KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES

IT-POLICY

Table of Contents

1. Need for IT Policy

- IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for all the Students, faculty, Staff, Management and visiting Guests.
- Due to the policy initiative and academic drives, IT resource utilization in the Campus has grown by leaps and bounds during the last decade.

Campus has network connections to every computer system covering two blocks.

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

Computer Center is running the Firewall security, DHCP, DNS, email, web and application servers and managing the network of the institute.

College is getting its Internet bandwidth from BSNL & BlueWeb Technologies. Total bandwidth availability from BSNLsource is 40 Mbps and BlueWeb Technologies is 50 Mbps (leased line 1:1).

With the extensive use of the Internet, network performance outreach in three ways:

- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.
- When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users, who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service and Quality of Experience. Reducing Internet traffic is the answer.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires.

It may be noted that institute IT Policy applies to technology administered by the institute centrally or by the individual departments, to information services provided by the institute administration, or by the individual departments, or by individuals of the institute community, or by authorized resident or non-resident visitors on their own hardware connected to the institute network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the institute, or hostels and guest houses, or residences wherever the network facility was provided by the institute.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the Institute's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by the institute by any institute member may even result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

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

Resources

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

2. Vision and Mission

VISION

- To produce eminent and ethical Engineers and Managers for society by imparting

quality professional education with emphasis on human values and holistic excellence.

MISSION

- To incorporate benchmarked teaching and learning pedagogies in curriculum.
- To ensure all round development of students through judicious blend of curricular, co-curricular and extracurricular activities.
- To support cross-cultural exchange of knowledge between industry and academy.
- To provide higher/continued education and research opportunities to the employees of the institution.

3. IT Hardware Installation Policy

Institute network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

a) 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.

b) End User Computer Systems

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

c) Warranty & Annual Maintenance Contract

Computers purchased by any Department/Cells should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers would be maintained by Computer Center or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

d) 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.

e) 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.

f) 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.

g) Maintenance of Computer Systems provided by the Institute

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

h) Computer Center Interface

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/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The Computer Center will provide guidance as needed for the individual to gain compliance.

4. Software Installation and Licensing Policy

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

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

computers connected to the institute campus network. In case of any such instances, institute will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

a) 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.

b) Backups of Data

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

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

c) Computer Center Interface

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/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The Computer Center will provide guidance as needed for the individual to gain compliance.

5. Network (Intranet & Internet) Use Policy

Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the Institute IT Policy. The Computer Center is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to Computer Center.

a) IP Address Allocation

Any computer (PC/Server) that will be connected to the institute network should have an IP address assigned by the Computer Center. Departments should follow a systematic approach, the range of IP addresses that will be allocated to each building / V LAN as 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 has to take IP address allocation from Computer Center / respective department.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports.

b) Proxy Configuration by Individual Departments /Cells

Use of any computer at end user location as a proxy 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 Computer Center.

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

c) 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 Computer 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.

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

Computer 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.

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 Computer 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.

d) Wireless Local Area Networks

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

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

If individual department wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the institute authorities whose application may be routed through the In Charge, Computer Center.

6. Email Account Use Policy

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

Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://gmail.com with college domain id **(kitsguntur.ac.in)** as their User ID. For obtaining the institute's email account, user may contact Computer Center for email account and default password by submitting an application in a prescribed proforma.

7. Web Site Hosting Policy

a) Official Pages

Departments, Cells, Committees, Academics, placements, central facilities may have pages in college official Web Site.

As on date, the Computer Center is responsible for maintaining the official web site of the institute., https://kitsguntur.ac.in/site/kits.php

b) Personal Pages

It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the institute by sending a written request or mail to Computer 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.

c) Responsibilities for updating Web Pages

System admin and web-site coordinator are responsible to send updated information time to timeabout their Web pages to Computer Center.

Information in a table form:-

Sl No.	Particulars	Details
1.	Bandwidth	90 MBPS
2.	Wi-Fi Router	15
3.	Firewall	Sonic wall NSA
4.	Computer	I3,i5 processor, 4 to 8 GB Ramand 500 GB/1 TB HDD
5.	CCTV	Throughout the campus