KLS Gogte Institute of Technology,
BELAGAVI-590008

IT Policies & Guidelines

(Release: May. 2022 Version 1.0)

Prepared by
Computer Center

KLS Gogte Institute of Technology

IT Policy

(Release: May. 2022 Version 1.0)

Need for IT Policy

- Basically the IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the KLS GIT on the campus.
- This policy establishes strategies and responsibilities for protecting the **Co**nfidentiality, **I**ntegrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the KLS GIT.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions. Realizing the importance of these services, KLS GIT took initiative way back in 2000 and established basic network infrastructure in theacademic complex of the campus.

Over the last five years, not only active users of the network facilities have increased many folds but also the web-based and streaming applications have increased. This is a welcome change in the academic environment. Now, the College has about 1200 network connections covering more than ten buildings (Main Building, Mech Building, Library, Structural, IT Block, Boys Hostel, Girls Hostel, Basic Workshop, IIPC Cell, and Aero workshop) across the campus and expected to reach 1500 connections very soon. Computer Center is the department that has been given the responsibility of running the College intranet & Internet services. It also running the Firewall security Sophos, DHCP, DNS, email, web andapplication servers and managing the network of the College.

KLS GIT is has Total bandwidth capacity of 1Gbps Internet leased line from various ISPs like BSNL - 100Mbps, FAAST - 450Mbps and AirTel - 450Mbps. On one hand, resources are not easily available for expansion to accommodate the continuousrise in Internet needs, on the other hand uncontrolled, uninterrupted and free web access can giverise to activities that are neither related to Teaching/learning processes nor governance of the college.

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

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

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

1. When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide AreaNetwork (WAN) is a potential bottleneck.
2. 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.
3. 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 ofthe 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. Reducing Internet traffic is the answer. Hence, in order to secure the network, Computer Center has been taking appropriate steps by installing firewalls, access controlling and installing Anti-virus checking and content filtering software.

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 intheir respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation.

Hence, KLS GIT also is proposing to have its own IT Policy that works as guidelines for using the College 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 well defined IT policies and guidelines that would be relevant in the context of this Institute. While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of College to understand how College policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

i. IT Hardware Installation Policy
ii. Software Installation and Licensing Policy
iii. Network (Intranet & Internet) Use Policy
iv. E-mail Account Use Policy
v. Web Site Hosting Policy
vi. Storage Use Policy

Further, the policies will be applicable at two levels:

A. End Users Groups (Faculty, students, administrators, Officers and other staff)
B. Network Administrators

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

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

The IT Policy framed with the available resources in the campus. These includes:

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

- Streaming and Multimedia Contents

Table of Contents

1. IT Hardware Installation Policy

College 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.

1.1 Who is Primary User?

An individual in whose room/office 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 personresponsible for compliance.

1.2 What are End User Computer Systems?

Apart from the client PCs used by the users**,** the college 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.

1.3 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 in house maintenance. Such maintenance should include OS re-installation, replacing damaged parts and checking virus related problems also.

1.4 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 theelectrical points that are provided with proper earthling and have properly laid electrical wiring.

1.5 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.

1.6 Maintenance of Computer Systems provided by the College

All the computers and accessories are procured centrally depending on requirement and Computer Center Maintenance Cell will attend the complaints received from the department.

The following is the process followed by the maintenance cell to address the issues occurred: Diagram.

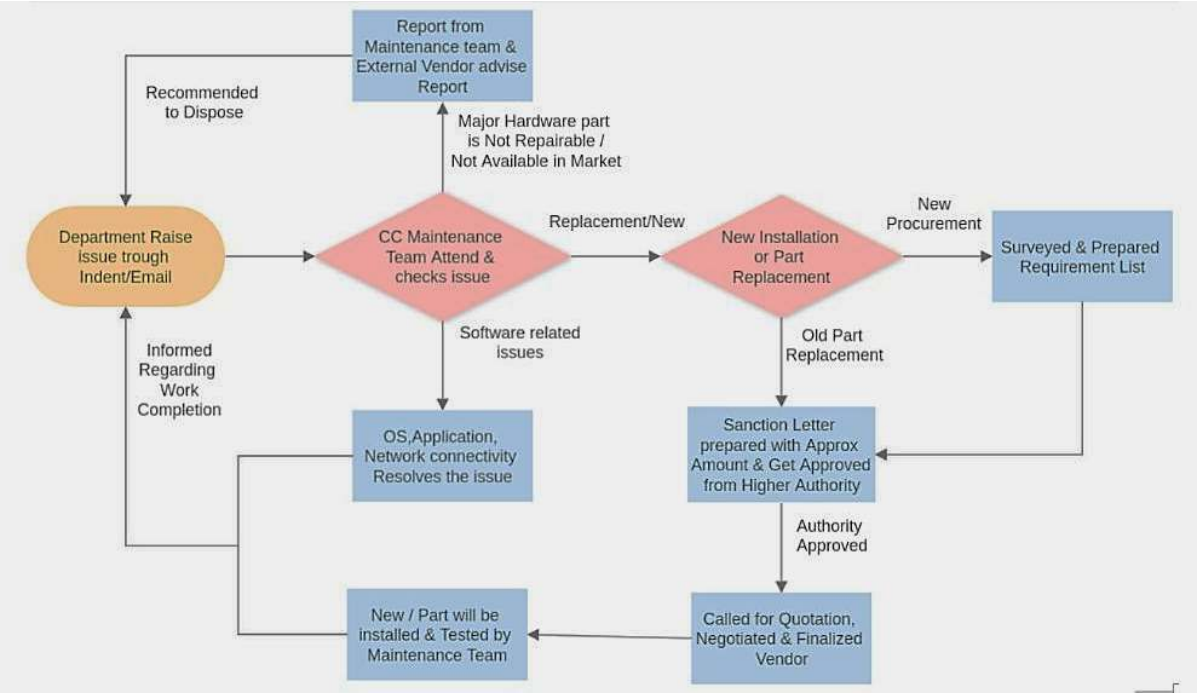

Figure 1.1: Process of Maintenance of Computers/ Network/ Accessories.

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

2.1 Operating System and its Updating

2.1.1 Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once ina week or so.

2.1.2 Individual users should make sure that respective computer systems have their MS windows base OS Licensing active under college campus-wide Microsoft Licensing.

2.1.3 College 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.

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

2.1.5 The computers that are connected to the network will follow the naming convention as depicted below for proper identification of systems.
Department_Staff-Initial_SystemNumber
Example: CC_VSP_01

2.2 Application Software and its Licensing

2.2.1 Computer systems used in the college should have legal application software installed. The primary user of a computer system is responsible for keeping the computer system compliant with this Legal License policy.

2.2.2. College as a policy encourages user to go for open source software such as Open office, freeware software to be used on their application usage.

2.3 Antivirus Software and its updating

2.3.1 Computer systems used in the college 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.

2.3.2 Individual users should make sure that respective computer systems have current virus protection software updated and maintained virus free.

2.4 Backups of Data

Individual users should take up 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 CD or other storage devices such as pen drives or Google drive.

2.5 Noncompliance

KLS GIT 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

3. Network (Intranet & Internet) Use Policy

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

3.1 IP Address Allocation

Any computer (PC/Server) that will be connected to the network, should have an IP address assigned by the Computer 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 send Email request to the Computer Center for IP address allocation. 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 sending Email requisition form meant for this purpose.

3.2 Dynamic Host Control Protocol (DHCP) and Proxy Configuration by Individual Departments /Sections/Users

- Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the College.
- Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by Computer Center.
- Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration. Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network.

3.3. Running Network Services on the Servers

Individual departments/ Staff individuals connecting to the college 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 College IT policy for running such services.
Non-compliance with this policy is a direct violation of the IT policy, and will result in termination of their connection to the Network.

3.4. Wireless Local Area Networks

This policy applies, in its entirety, to College, department, or division. wireless devices connected to wireless local area networks.

3.3.1. 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.

3.3.2. If individual or Department wants to have wireless network, prior to installation of such network, they should obtain permission from the Computer Center Head whose application must be routed through the Principal.

3.3.3. Use of personal wireless router in the college campus network is prohibited.

4. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the college administrators, it is recommended to utilize the college e-mail services, for formal 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 communications are official notices from the KLS and University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general 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 must use the email facility by logging on to **https://mail.git.edu or https:// gmail.com** with their **User ID** and **password**. For obtaining the email account, user may contact Computer Center for email account and default password by sending Email through HOD in a prescribed format

Users may be aware that by using the email facility, the users are agreeing to abide by the following rules:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. 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.
4. 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 itsauthenticity 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. 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.

6. 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.
7. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
8. 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.
9. While using the computers that are shared or other users as well, any email account open should be promptly closed without fail by the email account holder.
10. Impersonating email account of others will be taken as a serious offense under the IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of email usage policy.
12. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may take necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 12 are broadly applicable even to the email services that are provided by other sources such as gmail.com, Hotmail.com, Yahoo.com etc., as long as theyare being used from the college campus network, or by using the resources provided by the college to the individual for official use even from outside.

5. Responsibilities of Computer Center

The GIT Computer center is established to cater the computing needs of staff, student and take care of planning, development, co-ordination and maintenance of computing infrastructure. Following are the operations and responsibilities:

5.1. Campus Network Backbone Operations

5.1.1. The campus network backbone and its active and passive components are administered, maintained and controlled by Computer Center.

5.1.2. Computer Center operates the campus network backbone such that service levels are maintained as required by the College Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

5.2 Physical Demarcation of Campus Buildings' Network

5.2.1 Physical connectivity of existing campus buildings / Newly constructed building connected to the campus network backbone is the responsibility of Computer Center. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the Computer 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 Computer Center.

5.2.2 Computer 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.

5.3 Network Expansion

Major network expansion is also the responsibility of Computer Center. Every 3 to 5 years, Computer Center reviews the existing networking facilities, and need of the possible expansion. Network expansion will be carried out by Computer Center when the college makes thenecessary funds available.

5.4 Wireless Local Area Networks

5.4.1 Where access through Fiber Optic/UTP cables is not feasible, in such locations Computer Center considers providing network connection through wirelessconnectivity.

5.4.2 Computer Center is authorized to consider the applications of Sections,

departments, or divisions for the use of Wireless service from Computer Center prior to implementation of wireless local area networks.

5.4.3 Computer 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.

5.5 Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only beretained until the administrative need for them, later they may be destroyed.

5.6 Global Naming & IP Addressing

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

5.7 Providing Net Access IDs and email Accounts

Computer 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 college upon receiving the requests from the individuals on prescribed proforma.

5.8 Network Operation Center

Computer 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 Computer Center technical staff for problem resolution.

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the Computer Center. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, Computer 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 reportwill be sent to higher authorities in case the offenses are of very serious nature.

5.9 Network Policy and Technology Standards Implementation

Computer 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.

5.10 Receiving Complaints

Computer Center may receive complaints if any of the network related problems are noticed by them during the use of end-user computer systems related complaints. Such complaints should be by email/phone.The designated person in Computer Center receives complaints from the users/COMPUTER CENTER and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable amount of time limit.

5.11 Maintenance of Computer Hardware & Peripherals

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

5.12 Scope of Service

COMPUTER CENTER will be responsible only for solving the hardware, Network related problems or OS or any other application software that were legally purchased by the college.

5.13 Installation of Unauthorized Software

COMPUTER CENTER or its service engineers should not encourage installing any unauthorizedsoftware on the computer systems of the users. They should strictly refrain from obliging such requests.

5.14 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 university, such incidents should be brought to the notice of the coordinator and college authorities.

5.15 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.

5.16 Coordination with INTERNET UNIT

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network issue or the software installed or hardware malfunctioning, COMPUTER CENTER staff will coordinate to resolve the problem. This task should not be left to the individual user.

6. Responsibilities of Department or Sections

6.1 User Account

- Any Center, department, or Section or other entity can connect to the college network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the college.
- The user account will be provided by Computer Center. Once a user account is allocated for accessing the computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the college 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 unauthorized use of their user account by others.
- As a member of KLS GIT community, when using the network facilities andits user account, it becomes user's duty to respect the College reputation in all his/her electronic dealings within as well as outside the College. It is the duty of the user to know the IT policy of the College and follow the guidelines to make proper use of the KLS GIT technology and information resources.

6.2 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 Section, department or division side of the network backbone.
- The Section, department, or division is also responsiblefor 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, or division should identify at least one person as a Point of Contact and communicate it to Computer Center for any network/system related problem at its end.

6.3 Security

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

6.4 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 college are the property of the KLS GIT and are maintained by Computer Center.

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 Computer 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.

6.5 Additions to the Existing Network

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

The following procedures to be followed for any network expansions:

- All the internal network cabling should be as on date of CAT 6 Un-Twisted Pair cable(UTP).
- 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. Managed switches give the facility of managing them through web so that Computer 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 located due to the fact that it is behind an hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

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

7.1 Mandatory

1. Provide the e-mail address or contact number of the Web page designer.
2. Provide a link to the KLS GIT home page from the parent (department of origin) home page.
3. Provide a link to the parent home page ("Return to department's home page") on all supportinglocal pages.
4. Maintain up to date pages. Proofread pages and test links before putting them on the Web, andregularly test and update links.
5. Know the function of HTML tags and use them appropriately.
6. Make provision for providing information without images as printer-friendly versions of theimportant web pages.

7.2 Recommended

1. Provide information on timeliness (for example: August 2021; updated weekly/monthly etc….).
2. Provide a section indicating "What's New."
3. Provide a caution statement if link will lead to large pages or images.
4. Indicate restricted access where appropriate.
5. Avoid browser-specific terminology.
6. Provide link text that is clear without the link saying 'click here' whenever hyperlinks are used.
7. Maintain visual consistency across related pages.
8. Provide a copyright statement (if and when appropriate).
9. Keep home pages short and simple.
10. Avoid using large graphics or too many graphics on a single page.
11. Provide navigational aids useful to your users (Link to Home, Table of Contents, Next Page, etc.).
12. Maintain links to mentioned pages.
13. Make your Web pages easy to maintain for yourself and anyone who might maintain them in the future.
14. Avoid active links to pages that are in development. Place test or draft pages in your "test," "temp," or "old" sub-directory. Remember that nothing is private on the Internet: unlike pages in your directory may be visible.
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.
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).

17. Conform to accepted, standard HTML codes.

8. Guidelines for Desktop Users

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

The following recommendations include:

1. All desktop computers should have the latest version of antivirus such as Kaspersky Anti-Virus (PC) or Quick Heal and should retain the setting that schedules scan and regularupdates of virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should beapplied (licensed MS windows) regularly, on anongoing basis. We recommend once in a week cycle for each machine check System update. Whenever possible, security policies should be set at the server level and applied to the desktop machines.
3. All Windows desktops (and Linux 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.
4. The password should be difficult to break. The following points may be followed to define the Password:
    a. must be minimum of 6-8 characters in length
    b. must include punctuation such as ! $ % & * , . ? + - =
    c. must start and end with letters
    d. must not include the characters # @ ' " `
    e. must be new, not used before
    f. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.
    g. passwords should be changed periodically and also when suspected that it is known to others.
    h. Never use 'NOPASS' as your password
    i. Do not leave password blank and
    j. Make it a point to change default passwords given by the software at the time of installation
5. The password for the user login should follow the same parameters outlined above.
6. The guest account should be disabled.
7. New machines with Windows should activate the built-in firewall.
8. 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.
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). 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 files should be copiedfrom 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.

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, 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.
13. If a machine is compromised, System needs to shut the network 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.