G. PULLAIAH COLLEGE OF ENGINEERING AND TECHNOLOGY:: KURNOOL
(Autonomous)

KURNOOL

4.3.1 - IT policy covering wi-fi, cyber security, etc., and allocated budget for updating its IT facilities

KURNOOL

IT POLICY

1. Overview

IT policy exists to maintain, secure, and ensure legal and appropriate use of information technology infrastructure established by the institute on the campus.

This policy establishes institute-wide strategies and responsibilities for protecting the **Co**nfidentiality, **I**ntegrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the institute.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, GPCET took initiative way back in 2000 and established strong network infrastructure.

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

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

1. Prolonged or intermittent surfing, affecting quality of work.
2. Heavy downloads that lead to choking of available bandwidth.
3. Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.
4. Confidential information being made public.

Further, all the staff and students, authorized visitors / visiting faculty and otherswho 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 member may even resultin disciplinary action against the offenders. If the matter involves illegal action, law enforcement agencies may become involved.

IT policies may be classified into following groups:

1. IT Hardware Installation Policy
2. Software Installation and Licensing Policy
3. Network (Intranet & Internet) Use Policy
4. E-mail Account Use Policy
5. Web Site Hosting Policy
6. Institute Database Use Policy

Resources:

1. Network Devices wired / wireless
2. Internet Access
3. Official Websites, web applications
4. Official Email services
5. Data Storage

6. Mobile/ Desktop / server computing facility
7. Documentation facility (Printers/Scanners)
8. Multimedia Contents
9. Cloud Services

2. IT Hardware Installation Policy

Staff 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 or hardware failures.

Who is Primary User?
An individual, whose computer is installed in their room/cabin is primarily used by them, is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the head of the department should make an arrangement and assign a person responsible for compliance.

Warranty & Annual Maintenance Contract
Computers purchased by any Section / Department / Project should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

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

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.

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.

Shifting Computer from One Location to another
Computer system may be moved from one location to another with prior written intimation to the ITIMS Officer, as ITIMS Centre maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention which comprises building name abbreviation and room no. As and when any deviation (from the list maintained by ITIMS Centre) 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 ITIMS Centre in writing / by email, connection will be restored.

Maintenance of Computer Systems provided by the Institute
For all the computers that were purchased by the institute centrally and distributed by the ITIMSOfficer will attend the complaints related to any maintenance related problems.

3. Software Installation and Licensing Policy

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

Respecting the anti-piracy laws of the country, GPCET IT policy does not allow any pirated / unauthorized software installation on the institute owned computers and the computers connected to

the 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 / individual's cabins.

Operating System and its Updating

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

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 any service-providing agency.

Backups of Data

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

Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data either on external hard disks or other storage devices such as pen drives.

GPCET 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 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.

4. Internet Access Request and Approval Policy

Internet connectivity presents with new risks that must be addressed to safeguard the facilities, vital information assets. Access to the internet will be provided to staff and students (further referred as users) to support academic activities and only on and as needed. Access to the internet by users that is inconsistent with academic needs results in the misuse of resources.

Internet access will be provided to users for their academic needs only and they restricted to access the contents under the academic category only.

As part of the internet access request process, the staff and students are required to read the internet usage and security policy. The user must sign the declaration in the application that they understand and agrees to comply with the policies. Users not complying with these policies could be subject todisciplinary action.

Approval and Access

1. Staff and students get allocated GPCET User Accounts upon employment or enrolment.
2. Students activate their accounts as part of the enrolment process.

All staff and student accounts are administered by IT Infrastructure Management Services (ITIMS) division for day to day management of GPCET user accounts. Staff and students who have IPADS / Laptops / IP managed device are able to apply for IP address / desktop admin rights to their machine by submitting **Application for IP Address Allocation** to ITIMS.

Removal of Access

Internet access will be discontinued upon completion of study of student, resignation of staff, completion of contract, or any disciplinary action arising from violation of this policy. The privileges granted to uses and continue sly monitored and may be revoked at any time if it is no longer needed by the user.

Usage Policy

Internet users of institute shall comply with applicable National / State / Cyber laws, rules and policies of institute. Examples of rules and policies include, the laws of privacy, copy right, trade mark,obscenity and pornography. The IT act 2000 which prohibit hacking, cracking, spoofing and similar activities.

1. According to the GPCET policy, the tethering / hotspotting of internet connection is liable fordeactivating the connection.
2. Users will be required to obtain necessary authorization before using institute connectivity.
3. Users will also be responsible for any activity originating from their account
4. Accounts and passwords should not be used by any other persons under any circumstances other those to whom they have been assigned by ITIMS Officer.
5. In case of unauthorized use of account is detected or suspected, the account owner should change the password and report the incident to ITIMS Officer.
6. Uses shall not use institute network and connectivity to get unauthorised access to remote computers which may damage the operations of GPCET Network.

Security and Privacy

1. Uses should engaging safe computing practices by establishing appropriate access restrictions for their account and computing devices, guarding their password and changing them regularly.
2. Users should note that their uses of institute connectivity are not completely private. As part the security measures, all the activities are logged and monitored at ITIMS computing center.
3. The institute, in its discretion may disclose the results of any such general or individual monitoring including the contents and records of communication to the appropriate authorities or law enforcement agencies and may use those results for disciplinary procedures.

Prohibited Downloads

The following downloads are specifically not allowed on computers unless approved in writing by ITIMS Officer:

1. Any peer to peer file sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications – called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer.
2. Any third party personal antivirus or firewall: Since adequate security has already been provided

for on all machines via pre-defined firewall rules, third party firewalls may interfere with these rules thus endangering the network.

3. Any Proxy servers, private fire wall, tunnelling software, connectivity sharing software
4. Hacking tools of any sort: The use of any such tools on college network is strictly prohibited.
5. Games & Movie trailers or previews.
6. Any other copyrighted content / materials / software which are not appropriate to the user.

5. WiFi Policy

1. Institute WiFi is available in the whole campus.
2. The access to institute Wifi is restricted to the registered device only. Usage of institute Wifi in an unregistered device by spoofing / tethering will be treated as violation of this policy.
3. Even if the access ID is different, the registered Wifi user is the sole responsible person for all the communications originated from the registered device.

6. Network (Intranet & Internet) Use Policy

Network connectivity provided through the institute, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the GPCET IT Policy. The Communication & Information Services (ITIMS Centre) 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 ITIMS Officer.

IP Address Allocation

Any computer (PC/Server/laptop) that will be connected to the institute network, should have an IP address assigned by the ITIMS Centre. 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 unauthorisedly from any other location.

As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the ITIMS Centre.

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 thesame 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.

DHCP and Proxy Configuration by Individual Departments / Sections / 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 ITIMS Centre.

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.

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 ITIMS Centre 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.

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

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

Network traffic will be monitored for security and for performance reasons at ITIMS Centre. 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.

7. Email Account Use Policy

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

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal institute communications are official notices from the institute to 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 http://employeeID.GPCET.ac. in with their user ID and password. For obtaining the institute's email account, user may contact ITIMS Officer 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:

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

personally held accountable, in case of any misuse of that email account.

8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.

8. Web Site Hosting Policy

Official Pages of departments and sections may have pages on GPCET's official Web page. The Official Web pages must confirm to the instate Web Site Creation Guidelines for Web site hosting.

As on date, the institute's webmaster is responsible for maintaining the official web site of the institute viz., **http://www.GPCET.ac.in** only.

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 to ITIMS Officer 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 ofpersonal 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, 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.

Affiliated Pages:
Faculty may host Web pages for "affiliated" professional organizations on institute / department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

Web Pages for eLearning
Faculty can host web pages for eLearning authored as a result of Teaching / Learning process. Faculty may have course content delivery materials (syllabi, OBE course description, lecture notes, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

Because majority of student pages will be published on the institute's Learning Management Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official GPCET or other Web sites.

9. Institute Database (eGovernance) Use Policy

This Policy relates to the databases maintained by the institute administration under the institute's eGovernance. Data is a vital and important resource for providing useful information. Its use must be protected even when the data may not be confidential. GPCET has its own policies regarding the creation of database and access to information and a more generic policy on data access.

1. **Database Ownership:** GPCET is the data owner of all the institutional data generated in the institute.

2. **Custodians of Data:** Individual sections or departments generate portions of data that constitute institute's database. They may have custodianship responsibilities for portions of that data.
3. **Data Administrators:** Data administration activities outlined may be delegated to some of the faculty in that department by the data Custodian.
4. **MIS Components:** The various components for the purpose of eGovernance and management information system requirements are:

    - Manpower Information Management System (MIMS)
    - Campus Management System (SAMVIDHA)
    - Students Information Management System (SIMS)
    - Financial Information Management System (FIMS)
    - Physical Resources Information Management System (PRIMS)
    - Project Information Monitoring System (PIMS)
    - Document Management And Information Retrieval System (DMIRS)
    - Examinations Management System (EMS)
    - Library Information Management System (LIMS)
    - Learning Management System (AKANKSHA)
    - Online Testing Platform (eExam Desk)
    - BuildIT Coding Platform (BITCP)

Here are some general policy guidelines and parameters for departments and administrative unit 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 staff and students, 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 Principal.
5. Requests for information from any courts, attorneys, etc. are handled by the office of the Principal and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the Principal for response.
6. At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes.
7. All reports for AICTE, JNTUH, UGC, MHRD and other government agencies will be prepared / compiled and submitted by the Principal, Controller of Examinations and Finance officer of the institute.
8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.
9. 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.

10. Video Surveillance Policy

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 / IP 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:

1. Prevent those having criminal intent.
2. Assist in the prevention and detection of crime.
3. Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
4. Facilitate the identification of any activities / event which might warrant disciplinary procedures 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.

Covert cameras may be used under the following circumstances on the written authorization or request of the Principal:

1. That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording.
2. That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

The Security Control Room

Images captured by the system will be monitored and recorded in the security control room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

No unauthorized access to the control room will be permitted at any time. Access will be strictly limited to the authorized members of senior management, police officers and any other person with statutory powers of entry.

Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Principal. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with alegitimate reason to enter the Control Room.

Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the center. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV / IP Camera images and recordings. The Control Room supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV / IP Camera.

Recording
Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time. Images will normally be retained for15 days from the date of recording, and then automatically over written and the log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the log will be updated accordingly. All hard drives and recorders shall remain the property of institute until disposal and destruction.

Access to images
All access to images will be recorded in the access log register and will be restricted to those staff need to have access in accordance with the purposes of the system.

Access to images by third parties
Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

1. Law enforcement agencies where images recorded would assist in a criminal enquiry and / or the prevention of terrorism and disorder.
2. Prosecution agencies.
3. Relevant legal representatives.
4. The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime.
5. People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
6. Emergency services in connection with the investigation of an accident.

Access to images by a subject
CCTV / IP Camera digital images, if they show a recognizable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV / IP Camera is entitled to ask for a copy of the data, subject to exemptions contained inthe Act. They do not have the right of instant access.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the IT Infrastructure Maintenance Services (ITIMS) Officer.

The ITIMS Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the ITIMS Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

The Data Protection Act gives the ITIMS Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

Request to prevent processing
An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

All such requests should be addressed in the first instance to the Security Control Room supervisor or the ITIMS Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

11. Responsibilities of the Administrative Units

ITIMS Officer needs latest information from the different administrative units of the institute for providing network and other IT facilities to the new members of the institute and for withdrawal of these facilities from those who are leaving the institute, and also for keeping the GPCET web site up-to- date in respect of its contents.

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

1. Information about new appointments / promotions.
2. Information about super annuations / termination of services.
3. Information of new enrolments.
4. Information on expiry of studentship / removal of names from the rolls.
5. Any action by the institute authorities that makes an individual ineligible for using the
6. institute's network facilities.
7. Information on important events / developments / achievements.
8. Information on different rules, procedures and facilities.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on mobile storage devices or mobiles or PDA or by email) should be sent to ITIMS Officer.

12. Responsibilities of ITIMS Office

Maintenance of Computer Hardware & Peripherals
ITIMS Centre is responsible for maintenance of the institute owned computer systems and peripherals that are either under warranty or annual maintenance contract.

Receiving Complaints
ITIMS Centre may receive complaints from ITIMS Officer, if any of the particular computer systems are causing network related problems. Centre may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems. The designated person in centre receives complaints from the users / ITIMS officer of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

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

Installation of Un-authorised Software
ITIMS Centre 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.

Reporting IT Policy Violation Incidents
If ITIMS Centre or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the institute, such incidents should be brought to the noticeof the ITIMS Officer and Principal.

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 ITIMS Officer by ITIMS Centre. After taking necessary corrective action ITIMS Centre or service engineers should inform ITIMS Officer about the same, so that the port can be turned on by them.

Rebuilding the Computer System
When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was

having earlier. Further, after installing the OS all the patches / latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

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

13. Enforcement

1. Users found violating this policy may be denied to access to the institute network for a minimum period of six months and may be subject to other penalties and disciplinary action.
2. The Institute network admin may suspend, block or restrict the access to an account, when it reasonably appears necessary to do so in order to protect the security, integrity or functionality of the network
3. Suspected violations of applicable laws may be referred to appropriate law enforcement agencies.
4. Alleged violations will be handled through institute disciplinary procedures applicable to the user.

14. Disclaimer

1. GPCET reserves the right, without notice, to limit or restrict individual's use and to inspect, copy, remove or otherwise alter any data, file or system which may undermine the authorized use of any computing facility or which is used in violation of institute rules and policies.
2. GPCET also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.
3. GPCET disclaims any responsibility for loss of data or inference with files resulting from its effort to maintain security and privacy.
4. GPCET reserves the right to amend these policies at any time without prior notice and to take necessary action to comply with applicable laws.