT.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of SAT. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the SAT. 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 SAT.
3. SAT 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.

iv) Network Expansion

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

Responsibilities of the Administrative Department

SAT needs latest information from the different Administrative Department 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 EGSPEC web site up-to-date in respect of its contents.

Guidelines for Those Running Application or Information Servers

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

- Obtain an IP address from SAT to be used on the server.
- 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 wide to server.
- Make sure that the server is protected adequately against virus and intrusions by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.
- Operating System and the other security software should be periodically updated.

Guidelines for Desktop Users

These guidelines are meant for all members of the EGSPEC Network User.
Due to the increase in hacker activity on campus, Institute EGSPEC 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.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.

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, SAT 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.

CCTV Surveillance Policy

The system comprises fixed position cameras, Monitors, Network video recorders, Storage, Public information signs. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of SAT 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 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 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 SAT. CCTV footage provided by the institute (SAT) upon receiving the requests from the individuals on prescribed Performa.

Security Mechanism Policy

1. Web policy to use un wanted restricted sites cannot be used for following Criminal Activities, Criminal Activity, Extreme, Intellectual Piracy, Intolerance & Hate, Phishing & Fraud, Plagiarism, Spyware & Malware, Culture and Entertainment, Hobbies, Hunting & Fishing, Live audio, Live video, Online Chat, Peer-to-peer & torrents, Photo Galleries, Radio & Audio Hosting, Society & Culture, Video hosting, Drugs and Controlled Substances, Alcohol & Tobacco, Controlled substances, Marijuana, Extreme or Violent Web Content, Criminal Activity, Extreme, Pro-Suicide & Self-Harm.
2. Most of the operating systems will have a firewall that will effectively take care of undesired and malignant content from the internet.
3. Prevents Unauthorized Remote Access and unethical hackers are there, who are making constant efforts to acquire access to vulnerable systems.
4. The ignorant user is never aware of who can access his system. A strong firewall prevents any sort of possibility of a prospective unethical hacker getting remote access into a system. A strong firewall is necessary to protect your data, your transactions and data.
5. The following policy used in our firewall, Application filter and web policy.
6. Application policy used to unwanted software and malware not allowed in our security mechanism and also unwanted software are not allowed to download for ex, all the mobile applications.

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 EGSPEC. 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.

Dr. S. RAMABALAN, M.E., Ph.D.,
PRINCIPAL
E.G.S. Pillay Engineering College,
Thethi, Nagore - 611 002.
Nagapattinam (Dt) Tamil Nadu.