

I.T POLICY



RAGHU ENGINEERING COLLEGE

(Autonomous)

(Approved by AICTE, New Delhi, Permanently Affiliated to JNTU Kakinada,
Accredited by NBA & NAAC by A Grade)

Dakamarri Village, Bheemunipatnam Mandal, Visakhapatnam Dist. – 531 162 (A.P)

Ph.: +91-8922-248001, 248002 Fax: + 91-8922-248011

E-mail: principal@raghuenggcollege.com website: www.raghuenggcollege.com

S.No	Chapter	Page Number
1	Need for IT Policy	2
2	Acceptable Use Policy	4
3	Employee Acceptable Use Policy	5
4	Student Acceptable Use Policy	7
5	Network Security Policy	9
6	Hostel Wi-Fi Use Policy	13
7	Email Use Policy	14
8	Hardware and Software Procurement Policy	17
9	IT Hardware Installation Policy	18
10	Software Installation & Licensing Policy	20
11	Web Site Hosting Policy	22
12	Database Use Policy	23
13	Responsibilities of Centre for Technical Support	25
14	Responsibilities of Sections, Department	28
15	Responsibilities of the Administrative Units	32
16	Guidelines for Desktop Users	33
17	Video Surveillance Policy	35
18	Maintenance Policy – Systems & Network	38

RAGHU ENGINEERING COLLEGE (REC)

IT POLICY

The guidelines for using REC computer and IT communication tools are upheld by the Centre for Technical Support (CTS). The annual evaluation of current policies and the selection of those to be audited for REC compliance are also included in the IT Policy process.

These policies apply to everyone in the REC community, and it is assumed that they are all well-understood. The whole spectrum of disciplinary measures, including expulsion or termination, will be applied to violators.

The REC maintains the right to interpret, modify, or eliminate any of the provisions of these policies as the REC deems necessary in its sole discretion in order to maintain the essential flexibility in the administration of policies.

1. NEED FOR IT POLICY

The goal of IT policy is to offer information about permissible and banned behaviour as well as policy infractions and to set direction. To help organisations, departments, and members of the REC community understand how institution policy applies to some of the key areas and to bring conformance with stated policies, guidelines have been developed and made available.

IT policies may be classified into following groups:

Acceptable Use Policy

Hardware and Software Procurement Policy

IT Hardware Installation Policy

Software Installation and Licensing Policy

Network Use Policy

E-mail Account Use Policy

Web Site Hosting Policy

Database Use Policy

Further, the policies will be applicable at two levels:

- I. End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- II. Network Administrators

It should be noted that the REC IT Policy applies to technology that is managed centrally by the institution or by specific departments, to information services offered by the REC administration or by specific departments, to members of the REC community, or by authorised residents or non-resident visitors using their own hardware connected to the institution's network.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the Institution, hostels wherever the network facility was provided by the Institution. When linked to the campus network, privately owned computers are subject to the Dos and Don'ts listed in the REC IT policy. Additionally, the Guidelines must be followed by all faculty, students, employees, departments, authorised visitors, visiting faculty, and others who may be given permission to utilise the REC IT Infrastructure. Any institution member who violates a specific provision of the REC's IT policy risks disciplinary action from the institution's administration.

Applies to,

Stake holders on campus or off campus Students:

- UG, PG
- Faculty
- Administrative Staff (Non-Technical /Technical)
- Higher Authorities
- Guests

Resources

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

2. ACCEPTABLE USE POLICY

An Acceptable Use Policy is a collection of guidelines implemented by the owner, creator, or administrator, departments, internet service providers, and website owners, frequently with little chance of being enforced. Its purpose is to lessen the possibility of legal action being taken by a user.

- Employee Acceptable Use Policy
- Student Acceptable Use Policy
- Network Security Policy
- Addressing and Domain Services
- Network Connections
- Wireless
- External Traffic, Services and Requests
- Network Security
- Enforcement
- Monitoring and Auditing
- Email Use Policy

3. EMPLOYEE ACCEPTABLE USE POLICY

Purpose

Access is allowed pursuant to institutional norms and comes with particular responsibilities and obligations regarding computer systems and networks that are owned or run by REC. Acceptable use must be moral, display academic integrity, and exercise moderation when using common resources. It exhibits respect for people's rights to privacy and freedom from harassment and intimidation as well as for intellectual property, data ownership, system security, and these rights.

Policy Statement

1. Sharing of passwords, PINs, tokens or other authentication information is strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).
2. It is not permitted to use REC resources to gain access to, support, or engage in any other activity that is at odds with the institution's objective. This includes, but is not limited to, unlawful activities, pornographic content, hate speech, bullying and aggressive behaviour, spam, hacking, etc. Individuals participating in routine pedagogically related activity or research are permitted an exemption, so long as it is in line with the mission of the REC.
3. The use of REC resources to conduct business for personal financial gain is prohibited.
4. Anti-virus and anti-malware software must be installed on your computer, kept up to date and currently enabled. If your software is not up to date or disabled it may lead to an infection.
5. Employees are responsible for their computer, including its hardware, software, and any network traffic transmitted by it. Please contact Centre for Technical Support (CTS) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.
6. The use of personal routers (wireless or wired) and/or DHCP servers outside of a contained lab environment is strictly prohibited. CTS will assist you if you require additional connectivity.

7. Without prior CTS approval, it is forbidden to use the institution network to deliver any service that is visible off-campus.

8. Configuring your computer to provide Internet or REC network system access to anyone who is not a REC faculty, staff member or student is prohibited.

4. STUDENT ACCEPTABLE USE POLICY

Purpose

Access to computer systems and networks owned or operated by REC imposes certain responsibilities and obligations and is granted subject to institution policies. Acceptable use must be moral, display academic integrity, and exercise moderation when using common resources. It exhibits respect for people's rights to privacy and freedom from harassment and intimidation as well as for intellectual property, data ownership, system security, and these rights.

Policy Statement

1. Sharing of passwords, PINs, tokens or other authentication information are strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).
2. It is not permitted to use REC resources to gain access to, support, or engage in any other activity that is at odds with the institution's objective. This includes, but is not limited to, unlawful activities, pornographic content, hate speech, bullying and aggressive behaviour, spam, hacking, etc. Individuals participating in routine pedagogically related activity or research are permitted an exemption, so long as it is in line with the mission of the REC.
3. The use of REC resources to conduct business for personal financial gain is prohibited.
4. Anti-virus and anti-malware software must be installed on your computer, kept up to date and currently enabled. If your software is not up to date or disabled it may lead to an infection.
5. Students are fully responsible for their computer, including its hardware, software, and any network traffic transmitted by it, regardless if this traffic was authorized by you or not. Please contact Centre for Technical Support (CTS) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.
6. The use of personal routers (wireless or wired) and/or DHCP servers is strictly prohibited.
7. Using the institution network to provide any service that is visible off campus is prohibited.
8. Configuring your computer to provide Internet or REC network system access to anyone who is not an authorized REC faculty, staff member or student is prohibited.

9. Connecting standard mobile devices used for the pursuit of academic work to REC wireless network is permitted.

10. Some examples of policy violations:

- a. Accessing another user's personal private data
- b. Consuming a disproportionate amount of bandwidth
- c. Attempting or coordinating a denial-of-service attack
- d. Probing and/or exploiting security holes in other systems either on or off campus
- e. Using unauthorized IP addresses
- f. Using a network protocol analyser or similar mechanism without prior authorization
- g. Degrading or restricting network access for others, either on or off campus
- h. Connecting to Institution systems that one has not been expressly permitted to access
- i. Downloading, sharing or using copyrighted material including music, movies, software or text books
- j. Participating in activities which are not consistent with the Mission of the institution

5. NETWORK SECURITY POLICY

Purpose

This policy aims to safeguard the integrity of the campus network, reduce the risks and losses brought on by security threats to computing resources, and provide the Institution community with dependable and secure network performance. This policy is necessary to provide a reliable campus network to conduct and prevent unauthorized access to institutional, research or personal data. Additionally, it is the Institution's duty under the law to protect its networks and systems from an authorised usage.

Addressing and Domain Services

1. Centre for Technical Support (CTS) is solely responsible for managing any and all Internet domain names related to REC. Individuals, Departments or administrative departments may not create nor support additional Internet domains without prior approval from CTS.
2. To ensure the stability of network communications, CTS will solely provision and manage both the public and private IP address spaces in use by the Institution.
3. CTS may delegate administrative responsibilities to individuals for certain network ranges, but retains the right of ownership for those networks.

Network Connections

1. Without CTS's previous assessment and consent, REC faculty, staff, or students are not permitted to connect any devices or systems to the Institution networks or to engage with an outside vendor to do so. Centers, and Departments must first acquire CTS approval before granting Internet or other network access to users or networks that are not directly connected to the Institution.
2. In order to maintain reliable network connectivity, no other department may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus without prior review and approval of CTS.

3. Users are permitted to attach devices to the network provided that they are: for use with normal Institution or student operations do not interfere with other devices on the network are in compliance with all other REC policies.

4. Unauthorized access to Institution networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with Institution network equipment.

5. Unauthorized access to Institution equipment/cabling rooms is also prohibited.

Wireless

1. Centre for Technical Support (CTS) is solely responsible for providing wireless networking services on campus. No other department may deploy wireless routers, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus.

2. CTS is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.

3. The Institution will maintain a campus wireless network based only on IEEE 802.11 standards. CTS will collaborate with academic departments where devices used for specific educational or research applications may require specific support or solutions.

4. CTS will provide a general method for network authentication to Institution systems. The IEEE 802.1x standard is the currently supported authentication method. Additional security protocols may be applied as needed.

5. All users of wireless network resources at REC are subject to the applicable Network Acceptable Use Policy. Users of wireless resources at REC agree to have read and be bound by the terms and conditions set forth in that policy.

External Traffic, Services and Requests

1. CTS will take action to prevent spoofing of internal network addresses from the Internet. CTS will also take action to protect external Internet sites from source address forgery from devices on the Institution network.

2. The Institution external Internet firewall default practice is to deny all external Internet traffic to the Institution network unless explicitly permitted. To facilitate this, Departments and other administrative departments must register systems with CTS which require access from the Internet. Users that would like to request access through the Institution firewall must contact CTS

3. Access and service restrictions may be enforced by Device, IP address, Port number or Application behaviour.

Network Security

1. CTS may look into any intrusion on computer networks, systems, or equipment. When necessary, CTS will collaborate with administrative or academic departments as well as police enforcement.

2. Adequate security must be implemented and maintained on all devices connecting to the network, and they must be set and kept up-to-date in a way that forbids misuse or unauthorised access.

3. It is the duty of all REC users to report any security issues to the relevant supervisor or CTS for further investigation.

4. CTS retains the right to isolate or disconnect from the Institution network at any moment any system or device.

5. Network usage that the Institution deems appropriate is allowed. Unsuitable behaviours can include, but are not limited to:

- a. Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCP or DNS servers; or a computer set up to act like such a device.
- b. Engaging in network packet sniffing or snooping.
- c. Setting up a system to appear like another authorized system on the network (Trojan).
- d. Other unauthorized or prohibited use under this or any other Institution policy.
 - i. Students may consult the Student Acceptable Use Policy for further information.
 - ii. Employees may consult the Employee Acceptable Use Policy for further information.

Enforcement

1. Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the Institution network. CTS may subsequently require specific security improvements where potential security problems are identified before the device may be reconnected.
2. It is against this policy to attempt to get around administrative or security access restrictions for information resources. This policy is broken if you help someone else or ask them to get around security or administrative access limits.
3. The Institution retains the right to investigate any alleged security breach or policy violation, copy or study relevant files and information stored on Institution systems, and test and monitor security.

Monitoring and Auditing

1. For the purpose of security auditing, CTS will keep track of and retain traffic logs for all network devices and systems.
2. CTS maintains the right to monitor, access, retrieve, read, and/or disclose data transmissions when there is a good basis to suspect a breach of institutional policy, criminal behaviour, monitoring that is necessary for legal purposes, or in response to a legitimate management request. A report of a policy violation or criminal offence, as well as incidental observations made while performing the regular tasks of CTS employees, may serve as reasonable grounds.

6. HOSTEL WIFI USE POLICY

- Wireless infrastructure is used in hostels to improve internet accessibility for academic reasons and to view premium online resources.
- The signal's accessibility varies from location to location. Additionally, the signal strength may differ from one site to another. Access to wireless internet is simply an extended service, and neither students nor anyone staying in the hostels can require that every area in every floor of every block have the same kind of signal strength, coverage, and throughput. Wireless services are only available at the college's discretion, and if necessary for any technical reason, the college has the right to cease or interrupt the services at any time.
- The college owns the access points that are provided in the hostels, so any loss or damage to the equipment will be viewed as a serious violation of the college's code of conduct. Discipline will be taken against any students found responsible for the loss or damage of the wireless infrastructure or the corresponding equipment in the hostel buildings. If the wireless infrastructure is lost or damaged, CTS will assess the loss or damage and collect payment from all students staying in that floor, building, or hostel.
- Throughout all working days, Wi-Fi access will be disabled from 9 AM to 4 PM.

7. EMAIL USE POLICY

Summary

This policy applies to all Employees and Students and describes how emails received using the REC email address should be used appropriately.

Guidelines

1. No disruptive or offensive messages, including remarks regarding race, gender, disability, age, sexual orientation, religion, or national origin, may be created or sent using the REC email system. Any employees who receive emails from REC staff members with this content should report it right away to the Principal - REC.
2. The Acceptable Use Policy must be followed in every email sent or received through a REC mail account.
3. The REC's policies and processes will be followed in handling violations of this policy.

Employees

1. It is advised to use the REC e-mail services for all formal REC communication as well as for academic and other official reasons in order to maximise the efficiency of disseminating important information to all faculty, staff, students, and the Institution's administration.
2. Using email for official communications will make it easier to convey messages and documents to the campus and wider communities, as well as to specific user groups and people. Official messages from the Institution to its teachers, staff, and students are known as formal Institution communications. These messages may contain administrative information like details about human resources, policy announcements, messages for the entire institution, etc.
3. The email address must be kept active by being used frequently in order to get these notices. By entering their User ID and password into the G-Suite-hosted REC mail, staff and faculty can use the email service. Every employee receives an official REC email ID upon joining. The Center for Technical Support (CTS) creates the email IDs after receiving approval from the relevant departments.

Users might be informed that by using the email feature, they consent to the following rules:

1. The facilities should largely be used for academic and professional purposes, with some personal use permitted.

The amount of storage allotted to users is listed below.

- i. Core Group – Unlimited
- ii. Staff & Students – 15GB

2. Using the facility for illicit or commercial reasons is against REC IT policy and may result in facility withdrawal. Unauthorized and illegal software copying or distribution, sending unsolicited bulk e-mails, and creating harassing, threatening, abusive, vulgar, or fraudulent words or images are only a few examples of illicit uses.

3. Before sending someone a huge attachment through email, the sender should confirm that the recipient has email access to accept such files.

4. The user should keep the mail box's used space under the 80% mark since messages that are "mail box full" or "mailbox all but full" will bounce, especially if they come with huge attachments.

5. The user should not open any attachments or emails 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 crucial from the user's computer's security perspective, as such messages may contain viruses that have the ability to damage the important data on your computer.

6. Users are responsible for maintaining a backup of their account's incoming and outgoing mail.

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.

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

9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

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

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

12. Any spam mail received by the user into Inbox should not be forwarded to anyone and could be deleted.

Students

Students are given REC mail ID under the domain raghuenggcollege.in hosted in G-Suite with unlimited storage space. Students will be able to use all the features offered by Google. Once the student relieved from the college, the mail id will be deactivated after 2 years. A prior notification will be sent to student well in advance before the deactivating.

8. HARDWARE AND SOFTWARE PROCUREMENT POLICY

Policy

1. The procurement of all computing and communication hardware and software is coordinated by the office of Centre for Technical Support (CTS) in order to maximize the REC investment in Information Technology (IT).
2. To take advantage of IT tools in the most cost-effective manner possible, the REC has standardized a series of hardware and software products that integrate easily with the Institution's IT infrastructure. When considering the purchase of hardware or software, departments should coordinate their purchase with CTS.
3. While the acquisition of standard products is encouraged, some departments have need for special equipment. CTS will consult with the department to select the most appropriate equipment and to work out an agreement for continued support.
4. Departments who choose to buy IT resources not approved by CTS are responsible for their implementation and ongoing maintenance. CTS will not be responsible for interfacing such hardware or software to the campus network or information repository.
5. In accordance with the REC funding philosophy, costs for the acquisition of IT resources are borne by the purchaser.

9. IT HARDWARE INSTALLATION POLICY

Institution 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.

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.

What are End User Computer Systems

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

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department should preferably be with 2-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract either with a third party or with support from CTS. Such maintenance should include OS re-installation and checking virus related problems also.

Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through 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 earthing and have properly laid electrical wiring.

Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required.

Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written intimation to the CTS, as CTS maintains a record of computers

Maintenance of Computer Systems provided by the Institution

For all the computers that were purchased by the institution centrally and distributed by the Purchase Department, CTS Department will attend the complaints related to any maintenance related problems.

Noncompliance

REC 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 institution. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

10. 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, Institution IT policy does not allow any pirated/unauthorized software installation on the institution owned computers and the computers connected to the institution campus network. In case of any such instances, institution will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all Microsoft Windows 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.
2. Institution 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.

B. Antivirus Software and its updating

1. Computer systems used in the institution 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.
2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.
3. 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 serviceproviding agency.

C. Backups of Data

1. 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.
2. 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 fool proof solution. Apart from this, users should keep their valuable data either on DVD, Flash Drive or other storage devices.

11. WED SITE HOSTING POLICY

Policy

1. REChas an official website raghuenggcollege.in. Departments may have pages on REC's official Web page. Official Web pages must conform to the Institution Web Site Creation Guidelines for Website hosting. As on date, the Web Team at CTS is responsible for maintaining the official website of the institution.
2. Any department or an individual requires to publish any official content in the institution official website may sent the content to info@raghuenggcollege.in, committee responsible for approving the content, with a copy to the reporting authority. CTS web team will facilitate in creating and updating the content in the website.

12. DATABASE USE POLICY

This Policy relates to the databases maintained by the institution administration under the institution's e-governance. Data is a vital and important Institution resource for providing useful information. Its use must be protected even when the data may not be confidential.

REC 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 institution's approach to both the access and use of this institution resource.

A. Database Ownership: REC is the data owner of all the Institution's institutional data generated in the institution.

B. Custodians of Data: Individual Sections or departments generate portions of data that constitute Institution's database. They may have custodianship responsibilities for portions of that data.

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

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The institution's data policies do not allow the distribution of data that is identifiable to a person outside the institution.
2. Data from the Institution's Database including data collected by departments or individual faculty and staff, is for internal institution purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the institution makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the Institution Registrar.

5. Requests for information from any courts, attorneys, etc. are handled by the Principal Office of the Institution 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 Institution Principal for response Tampering of the database by the department or individual user comes under violation of IT policy.

Tampering includes, but not limited to:

- Modifying/deleting the data items or software components by using illegal access methods.
- Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/departments.
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.

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

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

13. RESPONSIBILITIES OF CENTRE FOR TECHNICAL SUPPORT (CTS)

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by CTS.
2. CTS operates the campus network backbone such that service levels are maintained as required by the Institution Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of CTS.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of CTS. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the CTS. 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 CTS.
3. It is not the policy of the Institution 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 Institution's Internet links.

C. Network Expansion

Major network expansion is also the responsibility of CTS. Network expansion will be carried out by CTS when the institution makes the necessary funds available based on the requirement.

D. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations CTS considers providing network connection through wireless connectivity.
2. CTS is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from CTS prior to implementation of wireless local area networks.

3. CTS 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.

E. 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.

F. Global Naming & IP Addressing

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

G. Providing Net Access

By default, all the faculty members are given internet access in their laptops. Students are given internet access under the supervision of the faculty.

H. Network Operation Center

CTS is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available 12 hours a day, 7 days a week. All network failures and excess utilization are reported to the CTS technical staff for problem resolution.

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the CTS. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, CTS will analyze 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.

I. Network Policy and Technology Standards Implementation

CTS 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.

J. Receiving Complaints

CTS may receive complaints from departments/schools/any user, if any of the networks related problems faced by them during the course of using the infrastructure. Such complaints should be by using the ticketing system available in the intranet portal or people orbit. However, users may register their complaint using email/phone call also. CTS Technical staff coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

CTS will be responsible only for solving the Hardware/Software/network related problems or services related to the Hardware/Software/Network only.

L. Disconnect Authorization

CTS will be constrained to disconnect any 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, CTS endeavours 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, CTS provides the conditions that must be met to be reconnected.

14. RESPONSIBILITIES OF DEPARTMENT OR SECTIONS

A. User Account

Any Centre, department, or Section or other entity can connect to the Institution network using a legitimate user account for the purposes of verification of affiliation with the institution. However, the users in workgroup can access the network with any user account.

Once a user account is allocated for accessing the institution's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the institution 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 REC Institution community, when using the institution network facilities and its user account, it becomes user's duty to respect the Institution's reputation in all his/her electronic dealings within as well as outside the Institution. It is the duty of the user to know the IT policy of the institution and follow the guidelines to make proper use of the institution's technology and information resources.

B. Logical Demarcation of Department/ Section/Division Networks

In some cases, Section, department or Division might have created a internal network within their premises. In such cases, the Section, department, or division assumes responsibility for the network service that is provided on all such internal networks on the department or division 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.

C. Supply of Information by Department, or Section for Publishing on / updating the REC Website

All Centers, Departments, or Divisions should provide updated information concerning them to CTS by e-mail for uploading it in the website. If the content is in large size, may sent to CTS through pen drive or CD.

D. Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the Institution 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.

E. 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 institution are the property of the institution and are maintained by CTS.
- Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,
 - Removal of network inlet box.
 - Removal of UTP cable from the room.
 - Opening the rack and changing the connections of the ports either at jack panel level or switch level.
 - Taking away the UPS or batteries from the switch room.
- Disturbing the existing network infrastructure as a part of renovation of the location CTS 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.

F. Additions to the Existing Network

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

Institution Network policy requires following procedures to be followed for any network expansions: All the internal network cabling should be as on date of CAT6UTP. UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network. UTP cables should be properly terminated at both ends following the structured cabling standards. Only managed switches should be used. Such management module should be web enabled. Using unmanaged switches is prohibited under institution's IT policy. Managed switches give the facility of managing them through web so that CTS 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. As managed switches require IP address allocation, the same can be obtained from CTS on request.

G. 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.

H. Campus Network Services Use Policy

The "Campus Network Services Use Policy" should be read by all members of the institution who seek network access through the institution campus network backbone. This can be found on the Intranet 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 institution IT policy. It is user's responsibility to be aware of the Institution IT policy. Ignorance of existence of institution IT policy is not an excuse for any user's infractions.

I. Enforcement

CTS periodically scans the Institution 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.

15. RESPONSIBILITIES OF THE ADMINISTRATIVE UNITS

CTS needs latest information from the different Administrative Units of the Institution for providing network and other IT facilities to the new members of the institution and for withdrawal of these facilities from those who are leaving the institution, and also for keeping the institution web site upto-date in respect of its contents.

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

- A. Information about New Appointments/Promotions.
- B. Information about Super annotations / Termination of Services.
- C. Information of New Enrolments.
- D. Information on Expiry of Studentship/Removal of Names from the Rolls.
- E. Any action by the institution authorities that makes an individual ineligible for using the institution's network facilities.
- F. Information on Important Events/Developments/Achievements.
- G. Information on different Rules, Procedures, and Facilities

Information related to items nos. A through E should reach Admin (Systems) and Information related items nos. F and G should reach webmaster well in-time.

16. GUIDELINES FOR DESKTOP USERS

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

The following recommendations include:

1. All desktop computers should have antivirus and should retain the setting that schedules regular updates of virus definitions..
2. 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.
3. The password should be difficult to break. Password, defined as: must be minimum of 6-8 characters in length must include punctuation such as !\$% & *,.?+ -= must start and end with letters must not include the characters # @ "" must be new, not used before Avoid using your own name, or names of your wife or children, or name of your department, or Room No. or House No & etc. passwords should be changed periodically and also when suspected that it is known to others. Never use 'NOPASS' as your password. Do not leave password blank and Make it a point to change default passwords given by the software at the time of installation
4. The password for the user login should follow the same parameters outlined above.
5. The guest account should be disabled.
6. New machines with Windows XP should activate the built-in firewall.
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.
8. 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.

9. 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).
10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
11. 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.
12. In addition to the above suggestions, CTS 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.
13. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.
14. If a machine is compromised, CTS 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. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, CTS technical personnel can scan the servers for vulnerabilities upon request.

17. VIDEO SURVEILLANCE POLICY

A. The system

1. The system comprises: Fixed position cameras; Monitors; Multiplexers; digital recorders; Storage;
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.
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.
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.

B. Purpose of the system

The system has been installed by institution with the primary purpose of reducing the threat of crime generally, protecting college premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to: Deter those having criminal intent Assist in the prevention and detection of crime Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to administrators and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken. In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used: To provide recorded images for the world-wide-web. To record sound other than in accordance with the policy on covert recording. For any automated decision taking

C. The Security Control Room

1. Images captured by the system will be monitored and recorded in the Security Control Room. Monitors are not visible from outside the control room.
2. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry.
3. 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.

D. Security Control Room Administration and Procedures

1. 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.
2. 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.

E. 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.

F. Recording

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

2. Images will normally be retained for 20 to 30 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.
3. All hard drives and recorders shall remain the property of institution until disposal and destruction.

G. Access to images

1. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.
2. Access to images by third parties
3. 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: Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder Prosecution agencies Relevant legal representatives 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 People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings. Emergency services in connection with the investigation of an accident.

H. Complaints

It is recognized that members of Institution and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Chief Security Officer.

18. MAINTENANCE POLICY –SYSTEM & NETWORK

Lab System Maintenance Policy

Lab systems are maintained by the Lab assistant. Primary level problems are taken care by Lab assistant.

- Power connections
- Booting problem
- Network problem
- Software installation / uninstallation
- Hardware troubleshoot o Hardware replacement
- Time schedule Internet maintenance.

Major Network, Software and Operating system related Problem are taken care by CTS Staff

Standalone Systems Maintenance Policy

Other than lab systems are maintained by CTS staff, notably like Administration Office, Principal Office, Departments, Library, Seminar Hall systems.

Escalation methods:

- Phone call
- Official Letters
- Meeting in-person

General problem:

- Power connections
- Booting problem
- Network problem
- Software installation /uninstallation
- Hardware troubleshoot o Hardware replacement

Network & Surveillance Maintenance:

Network switch, Wireless Access points, CCTV, Biometric and Digital Medias

- Network switches are configured and installed in required locations
- VLAN creations based on lab and Department o
- Port security
- Increasing the switch on demand.

Wireless Access points

Access points are placed in staffrooms, near class rooms, labs and on demand places

- Channelizing based on users
- Widening the Access points depends on signal coverage.
- Access points are deployed temporarily on demand basis.
- DHCP used to bring the Laptops into the Network
- Internet are provided by binding the MAC address.
- Internet Policy varies depending upon the functionality of the users.

Surveillance

CCTV cameras are erected in the important location in Buildings, Hostels and Roadside.

- CCTV configured and installed in the required locations o Bullet and Doom CCTV are used based on the places Faulty CCTV are serviced and installed.
- The video datas are stored for 1 month.
- The footage are given on demand by Security team, supported by CTS
- The Playback and administration are done by Monitoring software of the Brand.

