IT Policy

VIT-AP University, Amaravati
December 2021

Table of Contents

VIT-AP IT Policy

(Release: October 2021 Version 1.0)

Centre for Technical Support (CTS) maintains the policies governing the use of VIT-AP computing and IT communication resources. The IT Policy process also includes an annual review of existing policies anda selection of those policies to be audited for verification of compliance within the VIT-AP.

Every member of the VIT-AP community is bound by these policies and is expected to be thoroughly familiar with them. Violators will be subject to the full range of disciplinary sanctions, up to and including expulsion or termination.

In order to retain necessary flexibility in the administration of policies, the VIT-AP reserves the right to interpret, revise, or delete any of the provisions of these policies as the VIT-AP deems appropriate in its discretion.

Need for IT Policy

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 VIT-AP community to understand how institution policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

- Acceptable Use Policy
- Hardware and Software Procurement Policy
- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- VIT-AP 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 VIT-AP IT Policy applies to technology administered by the institution centrally or bythe individual departments, to information services provided by the VIT-AP administration, or by the individual departments, or by individuals of the VIT-AP community, or by authorized resident or non- resident visitors on their own hardware connected to the institution network.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the Institution, hostels and guest houses, or residences wherever the network facility was provided by the Institution. Computers owned by theindividuals, 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 VIT-AP IT policy.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the VIT-AP IT Infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by VIT-AP by any institution member may even result in disciplinary action against the offender by the institution 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

Acceptable Use Policy

An Acceptable Use Policy is a set of rules applied by the owner, creator or administrator, Schools, Centers, Departments, internet service providers, and website owners, often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

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

Employee Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by VIT-AP imposes certain responsibilitiesand obligations and is granted subject to institution policies. Acceptable use must be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment.

Policy Statement

1. Sharing of passwords, PINs, tokens or other authentication information is strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).
2. The use of VIT-AP resources to access, further or otherwise participate in activities which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activities, sexually explicit material, hate speech, violent behavior & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with VIT-AP mission.
3. In addition to standard electronic resources, members of the Institution community are expected to make appropriate use of the Institution Telephone system. Examples of inappropriate actions:
   a. Unauthorized use of another individual's identification and authorization code
   b. Use of the Institution telephone system to send abusive, harassing, or obscene messages
4. The use of VIT-AP resources to conduct business for personal financial gain is prohibited.
5. Anti-virus and anti-malware software must be installed on your computer, kept up to date and currently enabled. If your software is not up to date or disabled, it may lead to an infectionwhich may result in your network access being disabled.
6. Although CTS deploys Windows patches for Institution issued devices, employees are responsible for keeping their computer updated with all other security patches/fixes from theappropriate software update services. This includes updating applications, such as MS Office,Adobe, iTunes, Firefox, Chrome, etc. This also includes operating system patches for non- institution devices. If your computer is not up to date, it could lead to malware infection whichmay result in your network access being disabled.
7. Employees are responsible for their computer, including its hardware, software, and any network traffic transmitted by it. Please contact Centre for Technical Support (CTS) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.
8. The use of personal routers (wireless or wired) and/or DHCP servers outside of a contained lab environment is strictly prohibited. CTS will assist you if you require additional connectivity

9. Using the institution network to provide any service that is visible off campus without prior CTS approval, is prohibited. This applies to services such as, but not limited to, HTTP (Web), SSH, FTP, IRC, email, private VPN, etc.
10. Configuring your computer to provide Internet or VIT-AP network system access to anyone who is not a VIT-AP faculty, staff member or student is prohibited.
11. Connecting any device or system to the institution data networks without the prior review and approval of CTS is prohibited.

Student Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by VIT-AP imposes certain responsibilitiesand obligations and is granted subject to institution policies. Acceptable use must be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment.

Policy Statement

1. Sharing of passwords, PINs, tokens or other authentication information are strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).
2. The use of VIT-AP resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behavior & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with VIT-AP mission.
3. The use of VIT-AP information systems for commercial gain is prohibited.
4. Anti-virus and anti-malware software must be installed on your computer, kept up to date and currently enabled. If your software is not up to date or disabled, it may lead to an infectionwhich may result in your network access being disabled.
5. Students are responsible for keeping their computer updated with security patches/fixes from the appropriate software update services (Windows Update on windows computers, Software Update on Apple computers). This includes updating applications, such as MS Office, Adobe, iTunes, or Firefox. If your computer is not up to date it may lead to virus infection which mayresult in your network access being disabled.
6. Students are fully responsible for their computer, including its hardware, software, and any network traffic transmitted by it, regardless if this traffic was authorized by you or not. Pleasecontact Centre for Technical Support (CTS) if you have any questions about whether or not certain software/hardware might conflict with this acceptable use policy.
7. The use of personal routers (wireless or wired) and/or DHCP servers is strictly prohibited.
8. Using the institution network to provide any service that is visible off campus is

prohibited. This applies to services such as, but not limited to, HTTP (Web), FTP, IRC, peer-to-peer (p2p) multimedia sharing, game servers and email.

9. Configuring your computer to provide Internet or VIT-AP network system access to anyone who is not an authorized VIT-AP faculty, staff member or student is prohibited.
10. Connecting standard mobile devices used for the pursuit of academic work to VIT-AP wireless network is permitted. Connecting any other device or system to the institution data networkswithout the prior review and approval of CTS is prohibited.
11. Some examples of policy violations:
    a. Accessing another user's personal private data
    b. Consuming a disproportionate amount of bandwidth
    c. Attempting or coordinating a denial-of-service attack
    d. Probing and/or exploiting security holes in other systems either on or off campus
    e. Using unauthorized IP addresses
    f. Using a network protocol analyzer or similar mechanism without prior authorization
    g. Degrading or restricting network access for others, either on or off campus
    h. Connecting to Institution systems that one has not been expressly permitted to access
    i. Downloading, sharing or using copyrighted material including music, movies, software ortext books
    j. Participating in activities which are not consistent with the Mission of the institution

In addition, your network access may be disabled if VIT-AP receives complaints about or otherwisedetects inappropriate behavior.

Vendor Acceptable Use Policy

Policy Statement

1. Vendor agrees to develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, security, integrity and availability of all maintained or transmitted VIT-AP data.
2. Vendor agrees to only use VIT-AP data, systems, resources, integrations, and access solely for theoriginal purpose for which it was intended as stipulated in any contract which exists betweenVendor and VIT-AP.
3. Vendor will not mine VIT-AP data for any purpose whether internal or external to Vendor Company.
4. Vendor will not share VIT-AP data with any third party, without express permission of the Institution in writing.
5. Vendor agrees to use VIT-AP data, systems, resources, integrations and access in a manner whichis consistent with the Mission of the institution.
6. Vendor agrees to comply with all local laws as they apply to VIT-AP systems and data.
7. Vendor agrees to be knowable about and comply with all other VIT-AP policies.
8. The use of VIT-AP resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behavior & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with VIT-AP mission.

Network Security Policy

Purpose

This policy is intended to protect the integrity of the campus network, to mitigate the risks and lossesassociated with security threats to computing resources and to ensure secure and reliable network access and performance for the Institution community. This policy is necessary to provide a reliable campus network to conduct and prevent unauthorized access to institutional, research or personal data. In addition, the Institution has a legal responsibility to secure its computers and networks frommisuse.

Addressing and Domain Services

1. Centre for Technical Support (CTS) is solely responsible for managing any and all Internet domain names related to VIT-AP (e.g. vitap.ac.in). Individuals, academic Schools/Departments or administrative departments may not create nor support additional Internet domains withoutprior approval from CTS.
2. To ensure the stability of network communications, CTS will solely provision and manage boththe public and private IP address spaces in use by the Institution.
3. CTS may delegate administrative responsibilities to individuals for certain network ranges, butretains the right of ownership for those networks.

Network Connections

1. VIT-AP faculty, staff or students may not connect, nor contract with an outside vendor to connect,any device or system to the Institution networks without the prior review and approval of CTS.Schools, Centers and Departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the Institution must obtain prior approval from CTS.
2. In order to maintain reliable network connectivity, no other department may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus without prior review and approval of CTS.
3. Users are permitted to attach devices to the network provided that they are:
    - for use with normal Institution or student operations
    - do not interfere with other devices on the network
    - are in compliance with all other VIT-AP policies.
4. Unauthorized access to Institution networking equipment (firewalls, routers, switches, etc.)is prohibited. This includes port scanning or connection attempts using applications such asSSH/SNMP, or otherwise attempting to interact with Institution network equipment.
5. Unauthorized access to Institution equipment/cabling rooms is also prohibited.

Wireless

1. Centre for Technical Support (CTS) is solely responsible for providing wireless networking services on campus. No other department may deploy wireless routers, bridges, and/or DHCP(Dynamic Host Configuration Protocol) services on campus.
2. CTS is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.
3. The Institution will maintain a campus wireless network based only on IEEE 802.11 standards.CTS will collaborate with academic departments where devices used for specific educational or research applications may require specific support or solutions.
4. CTS will provide a general method for network authentication to Institution systems. The IEEE802.1x standard is the currently supported authentication method. Additional security protocols may be applied as needed.
5. All users of wireless network resources at VIT-AP are subject to the applicable Network Acceptable Use Policy. Users of wireless resources at VIT-AP agree to have read and be bound bythe terms and conditions set forth in that policy.

External Traffic, Services and Requests

1. CTS will take action to prevent spoofing of internal network addresses from the Internet. CTSwill also take action to protect external Internet sites from source address forgery from devices on the Institution network.
2. The Institution external Internet firewall default practice is to deny all external Internet trafficto the Institution network unless explicitly permitted. To facilitate this, academic Schools, Centers and Departments and other administrative departments must register systems with CTS which require access from the Internet. Users that would

like to request access through the Institution firewall must open a help desk ticket and complete a firewall access request form.

3. Access and service restrictions may be enforced by Device, IP address, Port number or Application behavior.
4. CTS reserves the right to decrypt SSL traffic which transits the Institution network.

Network Security

1. CTS may investigate any unauthorized access of computer networks, systems or devices. CTS will work with academic or administrative departments and law enforcement when appropriate.
2. All devices connecting to the network must have adequate security installed/maintained andmust be configured and maintained in such a manner as to prohibit unauthorized access or misuse.
3. If a security issue is observed, it is the responsibility of all VIT-AP users to report the issue to the appropriate supervisor or CTS for investigation.
4. CTS reserves the right to quarantine or disconnect any system or device from the Institution network at any time.
5. Network usage judged appropriate by the Institution is permitted. Some activities deemed inappropriate include, but are not limited to:

Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCPor DNS servers; or a computer set up to act like such a device.

a. Engaging in network packet sniffing or snooping.
b. Setting up a system to appear like another authorized system on the network (Trojan).
c. Other unauthorized or prohibited use under this or any other Institution policy.
    i. Students may consult the Student Acceptable Use Policy for further information.
    ii. Employees may consult the Employee Acceptable Use Policy for further information.

Enforcement

1. Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the Institution network. CTS may subsequently require specific security improvements where potential security problems are identified before the device may be reconnected.
2. Attempting to circumvent security or administrative access controls for information resourcesis a violation of this policy. Assisting someone else or requesting someone else to circumventsecurity or administrative access controls is a violation of this policy.
3. The Institution reserves the right to test and monitor security, and to copy or examine files and information resident on institution systems related to any alleged security incident or policy violation.

Monitoring and Auditing

1. CTS will maintain and monitor traffic logs for all network devices and systems for security auditing purposes.

2. CTS reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a Institution policy violation, criminal activity, monitoring required by law enforcement or with appropriate management request. Reasonable cause may be provided by the complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of CTS staff.
3. CTS may perform penetration testing of any Institution owned devices or systems on its networks in order to determine the risks associated with protecting Institution information assets. CTS may further perform non-intrusive security audits of any system or device attached to the Institution's networks in order to determine what risks that system may poseto overall information security.

Email Use Policy

Summary

This policy covers appropriate use of any email sent from VIT-AP email address and applied to all Employees, Students and Alumni.

Guidelines

1. VIT-AP email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, religion, or national origin. Employees who receive any emails with this content from any VIT-AP employee should report the matter to the Vice chancellor – VIT-AP immediately.
2. All email sent or received from a VIT-AP G-Suite server must comply with the Acceptable Use Policy.
3. Violations of this policy will be handled in accordance with VIT-AP policies and procedures.

Employees

1. In an effort to increase the efficient distribution of critical information to all faculty, staff andstudents, and the Institution's administrators, it is recommended to utilize the VIT-AP e-mail services, for all formal VIT-AP communication and for academic & other official purposes.
2. Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institution communications are official notices from the Institution to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institution messages, officialannouncements, etc.
3. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://gmail.comwith their User ID and password. On joining every employee gets an official VIT-AP e-mail ID from HR department. The e-mail ID's are created by the Email Team of VIT-AP after the communication from HR department.

Students

Students are given VIT-AP mail ID under the domain **vitap.ac.in** and **vitapstudent.ac.in** hosted in G-Suite. Students will be able to use all the features offered by google.

Alumni

All the alumni are given with a lifetime mail ID to interact with their classmates or college mates or with VIT-AP. Once the student becomes alumni, the mail id will be moved from the vitap.ac.in and vitapstudent.ac.in to vitapalum.ac.in without losing any mails. A prior notification will be sent to student well in advance before the migration.

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 extentfor personal purposes.

   VIT-AP has Google Workspace for Education Fundamentals. Hence, the pooled storage shared among all users in the organization is 100 TB.

2. All features of Google workspace like enable seamless collaboration, boost productivity, communicate flexibly, organize your tasks, and provide trusted security (by the ADMIN) are applicable to all users.
3. Using the facility for illegal/commercial purposes is a direct violation of the VIT-AP 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.
4. While sending large attachments to others, user should make sure that the recipient has emailfacility that allows him to receive such large attachments.
5. 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.
6. 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 damage the valuable information on your computer.
7. Users should configure messaging software (Outlook 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.
8. 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.
9. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

10. While using the computers that are shared by other users as well, any email account that wasaccidentally 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.
11. Impersonating email account of others will be taken as a serious offence under the VIT-AP IT security policy.
12. It is ultimately each individual's responsibility to keep their e-mail account free from violationsof institution's email usage policy.
13. Any spam mail received by the user into INBOX should not be forwarded to anyone and couldbe deleted.

Hardware and Software Procurement Policy

Policy

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

IT Hardware Installation Policy

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

Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

What are End User Computer Systems

Apart from the client PCs used by the users, the institution will consider servers not directly administered by CTS, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting asservers which provide services to other users on the Intranet/Internet though registered with the CTS, are still considered under this policy as "end- users" computers.

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract either with a third party or with support from CTS. Such maintenance should include OS re-installation and checking virus related problems also.

Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is requiredfor battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

Network Cable Connection

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

File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with passwordand also with read only access rule.

Shifting Computer from One Location to another

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

Maintenance of Computer Systems provided by the Institution

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

Noncompliance

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

CTS/Institution Administration Interface

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

Software Installation and Licensing Policy

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

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

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all Micro Soft Windows computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.
2. Institution as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.
3. Any MS Windows OS based computer that is connected to the network gets OS patch free updates from the central server located in the Data Centre. Such updating should be done atleast once in a week. Even if the systems are configured for automatic updates, it is user’s responsibility to make sure that the updates are being done properly.

B. Antivirus Software and its updating

1. Computer systems used in the institution should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
2. Individual users should make sure that respective computer systems have current virusprotection software installed and maintained.

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

C. Backups of Data

1. Individual users should perform regular backups of their VIT-AP all data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyedfiles may be impossible.
2. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume getscorrupted. In such an event formatting only one volume, will protect the data loss. However,it is not a fool proof solution. Apart from this, users should keep their valuable data either onDVD, Flash Drive or other storage devices.

Web Site Hosting Policy

Policy

1. VIT-AP has an official website www.vitap.ac.in for the public access. Schools, Centers and Departments of Teachers / Employees / Students may have pages on VIT-AP's official Web page. Official Web pages must conform to the Institution Web Site Creation Guidelines for Website hosting. As on date, the Web Team at CTS is responsible for maintaining the official website of the institution viz., http://www.vitap.ac.in only.
2. Any department or an individual requires to publish any official content in the institution official website may sent the content to asstdir.website@vitap.ac.in committee responsible for approving the content, with a copy to the reporting authority. CTS web team will facilitate in creating and updating the content in the website.
3. For the quick delivery of the content to the end users, VIT-AP is engaged with Akamai TechnologyPvt. Ltd, to cache the web page content to various part of the world by using their CDN Technology.

Database Use Policy

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

VIT-AP has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the institution's approach to both theaccess and use of this institution resource.

A. **Database Ownership**: VIT-AP is the data owner of all the Institution's institutional datagenerated in the institution.

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

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

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

1. The institution's data policies do not allow the distribution of data that is identifiable to aperson outside the institution.
2. Data from the Institution's Database including data collected by departments or individualfaculty and staff, is for internal institution purposes only.
3. One's role and function define the data resources that will be needed to carry out one's officialresponsibilities/rights. Through its data access policies, the institution makes information anddata available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the Institution Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Officeof the Institution and departments should never respond to requests, even with a subpoena.All requests from law enforcement agencies are to be forwarded to the Office of the Institution Registrar for response Tampering of the database by the department or individualuser 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 motiveseven by authorized individuals/departments.
- Causing database or hardware or system software crash thereby destroying the whole of orpart of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.

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

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

IT Policy for Data Centre

The Data Center is VIT-AP all important to the ongoing operations of the VIT-AP. The following policies andprocedures are necessary to ensure the security and reliability of systems residing in the Data Center.

Access to VIT-AP Data Centre

In order to ensure the systems housed within the data center are kept secure, the following policiesapply to all personnel requiring access:

1. All personnel who access the Data Center must have proper authorization. Individuals withoutproper authorization will be considered a visitor.
2. Visitors to the Data Center must adhere to the visitors' guidelines.
3. Authorizations will be verified on a quarterly basis.
4. All personnel must wear a valid Institution ID or Visitor's ID card at all times.
5. Authorized staff will have access to the Data Center at any time.
6. Systems housed within the Data Center that contain data classified as Level III or above willbe monitored by Data Center employees through live video cameras.

Policy

1. All servers exempt by item one above will be housed in the VIT-AP Data Center unless there is aexception.
2. All equipment in the VIT-AP Data Center will utilize shared services (Backup, Restore, SAN, FiberChannel, and Network) to the fullest extent possible unless there is a exception.
3. Any new infrastructure resources incorporated into the VIT-AP Data Center environment will become a shared resource, available to all, unless there is a exception.

Procedures

Access Authorization

Institution staff members must be pre-approved for unescorted access within the Data Centre. Vendor access must be sponsored by an authorized staff member, or a dean, director, or department heads.

Authorizations will only be approved for individuals who are responsible for installation and/or maintenance of equipment housed in the Data Centre. Approval processes are as follows:

1. Authorization email must be sent by the dean, director, or department heads of the person requesting access.
2. Head CTS or Deputy director CTS, Systems will review and approve.
3. Authorized staff/vendors will be allowed entrance into the Data Center by a Data Center employee but will then have unescorted access within the Data Center.
4. Authorized staff/vendors are responsible for logging in/out when entering/exiting the Data Center.

5. Anyone who is not a Data Center employee, an authorized staff member, or authorized vendoris considered a visitor. Visitors must be accompanied by either a Data Center employee or other authorized staff member at all times while in the Data Center. Exceptions to this policymust have the approval of the Head CTS or Deputy director CTS, Systems.

Responsibilities of Centre for Technical Support (CTS)

A. Campus Network Backbone Operations

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

B. Physical Demarcation of Campus Buildings Network

1. Physical connectivity campus buildings already connected to the campus network backboneis the responsibility of CTS.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility ofCTS. It essentially means exactly at which location the fiber optic based backbone terminatesin the buildings will be decided by the CTS. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of CTS.
3. It is not the policy of the Institution to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the Institution’s Internet links.

C. Network Expansion

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

D. Wireless Local Area Networks

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

E. Global Naming & IP Addressing

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

F. Providing Net Access

By default, all the faculty members are given internet access in their official laptops. However, in case the official laptops are not given to the faculty, net access is given to their personal laptops only after installing Institution AV agent in their laptop.

Research scholars can request internet access by sending an e-mail to headcts@vitap.ac.in or deputydiretorcts@vitap.ac.in markinga copy of the e-mail to their guide. Internet is enabled only if the Institution AV installed. CTS is authorized to remove internet access at any point in time in case if the scholar is found to be misusing the facility given. Misusing means, removal of AV installed by the Institution, abnormaldownload using web crawlers or by proxy tools or any such unethical activity.

G. Network Operation Center

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

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

H. Network Policy and Technology Standards Implementation

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

I. Receiving Complaints

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

J. Scope of Service

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

K. Disconnect Authorization

CTS 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, CTS 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, CTS provides the conditions that must be met to be reconnected.

Responsibilities of Department or Sections

A. User Account

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

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

As a member of VIT-AP Institution community, when using the institution network facilities and its user account, it becomes user’s duty to respect the Institution’s reputation in all his/her electronic dealings within as well as outside the Institution. It is the duty of the user to know the IT policy of the institution and follow the guidelines to make proper use of the institution’s technology and information resources.

B. Logical Demarcation of Department/ Section/Division Networks

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

C. Supply of Information by Section, Department, or Division for Publishing on / updating the VIT-AP Website

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

D. Security

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

E. Preservation of Network Equipment and Accessories

- Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the institution are the property of the institution and are maintained by CTS.
- Tampering of these items by the department or individual user comes under violationof 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 levelor switch level.
- Taking away the UPS or batteries from the switch room.
- Disturbing the existing network infrastructure as a part of renovation of the location CTS will not take any responsibility of getting them rectified and such tampering mayresult in disconnection of the network to that segment or the individual, until the compliance is met.

F. Additions to the Existing Network

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

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

- All the internal network cabling should be as on date of CAT6 UTP.
- UTP cabling should follow structured cabling standards. No loose and dangling UTP cables bedrawn to connect to the network.
- UTP cables should be properly terminated at both ends following the structured cablingstandards.
- Only managed switches should be used. Such management module should be web enabled. Using unmanaged switches is prohibited under institution's IT policy. Managed switches givethe facility of managing them through web so that CTS can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer systemis not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

- As managed switches require IP address allocation, the same can be obtained from CTS on request.

G. Structured Cabling as a part of New Buildings

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

H. Campus Network Services Use Policy

The "Campus Network Services Use Policy" should be read by all members of the institution who seek network access through the institution campus network backbone. All provisions of this policy are considered to be a part of the Agreement. Any Section, Department or Division or individual who is using the campus network facility, is considered to be accepting the institution IT policy. It is user's responsibility to be aware of the Institution IT policy. Ignorance of existence of institution IT policy is not anexcuse for any user's infractions.

I. Enforcement

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

Responsibilities of the Administrative Units

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

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

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

Information related to items nos. A through E should reach Head CTS or Deputy director CTS. Director and Information related items nos.

Guidelines on Computer Naming Conventions

1. In order to troubleshoot network problems and provide timely service, it is VIT-AP all to be able toquickly identify computers that are on the campus network. All computer names on the campus network must use the Institution standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of CTS.
2. All the computers should follow the standard naming convention

Guidelines for running Application or Information Servers

Running Application or Information Servers

1. Section/Departments may run an application or information server.
2. Individual faculty, staff or students on the VIT-AP campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the VIT-AP network.

Responsibilities for Those Running Application or Information Servers

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

1. Obtain an IP address from CTS to be used on the server
2. Get the hostname of the server entered in the DNS server for IP Address resolution. Institution IT Policy's naming convention should be followed while giving the hostnames.
3. Make sure that only the services that are essential for running the server for the purpose it isintended for should be enabled on the server.
4. Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall,anti-spam etc.
5. Operating System and the other security software should be periodically updated.
6. Sections/Departments may run an application or information server provided they do the following:
    - Provide their own computer, software and support staff
    - Provide prior information in writing to CTS on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization webserver, contact the CTS.

Guidelines for Desktop Users

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

The following recommendations include:

1. All desktop computers should have the latest version of antivirus such as K7 Anti-Virus (PC) 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. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
4. 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 toothers.
   - 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
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 XP 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. 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 oldhard disk gets into the newly formatted and installed hard disk.

10. 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).
11. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
12. 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.
13. In addition to the above suggestions, CTS recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise.
14. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by theloss of a machine.
15. If a machine is compromised, CTS will shut the port off. This will isolate the computer, until itis repaired as per the guidelines. At that time, the port will be turned back on.
16. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, CTS technical personnel can scan theservers for vulnerabilities upon request.

Video Surveillance Policy

A. The system

1. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.
2. Cameras will be located at strategic points on the campus, principally at the entrance and exitpoint of sites and buildings. No camera will be hidden from view and all will be prevented fromfocusing on the frontages or rear areas of private accommodation.
3. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
4. Although every effort has been made to ensure maximum effectiveness of the system it is notpossible to guarantee that the system will detect every incident taking place within the area of coverage.

B. Purpose of the system

The system has been installed by institution with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposeswill be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation tocrime and public order

- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or otheraction is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employeecompliance with contracts of employment

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

C. The Security Control Room

1. Images captured by the system will be monitored and recorded in the Security Control Room, "the control room". Monitors are not visible from outside the control room.
2. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, policeofficers and any other person with statutory powers of entry.
3. Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be grantedto persons with a legitimate reason to enter the Control Room.

D. Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handlingCCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staffare fully briefed and trained in respect of the functions, operational and administrative, arisingfrom the use of CCTV/IP Camera.

E. Recording

1. Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.
2. Images will normally be retained for 20 to 30 days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reachedthe end of its use it will be erased prior to disposal and the Log will be updated accordingly.
3. All hard drives and recorders shall remain the property of institution until disposal and destruction.

F. Access to images

1. Access to images will be restricted to those staff need to have access in accordance with thepurposes of the system.
2. Access to images by third parties

3. Disclosure of recorded material will only be made to third parties in strict accordance withthe purposes of the system and is limited to the following authorities:
    - Law enforcement agencies where images recorded would assist in a criminal enquiryand/or the prevention of terrorism and disorder
    - Prosecution agencies
    - Relevant legal representatives
    - The media where the assistance of the general public is required in the identificationof a victim of crime or the identification of a perpetrator of a crime
    - People whose images have been recorded and retained unless disclosure to theindividual would prejudice criminal enquiries or criminal proceedings.
    - Emergency services in connection with the investigation of an accident.

G. Complaints

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

Digital Signage Policy

This policy was created to outline the guidelines for use of the digital signage located in VIT-AP Campus.

Policy

Digital signage managed by Centre for Technical Support (CTS) as a visual communication medium to inform students, faculty, staff, and visitors about the Institution, Specific Departments, VIT-AP sponsoredEvents, Sports and, etc.

Information displayed includes (but is not limited to): Programs, Meetings and Activity; Campus News; Important Current Events; Campus Facts and Emergency Messages. Content displayed on screens is governed by the Institution policy on acceptable use of electronic information resources and according to privacy guidelines that are developed for the VIT-AP Institution.

Equipment – Installation

- Schools, departments and Centre's are responsible for the funding of equipment, licenses andinstallation costs. Department's digital signage requests must include their Dean's or Vice Chancellor approval for digital signage location and funding.
- Equipment purchases must be coordinated and approved through CTS in order to maintain consistent technological and installation requirements.
- CTS will purchase equipment, licenses and coordinate installation of hardware and software.
- CTS will maintain server and server software.

- Equipment must be installed by VIT-AP Estates Team. Additionally, VIT-AP Estates Team will approvedigital signage locations within buildings to comply with fire code, historical building and structural standards.
- Equipment that is presently in use can remain in place until updates are required so long as the system is compatible and can incorporate displayed content and was installed in a mannerthat complies with all applicable building codes.

Content Guidelines & Screen Design / Layout:

- CTS will develop standardized template for all campus monitors. User readability will be maintained between buildings and monitors.
- Do not use signs to promote commercial activity or advertisements from non-institution organizations.
- Messages that in VIT-AP e public participation in programs must include the VIT-AP accessibilitystatement.
- Messages should not use copyrighted images or content without permission or license.
- Messages should include the VIT-AP official logo.
- No corporate logos can be used on any digital signage except for Institution Events, Lectures, activities sponsored and/or hosted by donors, corporate sponsors and/or non-profit agenciescan be listed by name.
- Institutional messages requested by the top officials, that units add to scheduled messagerotations.
- The Office of Public Relations / Students Welfare Dept. will approve or disapprove the requests, producing and distributing slides configured for different signage systems. Requests for Posting Messages Content pertaining to events (particularly on-site), updates, research, and seminars will be given top priority for posting in Samsung Digital Signage TV. All additionalrequests will be considered on a case-by-case basis.
- Please allow 2-3 business days for creation of all non-emergency messages. Urgent, last-minute requests, will be expedited and published as quickly as possible.

Maintenance Policy – Systems & Network

Lab System Maintenance Policy

- Lab systems are maintained by the CTS.
- Primary level problems are taken care by CTS.
  - Power connections
  - Booting problem
  - Network problem
  - Software installation / uninstallation
  - Hardware troubleshoot
  - Hardware replacement
  - Time schedule Internet maintenance.
  - Clearing the Junks and cache through CCleaner.
- Major Network, Software and Operating system related Problem are taken care by CTS Staff

Standalone Systems Maintenance Policy

Other than lab systems are maintained by CTS staff, notably like Deans, Directors, Secretary, Departments, Smart rooms and Auditoriums systems.

- Escalation methods:
  - Email
  - Phone call via Extn.
  - Direct Mobile
  - Official Letters
  - Meeting in-person
- General problem:
  - Power connections
  - Booting problem
  - Network problem
  - Software installation /uninstallation
  - Hardware troubleshoot
  - Hardware replacement

Clearing the Junks and cache through CCleaner

<u>Network & Surveillance Maintenance:</u>

Network switch

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

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

<u>Wireless Access points</u>

Access points are placed in staffrooms, smart rooms & Auditoriums and on demand places

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

<u>Surveillance</u>

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

- CCTV configured and installed in the required locations
- Bullet and Doom CCTV are used based on the places
- Faulty CCTV are serviced and installed.
- The video data are stored for 21 days .
- The footage is given on demand by Security team, supported by CTS
- The Playback and administration are done by Monitoring software of the Brand.

Policy for online delivery of classes & exams

1. Microsoft Teams is the authorized / accepted platform for delivering all virtual classes.
2. Students are boarded in Microsoft Teams based on the list received from theAdmissions/Academic offices.
3. Faculty are given privilege to create class teams and enroll the students in their classes.
4. Class schedule have to be done by the respective faculty.
5. Teachers will take the Attendance, Assignments & Quizzes
6. Recording of classes will be done only by the faculty
7. Recorded classes are made available to the students, if the student misses the class due tonetwork/ power failure he/she will be authorize to view the recordings.

8. MS Team platform is used for giving assignments and conducting Quizzes and Tests.
9. FAT examination conducted using CodeTantra platform, where the faculty will be proctoringthe students on live.

Policy for online meetings

Any Department / School who needs online meeting facility, need to send a request to Centre for Technical Support department (CTS), well in advance to schedule the meeting and to facilitate online meetings. However, on demand request is also accepted based on the availability of slots.

The meetings are facilitated through MS Teams, Zoom & Google meet.

Policy for conducting Conference / Workshops for larger audience

Schools/Centers are encouraged to use either Microsoft Teams Live Event (or) Zoom integrated with YouTube and Facebook to reach the larger audience. A formal official email communication will be sent to CTS department to facilitate with the approval of Deans / Directors / HODs / Section Heads.

Remote Access & Support Policy

IT support will be given to Faculty, Staff & Students using remote support tools like Sophos SSL VPN or Any-Desk or Team Viewer.

Usage of Biometric devices during COVID'19

Biometric feature is disabled and enabled the Smart Card / Proximity Card for Access Control Systemsand Attendance.

Data Backup and Restore Policy

VIT-AP has many critical applications that will be backed up periodically so that it can be used in all cases of restore. Centre for Technical Support (CTS) is responsible for ensuring that mission critical applications and data are well preserved and protected against loss and destruction. Adequate backups allow data recovery when information technology systems or information has been destroyed by system malfunction or by accidental/intentional action.

Backup & Restore Policy

- ❖ Each critical / production server will be backed up on a regular basis.
- ❖ CTS will backup the data's like System state data, Financial database, Payroll database, File server, Mailboxes, Production web server, Production database server, Domain controllers &etc with appropriate backup methods.
- ❖ Backup of systems and data should take place at night away of the working hours.
- ❖ Copies of all backups will be stored in a secure, off-site location

- ❖ Backups should not be stored in the same building as the live data or system.
- ❖ Data and Restore processes must be tested frequently.
- ❖ Appropriate backup methods (i.e., full, incremental, or differential) should be employed dailyin accordance with the allotted backup window.
- ❖ Backup media must adhere to industry accepted backup technology standards, such as:
  - The media's read/write capacity shall be rapid enough to permit the backup to be completed during the allotted time (i.e., before the start of the next business day
  - The media's compressed capacity shall be large enough to hold the complete backup
  - The media should be readable after a minimum of 5 years in unattended storage.
  - Data compression algorithms may be used to minimize the volume of data on the backup medium. When compression is employed, the selected parameters and algorithms must be documented and observed during data restoration (decompression).

Verification of Backup Status

The designated member of CTS staff must check the backup status on the system first thing every morning and report any failures to the Assistant Director - Systems. The backup software has automatic verification, which checks data transfer, reports error if occur, immediately corrects those errors and verifies backup data store.

Backup Schedules

- Daily backups will be scheduled Monday through Friday outside of working hours.
- Weekly backups will be scheduled during each weekend (Saturday & Sunday) outside ofworking hours.
- Production Oracle databases will have their archive and redo logs backed up a minimum twotimes a day

Retention of Backups

Backups will be kept on Storage for the following durations.

- Daily backups [Incremental Backup] will be kept for a minimum 7 days.
- Weekly backups [Full Backup] will be kept for 4 weeks.
- Backup Retention period is 30 days.

Off-site Storage of Backups

All Daily, Weekly, and Monthly, backup media will be kept at a secure off-site location.

The secure off-site location is defined as a physical location far enough away from the VIT-AP-CTS as to be protected from a Data Center disaster. The location is safe from environmental hazards, and securefrom physical access by other persons.

Replication of Disk Backup Media

Replication of the disk backup media to and from the off-site location will occur automatically based upon the backup software's best practice configuration. CTS staff will be responsible for ensuring thatany disk replication is functioning correctly at all times.

Backup Software

Commvault software is an enterprise-level data platform that contains modules to back up, restore, archive, replicate, and search data. It is built from the ground-up on a single platform and unified codebase. Data is protected by installing agent software on the physical or virtual hosts, which use operating system or application native APIs to protect data in a consistent state. Production data is processed by the agent software on client computers and backed up through a data manager, the Media Agent, to disk, tape, or cloud storage. All data management activity in the environment is tracked by a centralized server, the CommServe, and can be managed by administrators through a central user interface.

Backup Administrator Responsibilities

Backup administrator is responsible for the following

- Checking if the backup has been successfully taken.
- Troubleshooting and managing backup failure.
- Maintain backup media: Check the storage for the backup whether it is disks or tapes.
- Maintaining the backup log.

Testing/Validation

Testing and validation will be performed monthly by CTS to ensure the correctness of backups and backup media.

A random selection of computer systems will have small data sets selected from random Weekly, and Monthly, backup media to be restored in a way that will not impact production needs.

Successful restoration of data will indicate the correctness of Backup Procedures.

Distribution of Logs/Video footages for Research purpose

Description:

This policy is for the distribution of Logs/Video footages (hereafter referred as datasets) to VIT-AP Students, Faculty and Research Scholars for carrying out their research work in specific domains.

Source of Logs/Footages

VIT-AP information systems like servers, workstations, firewalls, routers, switches, communications devices, NVRs etc.

Logs Distribution Policy

- Users can approach Centre for Technical Support (CTS) to get the required datasets throughproper channel.
- CTS will inspect the need and authenticity of their requirement.

- CTS can accept/reject the request on assessment, if accepted, the required dataset will beshared over electronic media (Email/FTP/Flash Drive/External HDD).

Logs Usage Policy

- Research Scholars/Student/Faculty authorized to receive the datasets or only allowed to usethe data for their research work specified in the request.
- They should not share/reproduce either full/any part of the data which was given for theiruse.
- They are not allowed to publish any form of the dataset given in public/social media
- On completion of the research, they need to completely destroy the datasets given and informCTS in writing which will be verified.

Enforcement

Students, Faculty and Research Scholars found in policy violation may be subject to disciplinary action, up to and including termination.