IT POLICY GCEK

GOVERNMENT COLLEGE OF ENGINEERING, KARAD
(An Autonomous Institute of Government of Maharashtra)

Dist. Satara, Maharashtra, India, PIN: 415124
Tel.: 91- 02164- 272414,
Web: http://www.gcekarad.ac.in

INDEX

Government College Engineering Karad IT Policy

2021 Ver. 1.0

1. Need for IT Policy

The IT highway is the new paradigm and the internet is the medium which has become the most important aspect of our Teaching learning process, with the current IT scenario it is imperative that the institution has a strong IT policy. Effective policies are often necessary in the event of an IT audit or litigation.

Policies also serve as blueprints that help the institution implement security measures and implement them hence, Government College of Engineering Karad hereafter referred as GCEK proposes to have its own IT Policy that works as guidelines for using the institute's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this institute. Furthermore the policy details are put forth here with.

GCEK has about 2000 network connections covering total campus of 43 arc across the campus with all PG, girls and boys hostels are connected and expected to reach 4000 connections very soon.

Data center is administrator for internet and network connectivity it also responsible Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the GCEK.

GCEK has Internet bandwidth from BSNL. Total bandwidth availability from BSNL source from 1 Gbps (leased line). GCEK has also got 100 Mbps connectivity under NKN Network of MHRD (NME-ICT).

- The need of IT policy is to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by GCEK on the campus.
- This policy establishes Campus-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the GCEK.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

1.1. IT policies may be classified into following groups:

1.1.1. IT Hardware Installation Policy
1.1.2. Software Installation and Licensing Policy
1.1.3. Network (Intranet & Internet) Use Policy
1.1.4. E-mail Account Use Policy
1.1.5. Web Site Hosting Policy
1.1.6. Institute Database Use Policy Further, the policies will be applicable at two levels:
1.1.7. End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
1.1.8. Network Administrators

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 recognized Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the institute.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the institute IT policy.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the institute 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.

1.2. Applies to

Stake holders on campus or off campus

1.2.1. Students: UG, PG, Research
1.2.2. Employees (Permanent/ Temporary/ Contractual)
1.2.3. Faculty
1.2.4. Administrative Staff (Non-Technical / Technical)
1.2.5. Higher Authorities and Officers
1.2.6. Guests

1.3. Resources

1.3.1. Network Devices wired/ wireless
1.3.2. Internet Access
1.3.3. Official Websites, web applications
1.3.4. Official Email services
1.3.5. Data Storage
1.3.6. Mobile/ Desktop / server computing facility
1.3.7. Documentation facility (Printers/Scanners)
1.3.8. Multimedia Contents

2. IT Hardware Installation Policy

GCEK 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.

2.1. Who is 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.

2.2. What are End User Computer Systems?

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

2.3. 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.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. Shifting Computer from One Location to another.

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

2.8. Maintenance of Computer Systems provided by the Institute.

For all the computers that were purchased by the institute centrally and distributed by the Store, institute Computer Maintenance Cell (COMPUTER CENTER) will attend the complaints related to any maintenance related problems.

2.9. Noncompliance

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

computers into compliance as soon as they are recognized not to be.

2.10. Data center & Computer center Interface

Data center & Computer center 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/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The Data center & Computer center will provide guidance as needed for the individual to gain compliance.

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, 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.

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

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.

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.

3.2. 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.

3.3. 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 Floppy, or CD or other storage devices such as pen drives.

3.4. Noncompliance

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

3.5. Data center & Computer center Interface

Data center & Computer center upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The Data center & Computer center will provide guidance as needed for the individual to gain compliance.

4. Network (Intranet & Internet) Use Policy

Network connectivity provided through the GCEK, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection is governed under the Institute IT Policy. The Communication & Information Services (Data center & Computer center) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the institute network should be reported to Data center & Computer center.

4.1. IP Address Allocation

Any computer (PC/Server) that will be connected to the GCEK network should have an IP address assigned by the Data center. 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 unauthorized 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 Data center.

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.

4.2. DHCP and VLan 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 Data center. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration. On-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.

4.3. 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 Data center 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.

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

Data center will be constrained to disconnect client machines where potentially damaging software is found to exist.

A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Access to remote networks using an Institute 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 Data center. 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.

4.4. Wireless Local Area Networks

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

4.4.2. Departments or divisions must inform Data center for the use of radio spectrum, prior to implementation of wireless local area networks.

4.4.3. Departments or divisions 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.

4.4.4. 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 Co-coordinator, Data center.

4.5. Internet Bandwidth obtained by Other Departments

4.5.1. Internet bandwidth acquired by any Section, department of the institute under any research program/project should ideally be pooled with the institute's Internet bandwidth, and be treated as institute's common resource.

4.5.2. Under particular circumstances, which prevent any such pooling with the institute Internet bandwidth, such network should be totally separated from the institute's campus network. All the computer systems using that network should have separate

4.5.3. IP address scheme (private as well as public) and the institute gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the institute IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to DATA CENTER.

4.5.4. Non-compliance to this policy will be direct violation of the institute's IT security policy.

5. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, 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.

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 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. For obtaining the institute's email account, user may contact DATA CENTER 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:

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

5.2. 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.

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

5.4. 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.

5.5. 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.

5.6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

5.7. 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.

Any such activity will be punished under the IT Cyber Act.

5.8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

5.9. 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.

5.10. Impersonating email account of others will be taken as a serious offence under the institute IT security policy.

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

5.12. Any Spam mail received by the user into INBOX should be forwarded to spam@gcekarad.ac.in

5.13. If any difficulty found in accessing mail or any change required should be address to netadmin@gcekarad.ac.in

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

6. Web Site Hosting Policy

All Document circular, notices, Call Quotation to be hosted on website of GCEK requires all the permission through proper channel. The form of hosting document on website is given in appendices 3.

No pages or data will be shared on website without appendices 3 document. If any shares data without appendices 3 document disciplinary action will be taken by concerned authority.

6.1. Official Pages

The Departments and Associations of Teachers/Employees/Students may have pages on GCEK on the official Web page.

Official Web pages must conform to the Institute 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.gcekarad.ac.in only.

6.2. Personal Pages:

The institute computer and network infrastructure is a limited resource owned by the institute. 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 DATA CENTER giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the institute. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

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

6.3. Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on 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.

6.4. Web Pages for eLearning

Though the institute does not have this facility as on this date, this Policy relates to future requirements for 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.

Because majority of student pages will be published on the Institute's 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 GCEK or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

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

6.4.1. Servers:

It is recommended that pages be placed on the student information server, but pages developed for classes also may be placed on departmental servers or the main campus server meant for eLearning purpose.

6.4.2. Maintenance:

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

The instructor will maintain pages that are published on departmental servers or the main campus server meant for eLearning purpose.

6.4.3. Content Disclaimer:

The home page of every class-generated site will include the GCEK Content

Disclaimer (for pages published on the eLearning information server, the content disclaimer should be generated automatically):

6.4.4. Class Information:

The home page of every class-generated site will contain the name of the class, the student's name, the date, and a link to the class home page.

6.4.5. Pages Generated by Class Groups:

Pages produced by class groups, if placed on the eLearning information server, will be placed on the server under the name of the designated group leader.

6.4.6. Official Pages:

If Web pages developed for eLearning become the part of the "official" GCEK page, they must be removed from the eLearning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

6.5. Student Web Pages

Though the institute does not have this facility as on this date, this policy relates to future requirements for personal student Web pages. Policies for student pages authored as a result of academic assignments are in II above. It is recognized that each individual student will have individual requirements for his/her pages. As the institute's computer and network infrastructure is a limited resource owned by the institute, only web pages of students related to their assignments will be accepted on the Students web pages. The contents of personal pages hosted by the students even on outside web site must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws.

The following are the storage and content requirements for personal student Web pages:

6.5.1. Servers:

Pages will be placed on the student information server.

6.5.2. Maintenance:

Pages published on the student information server will be maintained under the default rules for personal student pages.

6.5.3. Content Disclaimer:

Every personal page will include the GCEK Content Disclaimer (the content disclaimer will be generated automatically):

6.5.4. Responsibilities for Those Maintaining Web Pages

Sections, departments, units, and individuals are responsible for maintaining their own Web pages.

GCEK Web pages (including personal pages) must adhere to the GCEK Web Page Standards and Design Guidelines and should be approved GCEK Webpages Advisory Committee.

6.5.5. Policies for Maintaining Web Pages

Pages must relate to the Institute's mission.

Authors of official GCEK and affiliated pages (not class-generated or personal) are required to

announce their Web presence by sending an announcement to webmaster@gcekarad.ac.in. Mails sent to this address will be placed in a GCEK Public E-Mail Folder in the GCEK official web site. T. announcement should include:

1. The URL.
2. A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the GCEK Home Page and, if applicable, contain additional links to the sponsoring organization or department.

7. Institute Database Use Policy

This Policy relates to the databases maintained by the Institute administration under the Institute's e-Governance.

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.

GCEK 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.

7.1. Database Ownership: GCEK Institute is the data owner of the entire Institute's institutional data generated in the Institute.

7.2. 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.

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

7.4. Here are some general policy guidelines and parameters for departments and administrative unit data users:

7.4.1. The Institute's data policies do not allow the distribution of data that is identifiable to a person outside the Institute.

7.4.2. Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal Institute purposes only.

7.4.3. 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.

7.4.4. 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 of the Institute Registrar.

7.4.5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the Institute 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 Institute Registrar for response.

7.4.6. At no time May information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes.

This includes organizations and companies which may be acting as agents for the

Institute or its departments.

7.4.7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar, Dean Academics, Controller of Examinations and Finance officer of the Institute.

7.4.8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

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

7.4.9.1. Modifying/deleting the data items or software components by using illegal access methods.

7.4.9.2. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.

7.4.9.3. Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

7.4.9.4. 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.

8. RESPONSIBILITIES OF DATA CENTER

8.1. Campus Network Backbone Operations

The campus network backbone and its active components are administered, maintained and controlled by DATA CENTER.

DATA CENTER operates the campus network backbone such that service levels are maintained as required by the Institute Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

8.2. Physical Demarcation of Campus Buildings' Network

Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of DATA CENTER.

Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of DATA CENTER. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the DATA CENTER. 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 DATA CENTER.

DATA CENTER will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.

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.

8.3. Network Expansion

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

8.4. Wireless Local Area Networks

Where access through Fiber Optic/UTP cables is not feasible, in such locations DATA CENTER considers providing network connection through wireless connectivity.

DATA CENTER is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from DATA CENTER prior to implementation of wireless local area networks.

DATA CENTER is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

8.5. 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.

8.6. Global Naming & IP Addressing

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

8.7. Providing Net Access IDs and email Accounts

DATA CENTER provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the Institute upon receiving the requests from the individuals on prescribed Appendices 1 and 2.

8.8. Network Operation Centre

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

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

8.9. Network Policy and Technology Standards Implementation

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

8.10. Receiving Complaints

DATA CENTER may receive complaints from all departments Heads, 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.

DATA CENTER 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 be generally through phone call to DATA CENTER.

The designated person in DATA CENTER 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.

8.11. Scope of Service

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

8.12. Disconnect Authorization

DATA CENTER will be constrained to disconnect any Section, department, or division 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 Section, department, or division machine or network, DATA CENTER endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, DATA CENTER provides the conditions that must be met to be reconnected.

9. Responsibilities of Institute Computer Center

9.1.Maintenance of Computer Hardware & Peripherals

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

9.2.Receiving Complaints

COMPUTER CENTER may receive complaints through Head of Department, if any of the particular computer systems are causing network related problems.

COMPUTER CENTER 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 COMPUTER CENTER receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

9.3.Scope of Service

COMPUTER CENTER 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.

9.4.Installation of Un-authorised Software

COMPUTER CENTER 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.

9.5.Reporting IT Policy Violation Incidents

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

9.6.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 COMPUTER CENTER by DATA CENTER. After taking necessary corrective action COMPUTER CENTER or service engineers should inform DATA CENTER about the same, so that the port can be turned on by them.

9.7.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.

9.8.Coordination with DATA CENTER

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,

COMPUTER CENTER/service engineer may coordinate with DATA CENTER staff to resolve the problem with joint effort. This task should not be left to the individual user.

10.Responsibilities of Department

10.1. User Account

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

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

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

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

10.2. Logical Demarcation of Department

In some cases, department might have created an internal network with in their premises.

In such cases, the department assumes responsibility for the network service that is provided on all such internal networks on the department side of the network backbone. The department or division is also responsible for operating the networks on their side of the network backbone In a manner that does not negatively impact other network segments that are connected to the network backbone.

Each Section, department should identify at least one person as a Point of Contact and communicate it to DATA CENTER and COMPUTER CENTER so that DATA CENTER or COMPUTER CENTER can communicate with them directly in case of any network/system related problem at its end.

10.3. Supply of Information by Department, for Publishing on/ updating the GCEK Web Site

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

Hardcopy of such information duly signed by the competent authority at Department, level**,** along with a softcopy to be sent to the webmaster operating from DATA CENTER. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Department.

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

10.4. Setting up of Wireless Local Area Networks/Broadband Connectivity

This policy applies, in its entirety, to school, department, or division wireless local area networks/broadband connectivity within the academic complex. In addition to the requirements of this policy, Departments must register each wireless access point with DATA CENTER including Point of Contact information.

Obtaining Broadband connections and using the computers alternatively on the broadband and the Institute campus-wide network is direct violation of the Institute's IT Policy, as Institute. IT Policy does not allow broadband connections within the academic complex.

Departments must secure permission for the use of radio spectrum from DATA CENTER prior to implementation of wireless local area networks.

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

As inter-building wireless networks are also governed by the Institute IT Policy, setting up of such wireless .networks should not be undertaken by the Schools/Centers without prior information to DATA CENTER.

10.5. Security

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

10.6. Preservation of Network Equipment and Accessories

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

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

10.6.1.1. Removal of network inlet box.

10.6.1.2. Removal of UTP cable from the room.

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

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

10.6.1.5. Disturbing the existing network infrastructure as a part of renovation of the location DATA CENTER will not take any responsibility of getting them rectified and such tampering may result in disconnection of the network to that segment or the individual, until the compliance is met.

10.7. Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the Institute network policy and with prior permission from the competent authority and information to DATA CENTER.

Institute Network policy requires following procedures to be followed for any network expansions:

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

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

10.7.3. UTP cables should be properly terminated at both ends following the structured cabling standards.

10.7.4. Only managed switches should be used. Such management module should be web enabled. Using unmanaged switches is prohibited under Institute's IT policy. Managed switches give the facility of managing them through web so that DATA CENTER can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual

member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

10.7.5. As managed switches require IP address allocation, the same can be obtained from DATA CENTER on request.

10.8. Structured Cabling as a part of New Buildings

All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan. Engineering Branch may make provisions in their designs for at least one network point in each room. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

10.9. Campus Network Services Use Agreement

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

10.10. Enforcement

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

11.Responsibilities of the Administrative Units

DATA CENTER 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 GCEK web site up-to-date in respect of its contents.
The information that is required could be broadly of the following nature:

11.1. Information about New Appointments/Promotions.

11.2. Information about Super annulations / Termination of Services.

11.3. Information of New Enrolments.

11.4. Information on Expiry of Studentship/Removal of Names from the Rolls.

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

11.6. Information on Important Events/Developments/Achievements.

11.7. Information on different Rules, Procedures, and Facilities Information related items nos. A through E should reach Director (DATA CENTER) and Information related items nos. F and G should reach webmaster well in-time.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on mobile storage devices or mobiles or PDA or by email) should be sent to DATA CENTER so as to reach the above designated persons.

12. Guidelines on Computer Naming Conventions

In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network. All computer names on the campus network must use the Institute standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of DATA CENTER.

All the computers should follow the standard naming convention.

13. Guidelines for running Application or Information Servers

13.1. Running Application or Information Servers

13.1.1. Departments may run an application or information server.

13.1.2. Individual faculty, staff or students on the GCEK campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the GCEK network.

13.2. Responsibilities for Those Running Application or Information Servers

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

13.2.1. Application or information server content and services must follow content guidelines as described in GCEK Guidelines for Web Presence.

13.2.2. Obtain an IP address from DATA CENTER to be used on the server

13.2.3. Get the hostname of the server entered in the DNS server for IP Address resolution. Institute IT Policy's naming convention should be followed while giving the host names.

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

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

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

13.2.7. Sections/Departments may run an application or information server provided they do the following:

13.2.8. Provide their own computer, software and support staff

13.2.9. Provide prior information in writing to DATA CENTER on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization web server, contact the DATA CENTER.

14. Guidelines for hosting Web pages on the Internet/Intranet.

14.1. Mandatory:

14.1.1. Provide the full Internet e-mail address of the Web page maintainer.

14.1.2. Provide a link to the GCEK home page from the parent (department of origin) home page.

14.1.3. Provide a link to the parent home page ("Return to department's home page") on all supporting local pages.

14.1.4. Maintain up to date pages. Proofread pages and test links before putting them on the Web, and regularly test and update links.

14.1.5. Know the function of HTML tags and use them appropriately.

14.1.6. Make provision for providing information without images as printer-friendly versions of the important web pages.

14.2. Recommended:

14.2.1. Provide information on timeliness (for example: August 2005; updated Weekly; updated monthly, etc.).

14.2.2. Provide a section indicating "What's New."

14.2.3. Provide a caution statement if link will lead to large pages or images.

14.2.4. Indicate restricted access where appropriate.

14.2.5. Avoid browser-specific terminology.

14.2.6. Provide link text that is clear without the link saying '**click here'** Whenever hyperlinks are used.

14.2.7. Maintain visual consistency across related pages.

14.2.8. Provide a copyright statement (if and when appropriate).

14.2.9. Keep home pages short and simple.

14.2.10. Avoid using large graphics or too many graphics on a single page.

14.2.11. Provide navigational aids useful to your users (Link to Home, Table of Contents, Next Page, etc.).

14.2.12. Maintain links to mentioned pages.

14.2.13. Make your Web pages easy to maintain for yourself and anyone who Might maintain them in the future.

14.2.14. Avoid active links to pages that are in development. Place test or draft Pages in your "test," "temp," or "old" subdirectory. Remember that nothing Is private on the Internet: unlinked pages in your directory may be visible.

14.2.15. Check your finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended that you check your page with a Web validation service.

14.2.16. Think of your users--test with primary user groups (which will be mix of users linking through our high-speed network, and users linking via much slower modems).

14.2.17. Conform to accepted, standard HTML codes.

15. Guidelines for Desktop Users

These guidelines are meant for all members of the GCEK Network User Community and users of the Institute network.

Due to the increase in hacker activity on campus, Institute IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

15.1. All desktop computers should have the latest version of antivirus such as Symantec Anti-Virus (PC) or Quick Heal and should retain the setting that schedules regular updates of virus definitions from the central server.

15.2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.

15.3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.

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

15.4.1. must be minimum of 6-8 characters in length

15.4.2. Must include punctuation such as ! $ % & * , . ? + - =

15.4.3. must start and end with letters

15.4.4. must not include the characters # @ ' " `

15.4.5. must be new, not used before

15.4.6. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No. etc.

15.4.7. Passwords should be changed periodically and also when suspected that it is known to others.

15.4.8. Never use 'NOPASS' as your password

15.4.9. Do not leave password blank and

15.4.10. Make it a point to change default passwords given by the software at the time of installation

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

15.6. The guest account should be disabled.

15.7. 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.

15.8. 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 copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

15.9. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

15.10. 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.

15.11. In addition to the above suggestions, DATA CENTER recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise.

Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused

by the loss of a machine.

15.12. If a machine is compromised, DATA CENTER 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.

15.13. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, DATA CENTER technical personnel can scan the servers for vulnerabilities upon request.

16. Video Surveillance Policy

16.1. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.

16.2. 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.

16.3. 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.

16.4. 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.

16.5. Purpose of the system

16.6. The system has been installed by Institute with the primary purpose of reducing the threat of crime generally, protecting universities 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:

16.7. Deter those having criminal intent

16.8. Assist in the prevention and detection of crime

16.9. Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order

16.10. Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

16.11. In the case of security staff to provide management information relating to employee compliance with contracts of employment

16.11.1. The system will not be used:

16.11.2. To provide recorded images for the world-wide-web.

16.11.3. To record sound other than in accordance with the policy on covert

recording.

16.11.4. For any automated decision taking.

16.11.5. Covert recording.

16.12. Covert cameras may be used under the following circumstances on the written authorization or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

16.12.1. That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and

16.12.2. That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

16.12.3. 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.

16.12.4. 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

16.12.5. 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.

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

16.12.7. 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 Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

16.12.8. 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.

16.12.9. Security Control Room Administration and Procedures

16.12.10. Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

16.12.11. Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

16.12.13. Staff :-

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.

16.13. Recording

16.14. Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

16.15. Images will normally be retained for fifteen 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.

16.16. All hard drives and recorders shall remain the property of Institute until disposal and destruction.

16.17. Access to images

16.18. All access to images will be recorded in the Access Log as specified in the Procedures Manual

16.19. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

16.20. Access to images by third parties

16.21. 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:

16.21.1. Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
16.21.2. Prosecution agencies
16.21.3. Relevant legal representatives
16.21.4. 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
16.21.5. People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
16.21.6. Emergency services in connection with the investigation of an accident.
16.21.7. Access to images by a subject

16.22. 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
C.C.T.V. /IP Camera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

16.22.1. A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except Second and fourth Saturday), except when Institute is officially closed or from the Data Protection Officer, the Records Office during the same hours.

16.22.2. The Data Protection 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 Institute Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

16.22.3. The Data Protection Act gives the Data Protection 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.

16.22.4. All such requests will be referred to the Security Control room Supervisor or by the Data Protection Officer.

16.22.5. 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.

16.22.6. Request to prevent processing

16.22.7. 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.

16.22.8. All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection 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.

16.22.9. Complaints

16.22.10. 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 Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by

16.22.11. Obtaining and completing an Institute Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer; these rights do not alter the existing rights of members of Institute or others under any relevant grievance or disciplinary procedures.

16.22.12. Compliance monitoring

16.22.13. The contact point for members of Institute or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except second and fourth Saturday) except when Institute is officially closed.

16.22.14. Upon request enquirers will be provided with:

16.22.14.1. A summary of this statement of policy

16.22.14.2. An access request form if required or requested

16.22.14.3. A subject access request form if required or requested A copy of the Institute central complaints procedures

16.22.15. All documented procedures will be kept under review and a report

periodically made to the Estates Management Committee.

16.22.16. The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.

17. Campus Network Services Use Agreement

Read the following important policies before applying for the user account/email account. By signing the application form for IP address allocation/Net Access ID (user account)/email account, you agree to act in accordance with the IT policies and guidelines of GCEK Institute. 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 Intranet. 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.

17.1. Accounts and Passwords

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

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

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

17.2. Limitations on the use of resources

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

17.3. Computer Ethics and Etiquette

The User will not attempt to override or break the security of the Institute 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. Even sending unsolicited bulk e-mail messages comes under IT Policy violation.

In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

User's Net Access ID gives him/her access to e-mail, and campus computing resources. The use of these resources must comply with Institute policy and applicable. Electronically available information

17.3.1. may not contain copyrighted material or software unless the permission of the copyright owner has been obtained,

17.3.2. may not violate Institute policy prohibiting sexual harassment,

17.3.3. may not be used for commercial purposes,

17.3.4. should not appear to represent the Institute without appropriate permission, or to represent others,
17.3.5. may not appear to represent other organizations or companies,
17.3.6. may not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,
17.3.7. may not contain scripts or code that could cause a security breach or permit use of resources in opposition to Institute policy, and
17.3.8. WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show date of last revision and an address (e-mail or postal) for correspondence. DATA CENTER equipment does not support use of scripting in individual pages.

17.4. Data Backup, Security, and Disclaimer

DATA CENTER or COMPUTER CENTER will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an

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

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

17.5. Account Termination and Appeal Process

Accounts on GCEK 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, DATA CENTER will make an attempt to contact the user (at the phone number they have on file with DATA CENTER) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the DATA CENTER of the same But, if the termination of account is on the grounds of willful breach of IT policies of the Institute by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Director DATA CENTER, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Appeals Board duly constituted by the Institute for this purpose to review the evidence and hear reasons why an appeal should be considered. If the Appeals Board recommends revival of the account, it will be enabled. However, the Data Center of the Appeals Board is final and should not be contested.

Users may note that the Institute's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate Institute authorities.

All the above rules and regulation adhere to the government of india and government of maharastra IT policy and IT act. The policies will remain in tuned as per change as per the made by government from time to time.

https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf

https://www.meity.gov.in/content/view-it-act-2000

Appendix

Phone. No. (02164) 272414, 8275706613
Web : http://gcekarad.ac.in
Email: principal@gcekarad.ac.in,
principal.gcoekarad@dtemaharashtra.gov.in

Govt. of Maharashtra

GOVT. COLLEGE OF ENGINEERING, KARAD
(An Autonomous Institute of Govt. of Maharashtra)
Vidyanagar, Karad -415124 Dist.- Satara

Staff Internet Registration Form

Name of Staff:	**Please Paste your recent passport size photo here**
Name of Parent's/Guardian's :	
Address :	
Designation :	
Department :	
Username :	
Email ID :	
Mobile Number	

Declaration

I the undersigned; hereby declare that above information provided by me is true to best of my knowledge and belief. The user ID and password issued to me will be kept confidential. I am aware of cyber law and I will abide it. I will be solely responsible for my internet account and its usage. I will not be involved in viewing unsolicited websites and unethical internet usage and if found, my internet account will be suspended and I will be responsible for strict disciplinary action taken by institute / authority.

Date	**Signature of the Staff**
Verified the information and found Correct Department Internet Staff I/C	**Signature of Head of the Department**

For Office use only

User Id:	**Password:**	**Date:**

Authorized Signature

Government College of Engineering, Karad
Campus Wide Network and Central Computing Facility
Undertaking with respect to GCE Karad IT Usage Policy

All Users of IT infrastructure (Computers and the Network) at GCE Karad.

This policy outlines the responsible use of the Information Technology Infrastructure at GCE, Karad.

All users of GCE, Karad will be subject to the following Acceptable Use Policy

1. I shall be responsible for all use of this network. In case I own a computer and decide to connect it to GCE, Karad network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of "my computer".) In case I do not own a computer but am provided some IT resources by GCE, Karad, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored / archived emails, on Computer Centre or Department machines).

2. I will be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipment's, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

3. I understand that the IT infrastructure at GCE, Karad is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

4. I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use GCE, Karad IT resources to threaten, intimidate, or harass others.

5. I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

6. I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the GCE, Karad administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize GCE, Karad administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of GCE, Karad network.

7. I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, and other similar programs.

8. I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material). In particular, I have noted the following:
Electronic resources such as e-journals, e-books, databases, etc. made available by the Central Library, GCE, Karad are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited.
Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that
Systematic downloading will result in the publisher blocking the entire community of users at GCE, Karad from accessing

9. I understand that I will not take any steps that endanger the security of the GCE, Karad network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the GCE, Karad campus. In critical situations, GCE, Karad authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising

10. I understand that any use of IT infrastructure at GCE, Karad that constitutes a violation of GCE, Karad Regulations could result in administrative or disciplinary procedures.

I have read all IT Policy and abide the IT policy of Govt. College of Engineering, Karad.

Signature of Staff

Phone. No. (02164) 272414, 8275706613
Web : http://gcekarad.ac.in
Email: principal@gcekarad.ac.in,
principal.gcoekarad@dtemaharashtra.gov.in

Govt. of Maharashtra

GOVT. COLLEGE OF ENGINEERING, KARAD
(An Autonomous Institute of Govt. of Maharashtra)
Vidyanagar, Karad -415124 Dist.- Satara

Student Internet Registration Form

Name of Student:	**Please Paste your recent passport size photo here**
Name of Parent's/Guardian's :	
Address :	
Roll No :	
Department :	
Username :	
Email ID :	
Mobile Number	

Declaration

I the undersigned; hereby declare that above information provided by me is true to best of my knowledge and belief. The user ID and password issued to me will be kept confidential. I am aware of cyber law and I will abide it. I will be solely responsible for my internet account and its usage. I will not be involved in viewing unsolicited websites and unethical internet usage and if found, my internet account will be suspended and I will be responsible for strict disciplinary action taken by institute / authority.

Date	**Signature of the Student**
Verified the information and found Correct Department Internet Staff I/C	**Signature of Head of the Department**

For Office use only

User Id:	**Password:**	**Date:**

Authorized Signature

Government College of Engineering, Karad
Campus Wide Network and Central Computing Facility
Undertaking with respect to GCE Karad IT Usage Policy

All Users of IT infrastructure (Computers and the Network) at GCE Karad.

This policy outlines the responsible use of the Information Technology Infrastructure at GCE, Karad.

All users of GCE, Karad will be subject to the following Acceptable Use Policy

1. I shall be responsible for all use of this network. In case I own a computer and decide to connect it to GCE, Karad network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of "my computer".) In case I do not own a computer but am provided some IT resources by GCE, Karad, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored / archived emails, on Computer Centre or Department machines).

2. I will be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipment's, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

3. I understand that the IT infrastructure at GCE, Karad is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

4. I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use GCE, Karad IT resources to threaten, intimidate, or harass others.

5. I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

6. I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the GCE, Karad administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize GCE, Karad administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of GCE, Karad network.

7. I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, Trojans, and other similar programs.

8. I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material). In particular, I have noted the following:
Electronic resources such as e-journals, e-books, databases, etc. made available by the Central Library, GCE Karad are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited.
Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that
Systematic downloading will result in the publisher blocking the entire community of users at GCE, Karad from accessing

9. I understand that I will not take any steps that endanger the security of the GCE, Karad network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the GCE, Karad campus. In critical situations, GCE, Karad authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising

10. I understand that any use of IT infrastructure at GCE, Karad that constitutes a violation of GCE, Karad Regulations could result in administrative or disciplinary procedures.

I have read all IT Policy and abide the IT policy of Govt. College of Engineering, Karad.

Signature of Student

Phone. No. (02164) 272414, 8275706613
Web : http://gcekarad.ac.in
Email: principal@gcekarad.ac.in,
principal.gcoekarad@dtemaharashtra.gov.in

Govt. of Maharashtra

GOVT. COLLEGE OF ENGINEERING, KARAD
(An Autonomous Institute of Govt. of Maharashtra)
Vidyanagar, Karad -415124 Dist.- Satara

Form for uploading data on Institute Website

To, Date:

The DC In charge
GCE Karad

Subject: Uploading of contents on our college website.

Kindly arrange to upload the data as mentioned below on our college web site.

1. File name -
2. Data related to -
3. Uploading Date -
4. Date to remove from Web
5. Location on Website (optional) -
6. Hardcopy signed by HoD enclosed (Mandatory)
7. Soft copy of above data is
   a. Sent to email website@gcekarad.ac.in (Yes/No)

Faculty/Staff Head of Department Principal

Note: Please submit this form to DC In charge, GCE Karad at leastone week before the date of uploading

For DC Use only:

Data uploaded on: Data uploaded by: Link: Data removed on: Data removed by:

DC In charge