GUJARAT TECHNOLOGICAL UNIVERSITY
AHMEDABAD

IT Policies & Guidelines

(with effect from 6th April, 2023 Version 3.0)

Index

Chapter 1 Need for IT Policy

- Basically the University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.

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

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

- The purpose of Information Security Policy ("Policy") is to outline Organization expectations and required practices with regard to the administrative, physical and technical safeguards designed to protect the confidentiality, integrity, and availability of information.

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Over the last ten years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the university's academic environment. Now, the university has about 450 network connections across the campus. IT Dept. is the department that has been given the responsibility of running the university's intranet & Internet services.

IT Dept. is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university.

GTU is getting its Internet bandwidth from BSNL. Total bandwidth availability from BSNL source is 1 Gbps (leased line) under NKN Network of MHRD (NME-ICT) via BSNL. It also have bandwidth of 20 Mbps from Blazenet and BSNL.

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

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

With the extensive use of the Internet, network performance suffers 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. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe downloads, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network.

They can slow down or even bring the network to a halt.

A virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, Internet Unit has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

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. 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.

Policies also serve as blueprints that help the institution implement security measures.

An effective security policy is as necessary to a good information security program as a solid foundation to the building.

Hence, Gujarat Technological University also is proposing to have its own IT Policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this university.

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.

Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern its security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

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 university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- University Database Use Policy

Further, the policies will be applicable at two levels:

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

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

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 university IT policy.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by

the university by any university member may even result in disciplinary action against the offender by the university 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/ Temporary/ Contractual)
- 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

Chapter 2 IT Related Policies

2.1 IT Hardware Installation Policy

University 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. Who is Primary User

An individual who is having room, the computer is installed and is primarily used by him/her, is considered to be “primary” user. If a computer has multiple users, no one in them are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. What are End User Computer Systems

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

C. 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.

D. 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.

E. Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written intimation to the Store Dept., as Store Dept., maintains a record of computer identification names. Such computer identification names follow the convention that it comprises building name abbreviation and room no. As and when any deviation (from the list maintained by Store Dept.) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs Store Dept. in writing/by email, connection will be restored.

F. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the Store Dept., University Computer Maintenance Cell will attend the complaints related to any maintenance related problems.

G. Noncompliance

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

H. IT Dept. Interface

IT Dept. finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The IT dept. will provide guidance as needed for the individual to gain compliance.

2.2 Software Installation and Licensing Policy

Any System (PC) 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, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the department/individual personally responsible for any pirated software installed on the computers located in their departments/individual rooms. To install the additional software in university owned computers, prior permission of IT section is required.

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 based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. University policies encourage user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

3. Any Microsoft Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates a being done properly.

B. Antivirus Software and its updating

1. Computer systems used in the university 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.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

C. Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data. 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 users 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 Drive or other storage devices such as pen drives.

D. Noncompliance

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

2.3 Network (Intranet & Internet) Use Policy

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

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the INTERNET UNIT. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

As and when a new computer is installed in any location, the concerned user can download the application form available in Annexure-2 for the purpose of IP address allocation get the IP address from the IT Dept.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

B. 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 university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by IT Dept.

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. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running Network Services on the Servers

Individual departments/individual connecting to the university 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 IT Dept. in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

IT Dept. takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

IT Dept. 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 side activity adversely affects the Network performance.

Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University 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 IT Dept.

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. Dial-up/Broadband Connections

Computer systems that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the university's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies to School, department, or division wireless local area networks. In addition to the requirements of this policy school, departments, or divisions must register each wireless access point with IT Dept. including Point of Contact information.

2. School, departments, or divisions must inform IT Dept. for the use of radio spectrum, prior to implementation of wireless local area networks.

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

4. If individual School wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Registrar, IT Dept.

F. Internet Bandwidth obtained by Other Departments

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

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

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

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

2.4 Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University 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 University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University 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 gmail.com with their User ID and password. For obtaining the university's email account, user may contact IT Dept. for email account and default password by submitting an application in a prescribed proforma.

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

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of

security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.

6. Users should configure messaging software (Outlook Express/ any mail 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.
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 university IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.
12. Users are not required to delete any email communication from email account.

The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, office 365 etc., as long as they are being used from the university campus network, or by using the resources provided by the university to the individual for official use even from outside.

2.5 University Database Use Policy

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential.
GTU 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 university's approach to both the access and use of this university resource.

A. **Database Ownership:** Gujarat Technological University is the data owner of all the University's institutional data generated in the university.

B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute University'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.

D**. MIS Components:** For the purpose of eGovernance, Management Information System requirements of the university may broadly be divided into seven categories. These are:

- MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
- STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)

- FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
- PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
- PROJECT INFORMATION MONITORING SYSTEM (PIMS)
- LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
- DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

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

1. The university data policies do not allow the distribution of data that is identifiable to a person outside the university.

2. Data from the University Database including data collected by departments or individual faculty and staff, is for internal university purposes only.

3. Once role and function define the data resources that will be needed to carry out once official responsibilities/rights. Through its data access policies the university 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 University Registrar.

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

6. At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.

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

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

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

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

Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities.
If the matter involves illegal action, law enforcement agencies may become involved.

2.6 Acceptable Use Policy

All computer, email, voice, and Intranet systems, as well as access to the Internet and other on- line resources are provided by Organization for the use of its employees for university work purposes. These systems are the property of Organization and must be used in accordance with professional standards and Organization policies and procedures, including this Policy.

In some circumstances more specific policies and/or legal legislation may exist and take precedence over the general policies contained herein.

Lawful and Acceptable Use
All data created on corporate systems becomes the property of Organization and should be afforded confidential treatment to the extent required. While some level of personal use is tolerable, employees should exercise reasonable judgment and must adhere to all other policies and guidelines noted herein.

All users have an ongoing obligation to appropriately protect access to and use of Organization technology and information systems. This obligation applies to technology and information systems both in Organization business locations as well as off-premises technology, and information systems accessed remotely.

Etiquette
Users of Organization technology and information systems must treat communication via these systems as university communication. Care must be exercised to ensure that all communication is courteous and professional.

Users must keep in mind that all electronic information including e-mail exchanged over the Internet may be read by other persons. These communications may be used in court in connection with litigation.

Privacy and Monitoring
Users have no expectation of privacy regarding any electronic data stored on Organization information systems or regarding any activities conducted on-line with access or systems provided by Organization. By using Organization information systems and computer technology, each user consents that Organization or its designees may inspect, copy, or

disclose at any time and without further notice any electronic mail, electronic information, or any information contained on our systems.

Organization may monitor technology and information systems use as deemed necessary and may inform managers of potentially abusive behavior.

Reporting Information Security Weaknesses and Events
Users of Organization Information Systems must report information security weaknesses and events immediately after they are seen or experienced by email to head.it@gtu.edu.in.

Critical issues should be reported by phone to the IT Dept. If an employee suspects their computing environment may have been compromised they are not allowed to continue working without authorization then immediately inform to IT Dept.

Clean Desk
Organization employees must not leave any sensitive information in plain sight when away from their desks. Documents, media, and computing devices containing sensitive information must be stored in locked drawers/cabinets/rooms or otherwise secured.

Workstation Computing
Users assigned workstations and/or laptops must take reasonable steps to protect their computers from loss, theft or damage. Lost, stolen, and missing computers must be reported to IT Dept. immediately.

Users must be required to enter a password or use stronger authentication methods before accessing personal computing devices with University information.

Users must lock their workstations when unattended. An automatic screen saver or “lock” screen must turn on after 15 minutes of inactivity. A password or other authentication method must be required to regain access to the system.

Laptops and other mobile personal computers must have pre-deployment security hardening completed by IT including hard drive encryption installed and activated.

Users must not deactivate security software, change security settings or delete any logs without approval from IT Dept.

All the GTU users are required to follow the Certain security guidelines

Remote Access
Remote access to internal network systems must be authorized. Only Organization provided or approved equipment must be utilized to access Organization systems or store company information.
Users are required to enable/ use multi-factor authentication (MFA) in order to access University systems.

Copyrighted Materials
Computer programs, software code, textual materials, audio and video files, graphics and other forms of expression may be protected by copyright laws. Use of Organization equipment or software to copy or transmit any copyrighted material without the prior written authorization of the copyright owner is prohibited.

Unacceptable Use
Users must not use University technology and information systems in an unacceptable manner, unless explicitly authorized and as a part of their job function:
Examples include but are not limited to:

- Excessive time visiting non-work-related Internet sites
- Disrupting or intercepting Organization network computing environment or network communications
- Port scanning or security scanning Organization production infrastructure Executing network monitoring unless authorized.
- Circumventing user authentication or security of any host, network or account. Interfering with or denying service to any user.
- Providing employee information to external parties.
- Using Organization systems for improper or illegal receipt, transfer, possession, or storage of material
- Deliberately visiting Internet sites or sending/receiving email containing material that is obscene, pornographic, defamatory, illegal, or that violates any Organization policies
- Sending communications intended to harass, annoy, or intimidate another person Using any Organization technology or systems for personal gain
- Advocating for or against a political candidate, party, or organization Representing personal opinions as those of Organization
- Violating the license provisions of any software
- Harming or interrupting the operation of any system through deliberate actions or careless use, such as release of computer viruses
- Sending bulk unsolicited email (SPAM)
- Developing, maintaining, or hosting personal or otherwise unapproved websites Installing or using computer software on Organization-owned technology or
- information systems without prior manager permission
- Installing or using of non-approved network devices in Organization offices, such as wireless access points
- Providing unauthorized access to Organization systems or information
- Revealing account passwords or using another individual's user account or password Hiding or masking computer or Internet usage
- Accessing, changing or using another individual's files or output without explicit authority Installation and use of peer-to-peer file-sharing utilities.
- Installation and use of games, with the exception of default system-provided games.

Any employee found to have violated University Information Security policies may be subject to disciplinary action.

2.7 IT resource issuing policy for GTU staff members

Sr. No.	Name of Computing Resource/ Equipment/Accessory	Class 3	Class 1 & 2
1.	**Desktop Computer**	i5 or equivalent processor, 8GB RAM, 500GB HDD/SSD, Monitor 15'' to 20''	i7 or equivalent processor, 8GB RAM, 1TB HDD or 1TB SSD, Monitor 19'' to 24'' **For IT development/exam staff:** i9 or equivalent processor, 16GB RAM, 1TB HDD/SSD Monitor 19'' to 27''
2.	**Laptop**	---	i7 or equivalent processor, 8GB RAM, 1TB HDD/SSD **For IT development/exam staff:** i9 or equivalent processor, 16GB RAM, 1TB HDD/SSD
3.	**Only Monitor**	15'' to 20''	19'' to 27''
4.	**External Storage Device**	Up to 1TB HDD/SSD	Up to 4TB HDD/SSD
5.	**Printer**	LaserJet, Print only, Output Black & White only, USB connectivity, 12 ppm, A4 size paper print only, Manual duplex print	LaserJet, Print only, Output black & white only, Ethernet and USB connectivity, 14 ppm, A4 size paper print only, Manual duplex print
6.	**Multifunction Printer**	---	All-in-One (print, copy, scan), Auto-duplex printing, 50ppm, Auto document feeder, Ethernet, USB, Wireless Connectivity
7.	**Large Photocopy Machine**	**Allocated in Section/Department/ Centre/Cell/School managed by GTU** LaserJet, All in one (Copy, Print Scan), 21-30 ppm, Output Black & White only, Output capacity up to 500 sheets, Ethernet-USB-Wireless Connectivity, Touch screen with Graphics display, Scan to E-mail; Save-to-Network Folder; Saveto-USB drive, Maximum 5 paper trays, Magnification 25% to 400%.	

2.8 Policy of Usage of Credentials of remote servers, databases, computer systems, laptops, portals, email ids by GTU staff members

For maintaining ownership, trustworthiness, confidentiality and to avoid unauthorised access, the credentials policy covers following points:

The credentials of remote servers, databases, computer systems, laptops, portals, email ids assigned by GTU are to be kept with only those GTU staff members who are using it. The passwords must be changed frequently by user. In case, the credentials are given to other person (if required) then it will be sole responsibility of the owner of the credentials for any unethical practice. When any employees/staff leave the job he/she has to hand over the IT related details to IT section.

2.9 Laptop Allotment Policy

1. Laptop can be allotted to employees who have the grade pay greater than or equal to 5400 in 6th Pay Commission. Laptop is the substitute of Desktop so either Desktop or Laptop is given to the Staff member.
2. To decide the Laptop amount, deduct 33% depreciation using reducing method every year. Suppose GTU have purchased the laptop at the rate of Rs. 1 lakh. Then Subtract 33000 after first year (100000 -33000 = 67000). For the 2nd year again subtract (67000 – 22110 (33% of 67000) = 44890) and so on.
3. In case of Natural Calamities, laptop is lost then higher authorities will decide the final amount to pay by the staff member.
4. At the time of allotment of Laptop, staff is required to submit an undertaking that he / she is liable for any misuse of GTU confidential data or share the data with anyone.
5. Any employee wish to take the Laptop at the time of leave the job then it will be provide after the low level formatting.

2.10 Firewall Policy

In Firewall Policy, it is suggested to use the module captive policy for security purposes. IT Committee members has also recommended to put the signature message in all the important Gmail users email account for the security purpose.

Firewall policy is define in two categories with the following restrictions:

Category 1: For GTU Officer, Class – 1 & Class – 2

In Category 1, Gambling, Fashion and Beauty, Crime and Suicide, Drugs, Dating And Matrimonial, Alcohol and Tobacco, Advertisements, Adult Content, ns2realnameserver, Nudity, Swimwear and Lingerie, Porn etc. categories are blocked.

Category 2: For GTU Admin Asst., Contractual staff, Class – 3 and Class – 4, IT Maintenance staff

In Category 2, Shopping, Crime and Suicide, Cricket, Social Networking, Video Search, Games, Internet Radio TV, Internet Telephony, Fashion and Beauty, Alcohol and Tobacco, Nudity, Adult Content, Swimwear and Lingerie, Shares and Stock Market, Business and Economy, Finance, Gambling, Blogs, Jobs Search, Dating and Matrimonial, Chat, Sex Health and Education, Porn, Phishing and Fraud, P2P, Weapons, Hacking, Instant Messaging, Hate and Racism, Drugs, SPAM URL, Militancy and Extremist etc. categories are blocked.

2.11 Backup Policy of IT Dept

Servers/Services	Retention Period	Backup Location
University servers/ services	14 days	Replicated to the cloud
Test and development Servers / Services	14 days	Replicated to the cloud
University Databases	7 days	Replicated to the cloud in Simple Storage Service and physical server

Archiving

Upon expiration of a user account any data stored within the personal file store or mailbox will be archived and available offline for maximum of 1 year.

If a permanent archive is required, then the IT Section can transfer the data to DVD or similar media. However, authorization must be obtained from the Registrar of a School or Service Director of a Professional Services Unit. Once provided, the data will be the responsibility of the person making the request.

Local device storage

It is the responsibility of the data owner to ensure that any data temporarily stored on local PC hard disks is transferred to the network file store at the earliest opportunity.

Chapter 3 IT Related Guidelines

3.1 Guidelines on Computer Naming Conventions

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

2. All the computers should follow the standard naming convention.

3.2 Guidelines for hosting Web pages on the Internet/ Intranet

Mandatory:

1. Provide the full Internet e-mail address of the Web page maintainer.
2. Provide a link to the GTU 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 supporting local pages.
4. Maintain up to date pages. Proofread pages and test links before putting them on the Web, and regularly 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 the important web pages.

Recommended:

1. Provide information on timeliness (for example: Updated on 20-9-2020, 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" subdirectory. Remember that nothing is private on the Internet: unlinked 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).

3.3 Guidelines for Desktop Users

These guidelines are meant for all members of the GTU Network User Community and users of the University network.
Due to the increase in hacker activity on campus, University 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 Quick Heal or any other and should retain the setting that schedules regular updates of virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.
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. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks). When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.
7. 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.
8. In addition to the above suggestions, IT Section 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.

9. If a machine is compromised, IT Section 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.
10. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, IT Section technical personnel can scan the servers for vulnerabilities upon request.

3.4 Guidelines for condemnation & Disposal of IT Equipment

These guidelines will be applicable to all IT equipment installed in GTU campuses and include the following items:

- Servers
- PCs
- Dumb Terminals
- Printers
- UPS
- Laptop/Note-book/tablet
- Data Communication Equipment/LAN switches/routers/data cables.

Note:

i. Consumable items related to IT like used printer cartridges etc. are not included in the scope of scrapping on account of the fact of its nature as consumable.

ii. IT items like pen drives/CD/floppies, which are petty valued and are not capitalized, are not qualified for the detailed scrapping procedure.

Grounds for condemnation

The IT equipment can be condemned on following grounds:

1. Equipment outlived its prescribed life and certified by IT Dept. as unfit for its useful contribution. The prescribed life of various IT equipment is as following:

Device	Minimum Life
Desktop / PC / Dumb Terminals	5 years
Laptop	5 years
UPS excluding battery	5 years
Battery of UPS after warranty period	1 year
Printers	5 years
Data Communication equipment / switches / routers / data cables	5 years

2. Equipment which have become obsolete technology-wise and can't be upgraded and support from vendor either paid or unpaid does not exist and their use may result in security threat/ unauthorized access to data.

3. Beyond economical repair: When repair cost is considered too high (exceeding 50% of residual value of equipment taking depreciation into account), and the age of the equipment. Such cases should be deal on case to case basis and should have concurrence of finance. In case of IT equipment, a depreciation of 20% per year may be taken for calculation of residual value.
4. Equipment that has been damaged due to fire or any other unforeseen reason and have been certified as beyond repair by the authorized service agency and agreed upon by the IT Dept.

Disposal

Such equipment shall be disposed strictly following the procedure as laid down as per GFR 2017. Once the equipment has been condemned it should be removed from office use and kept in the area allocated for scrapped equipment. Department will also ensure removal of service and inventory labels from such equipment. If any Annual Maintenance Contract is running for such equipments/instruments should be stopped with the effective date of scrapping. All data including operating system must be removed after taking proper backup and preserved by user of the equipment.

Procedure

1. IT Dept. will be the nodal section for all the IT equipments procured. It will prepare and maintain assets' register for the same. However, individual section will also be provided with all the basic information.
2. Scrapping proposal will be initiated by the user section which will be compiled by IT Dept. for further processing for scrapping.
3. Each unit of department will prepare "IT equipment condemnation note" in the pro-forma attached as Annexure-1.
4. Department will constitute a condemnation committee which will review the condemnation notes and recommend about the condemnation of equipment as per approved guidelines. The committee should have at least one member from IT section and one from the finance wing.
5. All procedure and rules of the government on maintenance of records for condemnation of non-consumable items will be adhered to in these cases.

The condemnation report so prepared shall be put up for approval. The condemnation will be done only after approval is obtained from competent authority having such powers to approve condemnation. It is suggested that such Scraping Committee will meet twice in a year during the months of May-June and Nov. - Dec. in order to avoid piling up of unusable IT items.

Chapter 4 Responsibilities of Stakeholders

4.1 Responsibilities of IT Department

A. Campus Network Backbone Operations

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

B. Physical Demarcation of Campus Building's Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of IT Dept.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of IT Dept. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the IT Dept. 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 IT Dept.
3. IT Dept. will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. It is not the policy of the University 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 University's Internet links.

C. Network Expansion

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

D. Wireless Local Area Networks

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

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

G. Providing Net Access IDs and email Accounts

IT Dept. 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 university upon receiving the requests from the individuals on prescribed proforma.

H. Network Operation Center

IT Dept. 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 IT Dept. technical staff for problem resolution.

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

IT Dept. 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

IT Dept. may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call to IT Dept.

The designated person in IT Dept. receives complaints from the users and coordinates with the user / service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

IT Dept. will be responsible only for solving the network related problems or services related to the network.

L. Disconnect Authorization

IT Dept. will be constrained to disconnect any Section, department, or division from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Section, department, or division machine or network, IT Dept. endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, IT Dept. provides the conditions that must be met to be reconnected.

M. Maintenance of Computer Hardware & Peripherals

IT Dept. is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty and whose responsibility has officially been entrusted to this Cell.

N. Receiving Complaints

IT Dept. may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in IT Dept. receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

O. Scope of Service

IT Dept. will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company. IT committee has decided to empower the IT committee members to decide the brands to purchase all the IT related products.

P. Installation of Un-authorized Software

IT Dept. or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

Q. Reporting IT Policy Violation Incidents

If IT Dept. 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 IT Dept. and university authorities.

R. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the IT Dept. After taking necessary corrective action IT Dept. or service engineers should inform to user by email.

S. 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.

T. Coordination with IT Dept.

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning, IT Dept. /service engineer may coordinate staff to resolve the problem with joint effort. This task should not be left to the individual user.

4.2 Responsibilities of Department or Sections

A. User Account

Any Centre, department, or Section or other entity can connect to the University network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university. The user account will be provided by IT Dept., upon filling up the prescribed application form available in Annexure-2 and submitting it to IT Dept.

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

B. Logical Demarcation of Department/ Section/Division Networks

In some cases, Section, department or Division might have created an internal network with in 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 School, department or division side of the network backbone. The School, department, or division is also responsible for operating the networks on their side of the network backbone in a manner that does not negatively impact other network segments that are connected to the network backbone.

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

C. Supply of Information by Section, Department, or Division for Publishing on /updating the GTU Web Site

All Schools/Centers, Departments, or Divisions should provide updated information concerning them periodically. Hardcopy of such information duly signed by the competent authority at Section, Department, or Division level, along with a softcopy to be sent to IT Dept. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Section, Department, or Division. **It is also**

recommended that to update the IT policy as per the gap analysis report provided of ISO agency which is still under process.

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

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

1. This policy applies, in its entirety, to school, department, or division wireless local area networks/broadband connectivity within the academic complex. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with IT Section.
2. Obtaining Broadband connections and using the computers alternatively on the broadband and the university campus-wide network is direct violation of the university's IT Policy, as university. IT Policy does not allow broadband connections within the academic complex.
3. School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
4. As inter-building wireless networks are also governed by the University IT Policy, setting up of such wireless .networks should not be undertaken by the Schools/Centers without prior information to IT Section.

E. Security

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

F. 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 university are the property of the university and are maintained by IT Section.
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 IT Section 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.

G. Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the university network policy and with prior permission from the competent authority and information to IT Section.
University Network policy requires following procedures to be followed for any network expansions:

- All the internal network cabling should be as on date of CAT 6 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 for future expansion of network. Such management module should be web enabled. Using unmanaged switches is prohibited under university's IT policy. Managed switches give the facility of managing them through web so that IT Section 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 IT Section on request.

H. 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. Estate Dept. 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.

I. Campus Network Services Use Agreement

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

J. Enforcement

IT Section periodically scans the University 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.

4.3 Responsibilities of the Administrative Units

IT Section needs latest information from the different Administrative Units of the University for providing network and other IT facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the GTU web site up-to-date in respect of its contents.
The information that is required could be broadly of the following nature:

- Information about New Appointments/Promotions. Information about Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the university authorities that makes an individual eligible for using the university's network facilities.
- Information on Important Events/Developments/Achievements.

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

Chapter 5 Standard Operating Procedures

5.1 Standard operating procedures for Result Processing

Purpose

This describes the process for managing Result Processing System within the University. These projects include External, Internal, Mid and Viva Marks from the end customers.

Scope

This SOP is applied to Result Processing System.

Procedure

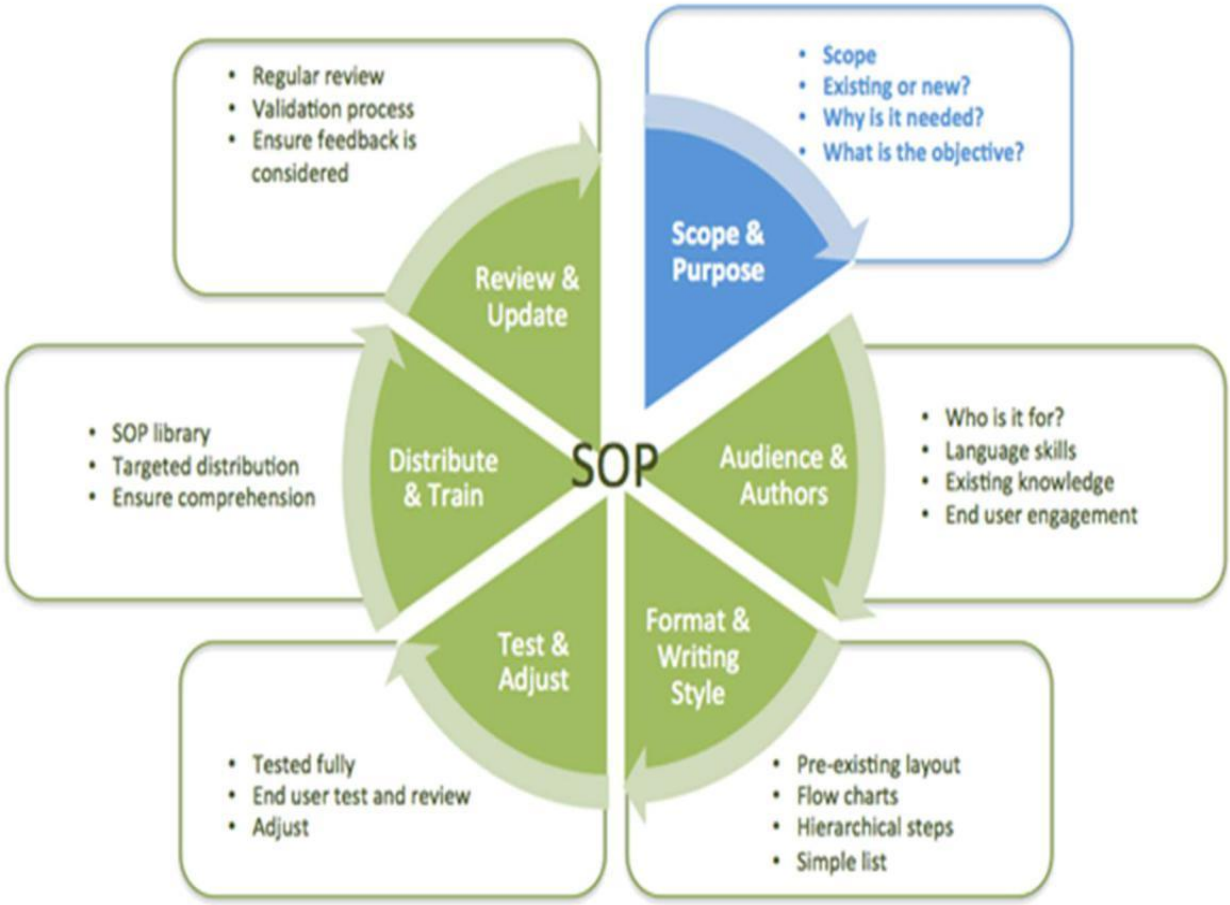
Suppose we are processing for the result of BE SEM – 8.

Steps	Process	Responsible Section
1	Collect the Mid and Internal Marks through Portal from Institute / College.	BE [Concern Section]
2	Collect the Viva Marks through Portal from Institute / College	BE [Concern Section]
3	Collect the E Marks through E – Assessment Agency	BE [Concern Section]
4	Park the History Marks from Programmer	BE + IT
5	Verify History Marks by Result Processing Team.	BE + IT
6	Park the Teaching Scheme of BE SEM – 8.	BE+ Academic
7	Verify Mid, Internal, Viva Marks by Result Processing Team and if anything is remaining then collect the marks using portal / by mail from Institute or flag it withheld. In verification, RPS team is required to verify the actual marks with max marks, min marks of teaching scheme.	BE + IT
8	After completion of above task, Start the Process of Result using Result Processing System (RPS).	BE + IT
9	If any error is generated or any data is missing during the process, create the document and solve the issues and start the process again from the beginning.	BE [Concern Section]
10	Generate the Result using RPS.	BE + IT
11	Verify Marks with Maximum Marks, Minimum Marks using teaching scheme. Check the Grade as per the marks. Check the SPI, CPI and CGPA. Check the No. of Backlogs. For remedial student, check No. of Backlog with grade history data (at least for 5 students).	BE [Concern Section]
12	Manually Generate the result of 20 different types of student records.	BE + IT
13	Compare the manual result with RPS result. If any data is mismatched then prepare the document and solve the issue and start the process again.	BE + IT
14	If Both the results are matched then send any 10 records with	IT

	History data, result data to Concerned Section, IT, OSD-EXAM and COE for verification by email.	
15	After receiving the email verification from all the authorities, generate the result statistics and 10 records printout for the signatures.	BE [Concern Section]
16	Once the signature process is completed, live the result on web.	IT

5.2 Standard operating procedures for software development

Project Plan



Purpose

This describes the process for managing software projects within the company from requirements development through to the delivery and maintenance of the project results. These projects include internal projects and projects are done for the end customers.

Scope

This SOP is to be applied to all software development projects.

Definitions/Abbreviations/Symbols

- Software Development – Activities that produce or enhance software and its documentation, including the testing and distribution of software that is developed.
- Project – A software development activity that occurs within a specific timeframe and produces specific, documented results.
- Project Manager – The individual who has been assigned primary responsibility for the management of the project.
- Customer – The person or entity for whom the project is performed.
- Deliverable – The project results to be delivered to the customer.
- Requirements – A list of expected results for the project, stated as the minimum functionality and performance that is acceptable.
- Task – A software development activity, intended to satisfy a portion of the requirements, which is assigned to a developer.
- Developer – A programmer who has been assigned a task for the project.
- Peer Developer – A programmer who has not been assigned a task, but is able to perform code review, testing, and other quality assurance functions.
- Issue Tracking System – A system for recording tasks and software bugs, and which allows the progress of these items to be tracked.
- Pivotal Tracker – The web-based issue tracking system.
- Codacy – The web-based code review system.

Procedure

Software requirements

Each project must have a software requirements document that describes the expected functionality, the interface, and any regulatory constraints for the software.

This document will be revised during project development by mutual agreement of the project manager and the customer, in consultation with the developers who are working on the project.

- The initial requirements document should be completed within one month of project initiation.
- Mandatory sections for the requirements document are as follows:
    - Scope
    - Purpose
    - Definitions and Abbreviations
    - Overview
    - Intended Users
    - Constraints (e.g. regulatory policies that must be adhered to)
    - Requirements Specification (each item is to be numbered)
    - Design Details
    - References
    - Appendices

- The customer must approve the requirements document by either signing the document itself or by signing a contract to which the document is appended (internal projects do not require a signature).
- All revisions to the requirements that occur after the initial signature must be done in accordance with contracts that are in force for the project and must be accompanied by signatures from both the project manager and the customer.

Design Documentation

- Elements of the design that are necessary in order to fulfill the software requirements, and cannot be changed without modifying the requirements, must be described within the requirements document itself.
- The documentation must describe, as a minimum:
    - How the major components of the software interact with each other
    - How end-user data will be modified by the software
- All design documents, including those that are not part of the requirements document, are to be filed with the requirements document.

Task management and issue tracking

The web-based application Pivotal Tracker is used to assign tasks to software developers, to keep track of ongoing software maintenance, and to record software bugs that have been discovered.

- The project manager will assign tasks to software developers through Pivotal Tracker, where each project task should:
    - State the project name, and refer to the requirements document.
    - Give the date when the task is to be completed.
- Developers may, where it improves their own ability to track their progress, add additional tasks to Pivotal Tracker that are sub-tasks of larger manager assigned tasks.
- All bugs reported by the customer are to be entered into Pivotal Tracker, including:
    - The date when the bug was reported.
    - The software version number in which the bug was discovered.
    - The severity of the bug.
- A weekly meeting must be held at which all active developers will report their progress on their tasks.
- The developer must notify the project manager when they mark a manager-assigned task as resolved within Pivotal Tracker.

Implementation and Unit Test

The developer is to implement the software and write unit tests that demonstrate that the software fulfils the requirements.

- The source code for each assigned development task should be accompanied by a sufficient number of unit tests to allow the developer to demonstrate that the requirements have been met.
- Unit tests should wherever possible, be able to run as a batch job without a user present.

  The purposes of a unit test are to:
    - Ensure that data is processed as per the requirement specification.

    - Ensure that the software is stable, i.e. does not freeze or crash when presented with a range of inputs.
- Allow continuous retesting of existing features as new features are added.
- The source code for unit tests is to be stored with the project source code itself, in a subdirectory called “Testing”.

Code review

Code review is a quality assurance practice whereby one developer reads another developer’s source code.

- Upon completion of a task, the tasked developer must request a code review via the Codacy web interface.
- This request should be made to a peer developer, or to the manager.
- If the manager is assigned a code review, then the manager may:
    - Perform the code review.
    - Re-assign the code review to a peer developer.

Internal release and user testing

The purpose of an internal release is to make the software available for testing.
The manager makes the decision for an internal release to be produced.

- The developer compiles the software to create an application, and stores it in a location that can be accessed by others.
- The project manager and the developer create a testing document together, which describes the software functions to be tested.
- One or more people are given the testing document and the software application, perform the activities stated in the testing document, and record the results.
- Depending on the results, new bugs may be added to Pivotal Tracker, and developer tasks previously marked as complete may be marked as incomplete.

Internal project auditing

Internal project auditing ensures that appropriate quality control measures have been applied to the software prior to delivery.

- The project manager must verify that:
    - The software meets all of the requirements stated in the requirements document.
    - No constraints stated in the requirements document have been violated.
    - All project tasks have been completed.
    - Sufficient testing has been performed.
- If any unmet requirements cannot be satisfied prior to the project deadline, the project manager must immediately communicate this fact to the customer and request either a modification to the project timeline or modification to the requirements.

Delivery of results

Delivery of the results may occur several times during a project, depending on whether delivery milestones are specified for the project, or whether the customer is to participate

in the ongoing evaluation of the project results. The following steps must be followed whenever a delivery occurs:

- The project manager assigns a version number to the software prior to delivery.
- The project manager, or a developer to whom the project manager has assigned this duty, creates a deliverable package that contains the project results.
- A copy of the deliverable package is stored at the Cain Core office for a period of not less than five years.
- The project manager delivers the package to the customer.
- The customer will perform acceptance testing on the software to ensure that it meets the requirements, and will communicate any concerns to the project manager.
- The project manager will decide if additional deliveries or contractual amendments are necessary in order to address the concerns of the customer.

Software Maintenance

Software maintainability refers to the ability to modify the software after delivery to the customer.

- Software maintenance activities include:
    - Ongoing testing of the software after delivery.
    - Fixing bugs that have been found in the software.
    - Deploying the software on new platforms.
    - Re-using portions of the software in new projects.
    - Storage of the software and its documentation.
- The project manager retains responsibility for maintaining the project for six months following delivery or longer if stipulated by the contract with the customer.
- Following this six-month period, project maintenance becomes a shared responsibility of all qualified project managers.
- Software is to be maintained for a minimum of 1 year, meaning that it must be possible to modify and re-deliver the project results within this period.

Responsibilities

Project Manager / Project Coordinator

- The initial draft of the requirements document.
- Iterate drafts of requirements document with Customer.
- Approval of requirements document.
- Task assignment.
- Reassignment of tasks with insufficient progress.
- Schedule meetings.
- Internal audit prior to delivery.
- Delivery.

Customer

- Iterate drafts of requirements document with Project Manager
- Approval of requirements document.
- Acceptance testing of delivered results.

Developer

- Implementation and code testing. Code documentation.

- Reporting progress to Project Manager.
- Assigning code reviews to Peer Developers.
- Internal releases of software.

Peer Developers

- Code reviews, when assigned.
- User-level testing of software.

Annexure-1

Performa for Preparation of Information for Scrapping of IT Equipment

(To be filled by user)

Name of user: _____

Designation: _____ Section: _____

Room No: _____ Tel No: _____-

Sr. No.	Item	Make & Model	Sr. No. of Item	Reason for Scrapping

User (Recommendation of IT Head)

Part-B

(To be filled by Procurement Section)

Sr. No.	Name of the Item with Sr. No.	Date of purchase as per record	Purchase cost as per record	Asset/Stock reg. entry page no.

(Signature of Store & Purchase Head)

Part-C

(To be filled by Scraping/Condemnation Section)

Sr. No.	Name of the Item	Reason for scrapping	Residual Value	Any other information/remarks

(Signature of Scrapping in-charge)

Annexure-2

GUJARAT TECHNOLOGICAL UNIVERSITY

IT SECTION

Application for Email id, Internet Access ID, IP Address Allocation

Sr. No.	Details to be filled	
1	Name of the Applicant Prof./Dr./Mr./Ms.	
2	Location of the System Section / Department	
3	Contact number	
4	Designation	
5	Identification Name of the System (Host Name)	
6	IO Box Number	
7	Make of the system ACER / Compaq / HCL / IBM / HP / Dell / If Other, Specify	
8	MAC / Physical / Adapter address	
9	Operating System	
10	Whether connected directly to the LAN or through another hub / switch	
11	Please specify the E-mail Account Name you wish to have	**_____@gtu.edu.in**

Date:

Signature of the Applicant