

VIT[®]

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

**INTERNAL ACADEMIC AND ADMINISTRATIVE AUDIT
AY 2023-2024 (01-07-2023 TO 30-06-2024)**

IT Policy

IT POLICY

IT Policy
(Release: August 2024 Version 5.0)

Prepared by
Centre for Technical Support, VIT

Table of Contents

Sl. No.	Chapter	Page Number
1	Need for IT Policy	3
2	Acceptable Use Policy	5
3	Employee Acceptable Use Policy	6
4	Student Acceptable Use Policy	8
5	Vendor Acceptable Use Policy	10
6	Network Security Policy	11
7	Hardware and Software Procurement Policy	14
8	IT Hardware Installation Policy	15
9	Software Installation and Licensing Policy	17
10	Web Site Hosting Policy	19
11	Database Use Policy	20
12	IT Policy for Data Centre	22
13	IT Policy for using VDI	23
14	IT Policy for Server Virtualization	24
15	Video Surveillance Policy	26
16	Digital Signage Policy	27
17	Systems & Network Maintenance Policy	29
18	Policy on using collaboration tools (Microsoft Teams, Zoom & Google Meet)	31
19	Remote Access & Support Policy	32
20	Data Backup & Restore Policy	33
21	Distribution of Logs/Video footages for Research purpose	35
22	Vulnerability Assessment and Patch Management	36
23	Password Management Policy	38
24	E-Waste Policy	40
25	Laptop Policy for faculty during Foreign Trip	41
26	Google Workspace Policy for Faculty & Staff	43
27	Internet Usage Policy	46
28	Deactivation of IT Services	48

IT POLICY

(Release: August 2024 Version 5.0)

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

Every member of the VIT 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 reserves the right to interpret, revise, or delete any of the provisions of these policies, as the VIT 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 community to understand how institution policy applies to some of the significant areas and to bring conformance with stated policies.

Further, the policies will be applicable at two levels:

- End User Groups (Faculty, Students, Research Scholars, Administrators, Officers and other Staff)
- Network Administrators

It may be noted that VIT IT Policy applies to technology administered by the institution centrally or by the individual departments, to information services provided by the VIT administration, or by the individual departments, or by individuals of the VIT community, or by authorised 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 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 VIT IT policy.



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the VIT IT Infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by VIT 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 Students
- Employees (Permanent/Temporary/Contractual)
- Faculty
- Research Scholars
- 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



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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

A handwritten signature in green ink that reads 'T. Jayar'.

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Employee Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by VIT imposes certain responsibilities and 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 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 behaviour & 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 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 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 infection which 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 the appropriate 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, which may result in your network access being disabled.

T. Jayar
REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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 network system access to anyone who is not a VIT 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.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Student Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by VIT imposes certain responsibilities and 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 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 behaviour & 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 mission.
3. The use of VIT 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 infection which 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 may result 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. 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.
7. The use of personal routers (wireless or wired) and/or DHCP servers is strictly prohibited.



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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 network system access to anyone who is not an authorized VIT faculty, staff member or student is prohibited.
10. Connecting standard mobile devices used for the pursuit of academic work to VIT wireless network is permitted. Connecting any other device or system to the institution data networks without 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 analyser or similar mechanism without prior authorization
 - g. Degrading or restricting network access for others, either on or off campus
 - h. Connecting to Institution systems that one has not been expressly permitted to access
 - i. Downloading, sharing or using copyrighted material including music, movies, software or text books
 - j. Participating in activities which are not consistent with the Mission of the institution


In addition, your network access may be disabled if VIT receives complaints about or otherwise detects inappropriate behaviour.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

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 data.
2. Vendor agrees to only use VIT data, systems, resources, integrations, and access solely for the original purpose for which it was intended as stipulated in any contract which exists between Vendor and VIT.
3. Vendor will not mine VIT data for any purpose whether internal or external to Vendor Company.
4. Vendor will not share VIT data with any third party, without express permission of the Institution in writing.
5. Vendor agrees to use VIT data, systems, resources, integrations and access in a manner which is consistent with the Mission of the institution.
6. Vendor agrees to comply with all local laws as they apply to VIT systems and data.
7. Vendor agrees to be knowable about and comply with all other VIT policies.
8. The use of VIT resources to access, further or otherwise participate in activity that 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 behaviour & 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 mission.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Network Security Policy

Purpose

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated 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 from misuse.

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

Network Connections

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



REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Wireless

1. Centre for Technical Support (CTS) is solely responsible for providing wireless networking services on campus. No other department may deploy wireless routers, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus.
2. CTS is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.
3. The Institution will maintain a campus wireless network based only on IEEE 802.11 standards. CTS will collaborate with academic departments where devices used for specific educational or research applications may require specific support or solutions.
4. CTS will provide a general method for network authentication to Institution systems. The IEEE 802.1x standard is the currently supported authentication method. Additional security protocols may be applied as needed.
5. All users of wireless network resources at VIT are subject to the applicable Network Acceptable Use Policy. Users of wireless resources at VIT agree to have read and be bound by the terms and conditions set forth in that policy.

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 and must 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 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 DHCP or 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.

T. Jayar

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



- i. Students may consult the Student Acceptable Use Policy for further information.
- ii. Employees may consult the Employee Acceptable Use Policy for further information.

External Traffic, Services and Requests

1. CTS will take action to prevent spoofing of internal network addresses from the Internet. CTS will also take action to protect external Internet sites from source address forgery from devices on the Institution network.
2. The Institution external Internet firewall default practice is to deny all external Internet traffic to the Institution network unless explicitly permitted. To facilitate this, academic Schools, Centers, 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 behaviour.
4. CTS reserves the right to decrypt SSL traffic which transits the Institution network.

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 resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.

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.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Hardware and Software Procurement Policy

Policies

1. The procurement of all computing and communication hardware and software is coordinated by the office of Centre for Technical Support (CTS) in order to maximize the VIT investment in Information Technology (IT).
2. To take advantage of IT tools in the most cost-effective manner possible, the VIT 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 consult with the department to select the most appropriate equipment and to work out an agreement for continued support.
4. Departments who choose to buy IT resources not approved by CTS are responsible for their implementation and ongoing maintenance. CTS will not be responsible for interfacing such hardware or software to the campus network or information repository.
5. In accordance with the VIT funding philosophy, costs for the acquisition of IT resources are borne by the purchaser.



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



IT Hardware Installation Policy

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

Who is Primary User

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

What are End User Computer Systems

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

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/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 required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

Network Cable Connection

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

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

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.

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 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 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 Purchase Department, CTS Department will attend the complaints related to any maintenance related problems.

Noncompliance

VIT 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.

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.



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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

- ❖ 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.
- ❖ 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.
- ❖ 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 at least 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

- ❖ 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.
- ❖ Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

T. Jayar

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



- ❖ 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 on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.
- ❖ Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on DVD, Flash Drive or other storage devices.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Web Site Hosting Policy

Policy

- ❖ VIT has an official website for the public access. Schools, Centers and Departments of Teachers / Employees / Students may have pages on VIT'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.
- ❖ Any department or an individual requires to publish any official content in the institution official website may sent the content to Web Upload 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.
- ❖ The SSL service will be used in Primary Domain and sub domain of the website to add an additional layer of security.
- ❖ CTS - Infra team will give high priority to keep the systems updated with security fixes.
- ❖ VIT offers WordPress hosting only to VIT Organizational Units and their sponsored activities. VIT does not manage the content of VIT-hosted sites. Each site has its own Webmaster and it is up to the designated Webmaster to manage their own content.
- ❖ For the benefits of the students and employees, VIT has an intranet portal to post day-to-day activities and circulars.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Database Use Policy

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

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

- A. **Database Ownership:** VIT is the data owner of all the Institution's institutional data generated in the institution.
- B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute Institution's database. They may have custodianship responsibilities for portions of that data.
- C. **Data Administrators:** Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

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

- ❖ The institution's data policies do not allow the distribution of data that is identifiable to a person outside the institution.
- ❖ Data from the Institution's Database including data collected by departments or individual faculty and staff, is for internal institution purposes only.
- ❖ One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the institution makes information and data available based on those responsibilities/rights.
- ❖ 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.
- ❖ Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the Institution and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the Institution Registrar for response. Tampering of the database by the department or individual user comes under violation of IT policy.

T. Jayar

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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, hardware, system software crash thereby destroying the whole of, or part of database deliberately with ulterior motives by any individual.
- ❖ Trying to break security of the Database servers.

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

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

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

IT Policy for Data Centre

The Data Center is vitally important to the ongoing operations of the VIT. The following policies and procedures are necessary to ensure the security and reliability of systems residing in the Data Center.

Access to VIT Data Centre

In order to ensure the systems housed within the data centre are kept secure, the following policies apply to all personnel requiring access:

1. All personnel who access the Data Center must have proper authorization. Individuals without proper 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 will be monitored by Data Center employees through live video cameras.

Policy

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



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

IT policy for Virtual Desktop Infrastructure (VDI)

VDI stands for Virtual Desktop Infrastructure, Our VDI service or Virtual Desktop Infrastructure service is a flexible end user experience that delivers maximum workplace productivity and convenience for our faculty, staff and students.

The desktop can be accessed from a variety of devices, including smart phones, tablets, laptops and regular desktops. You can access it on and off campus, from anywhere in the world provided there is internet connectivity.

Policy

- ❖ Must be a VIT student, faculty, or staff member.
- ❖ Must be enrolled in a class that will be using virtual desktops.
- ❖ Using this technology, the end user is free to use the mobile device of their choice and Access Institution specific / class specific software without additional costs for the supported software.
- ❖ When finished using the VDI, make sure to Disconnect and Logoff, rather than just Disconnect.
- ❖ Simply disconnecting will leave you logged into the VDI, tying up a virtual desktop and preventing someone else from using that resource.
- ❖ DO NOT save data on the virtual machine. Use your allotted network storage instead. Virtual machines are often reset and refreshed.



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



IT Policy for Server Virtualization

One of the most significant service offerings of the IT Services is the provision of 'Servers' facilities for IT operational, research and teaching groups and individuals. Our server provisioning preference and facilities are in the form of virtual machines (VMs) on the VMware ESXI / Nutanix AHV platform.

Virtual Server

Administrative Systems offers managed virtual servers as an alternative to managed physical servers. This service takes advantage of virtualization technology to host multiple virtual servers, each of which functions as a complete and independent server, on a single physical server.

Policy

Because of energy and space savings gained by using virtual servers, VIT has adopted a "virtual first" policy. We do recognize that virtual servers are not appropriate for all application needs; see the criteria below for our guidelines.

Unless your application or use requires:

- specific or proprietary hardware peripherals;
- databases or other I/O-intensive services;
- applications or systems that exceed current virtual server performance or capacity thresholds; or
- applications that explicitly do not support virtualization

Our policy is to deploy a virtual server.

Additionally, the virtual machine:

- will be hosted in VIT Data Centre
- if supported by VIT, must run on an OS from the list of supported operating system types.

Supported Guest Operating Systems:-

Virtual servers will be provisioned with latest versions of Ubuntu Linux, Oracle Linux, Cent OS and Windows Servers

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

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 exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
3. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
4. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

B. Purpose of the system

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

- ❖ Deter those having criminal intent
- ❖ Assist in the prevention and detection of crime
- ❖ Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- ❖ Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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.
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.

D. Recording

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

E. Access to images

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

F. 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.

T. Jayar

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Digital Signage Policy

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 sponsored Events, Sports and, etc.

Information displayed includes (but is not limited to): Programs, Meetings and Activities; 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 Institution.

Equipment – Installation

- ❖ Schools, departments and Centre's are responsible for the funding of equipment, licenses and installation 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 Estates Team. Additionally, VIT Estates Team will approve digital 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 manner that 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 activities or advertisements from non-institution organizations.

T. Jayar

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



- Messages that invite public participation in programs must include the VIT accessibility statement.
- Messages should not use copyrighted images or content without permission or license.
- Messages should include the VIT 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 agencies can be listed by name.
- Institutional messages requested by the top officials, that units add to scheduled message rotations.
- 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 additional requests 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.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Systems & Network Maintenance Policy

Lab System Maintenance Policy

- The Lab assistant maintains lab systems.
- Primary level problems are taken care by Lab assistant.
 - 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:
 - CMS ticketing systems
 - 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

T. Jayal

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Network & Surveillance Maintenance:

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.

Wireless Access points

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.

Surveillance

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

- 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's are stored for 1 month.
- The footage are given on demand by Security team, supported by CTS
- The Playback and administration are done by Monitoring software of the Brand.

REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Policy on using collaboration Tools (Microsoft Teams, Zoom & Google Meet)

Online delivery of Classes & Exams


- ❖ Microsoft Teams is the authorized / accepted platform for delivering all virtual classes.
- ❖ Students are boarded in Microsoft Teams based on the list received from the Admissions/Academic offices.
- ❖ Faculty are given privilege to create class teams and enrol the students in their classes.
- ❖ Class schedule have to be done by the respective faculty.
- ❖ Teachers will take the Attendance, Assignments & Quizzes
- ❖ Recording of classes will be done only by the faculty
- ❖ Recorded classes are made available to the students, if the student misses, the class due to network/ power failure he/she will be authorize to view the recordings.
- ❖ MS Team platform is used for giving assignments and conducting Quizzes and Tests.
- ❖ FAT examination conducted using CodeTantra platform, where the faculty will be proctoring the students on live.

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.

Conference / Workshops for larger audience

Schools/Centres 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.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India³¹

Remote Access & Support Policy

- ❖ IT support will be given to Faculty, Staff & Students using remote support tools like Any-Desk, Ultraview, Microsoft Quick Assist and Team Viewer.
- ❖ Remote usage of computing facilities can be provided to students using Virtual Desktop Infrastructure (VDI), VPN (Global Protect), Direct Nating access with the approval of Deans / Programme Co-ordinators and Faculty.
- ❖ Remote access to employees can be provided using VDI to access Institution resources.



REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Data Backup and Restore Policy

VIT 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 daily in accordance with the allotted backup window.


Backup Schedules

- ❖ Daily backups will be scheduled Monday through Saturday outside of working hours.
- ❖ Weekly full backups will be scheduled during each weekend (Saturday/Sunday) outside of working hours.

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.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956) 33
Vellore-632 014, Tamil Nadu, India

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-CTS as to be protected from a Data Center disaster. The location is safe from environmental hazards, and secure from 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 that any disk replication is functioning correctly at all times.

Backup Administrator Responsibilities

Backup administrator is responsible for the following

- ❖ Checking if the backup has been successfully taken.
- ❖ Troubleshooting and managing backup failure.
- ❖ 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.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



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 Students, Faculty and Research Scholars for carrying out their research work in specific domains.

Source of Logs/Footages

VIT 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 through proper 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 be shared 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 use the 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 their use.
- ❖ 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 inform CTS 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.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Vulnerability Assessment & Patch Management Policy

Overview

IT Infrastructure must be properly maintained with the most up to date patches and updates. This is to minimize system vulnerability and to ensure the confidentiality, integrity and availability of its systems and data stored on its systems.

Scope

This policy applies to:

- ❖ All systems, including servers, workstations, laptops, tablets, smartphones, network devices, IoT devices, surveillance & etc.
- ❖ Both Institution-owned systems and personal systems that are connected to the VIT Networks (including wireless) or used for Institution work.
- ❖ All software on these systems, including firmware, BIOS, hypervisor, operating system, drivers, libraries, middleware and applications.

Policy

- ❖ All IT systems shall be manufacturer supported and have up-to-date and security patched operating systems and application software.
- ❖ Security patches must be installed to protect assets from known vulnerabilities.
- ❖ Patches rated 'Critical' by the vendor must be installed within 7 days of release from the operating system or application vendor unless prevented by University change control procedures.
- ❖ Patches rated 'High' by the vendor must be installed within 14 days of release from the operating system or application vendor unless prevented by University change control procedures.
- ❖ Patches rated 'Low' or 'Medium' by the vendor must be installed within 28 days of release from the vendor, unless mitigating controls are in place to prevent the exploit being realised, in which case it may be deferred to the nearest maintenance window.
- ❖ A shorter timeframe may be mandated based on the assessed severity and potential/actual impact.
- ❖ All servers shall comply with recommended minimum requirements (default operating system level, patching levels, service packs etc.) as specified by CTS.
- ❖ Patching of systems will be centrally managed wherever possible, unless there are clear reasons for patching to be performed locally.

T. Jayar

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



- ❖ Users shall reboot their device/s when prompted to do so. - Users may defer rebooting a device a maximum of two times (critical rated patches excepted) within the first 10 days of a patch being deployed by CTS, after which time it shall be automatically rebooted.
- ❖ For many systems, it will be appropriate to enable automatic updates. This is the recommended method for patching the network devices, workstations, and may also be appropriate for some servers. Whereas in other cases, applying patches manually may be preferable. In most cases, installing an update or security patch is the preferred approach to address a vulnerability.

Monitoring and Reporting

Reporting metrics that summarise the outcome of each patching cycle shall be compiled and maintained by CTS. These shall be used to evaluate patching levels and assess current levels of risk.

Exceptions

There are some systems that cannot be patched. For example, systems that are end of life or that require a precise version of software to operate. Exceptions must be risk assessed, have formal documented approval and be recorded.

Roles and Responsibilities

- ❖ Vulnerability assessment and patching will only be carried out by designated roles. These roles are:
 - a) Data Centre & Monitoring – Assessment & Patching
 - b) Server Infrastructure Team – Assessment & Patching
 - c) Network Infrastructure Team – Assessment & Patching
 - d) Desktop Management Team – Assessment & Patching
 - e) IT Security Team – Assessment
- ❖ Deputy Director - Systems is accountable for ensuring that all systems are managed in accordance with Institution IT policies.
- ❖ IT staff and any other staff who manage systems and applications are responsible for:
 - a) Proactively applying security updates to these systems
 - b) Recording changes on the Institution change control system
 - c) Monitoring the security status of their systems, including that the patches which are supposed to be installed have installed correctly
 - d) Taking action if they are notified about a specific vulnerability
e.g. reported by the CTS Network Security team
- ❖ The IT Security Team provide advice on security risks and appropriate measures to deal with them. They also run network vulnerability scans, distribute the results, track actions taken to address vulnerabilities found and ensure escalation takes place where appropriate

T. Jayar
REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Password Management Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of a department's entire network. Any device connected to the campus networks must implement authentication and authorization processes that uniquely identify all users and appropriately control access to systems.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all faculty, staff and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system connected to the campus network, has access to the campus network, or stores any non-public VIT information. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Policy:

VIT requires that:

- ❖ All systems-level passwords (e.g., root, administrator, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
- ❖ All production system-level passwords must be part of the Team password management database.
- ❖ All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 10 passwords.
- ❖ User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- ❖ Passwords must not be inserted into email messages or other forms of electronic communication.



REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Users must select strong passwords. Strong passwords have the following characteristics:

- ❖ Be at least 12 - 32 characters in length
- ❖ Be a mixture of letters and numbers
- ❖ Be changed at least every 90 days
- ❖ Be different from the previous 10 passwords
- ❖ Can NOT contain your EMPID, First Name, or Last Name
- ❖ Not contain 4 consecutive characters used from the previous password
- ❖ Not contain the user's user id

Note that poor, weak passwords have the following characteristics:

- ❖ The password contains less than six characters
- ❖ The password is a word found in a dictionary (English or foreign)
- ❖ The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, and so on
 - Computer terms and names, commands, sites, companies, hardware, software
 - Birthdays and other personal information such as addresses and phone numbers
 - Word or number patterns like aaabbbb, qwerty, zyxwvuts, 123321, and so on
- ❖ Any of the above spelled backwards
- ❖ Any of the above preceded or followed by a digit (for example, secret1, 1secret)

Further, systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

Members of the VIT must follow these guidelines for passwords:

- ❖ Don't reveal a password over the phone to ANYONE
- ❖ Don't reveal a password in an e-mail message
- ❖ Don't talk about a password in front of others
- ❖ Don't hint at the format of a password, like, "my family name"
- ❖ Don't reveal a password on questionnaires or security forms
- ❖ Don't share a password with family members
- ❖ Don't reveal a password to co-workers

Members of VIT must not use the "Remember Password" feature of applications.

Members of VIT must not write passwords down and store them anywhere in your office. Further, passwords must not be stored on ANY computer system without encryption.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

E-Waste Policy

Purpose:

“E-waste”, “electronic waste”, “e-scrap” and “end-of-life electronics” are terms often used to describe used electronics that are nearing the end of their useful life, and are discarded, donated or given to a recycler. Though “e-waste” is the commonly used term, VIT considers e-waste to be a subset of used electronics and recognizes the inherent value of these materials that can be reused, refurbished or recycled to minimize the actual waste that might end up in a landfill or improperly disposed in an unprotected dump site.

VIT has entered into an arrangement with an authorized service provider for management of the entire process of disposal of Electronic and Electrical wastes right from Collection to disposal at Approved facilities of the service provider.

Policy & Guideline

- ❖ Centre for Technical Support (CTS) officials will identify the old electronic assets which is beyond 9 years and considered them as obsolete.
- ❖ Entire list of items will be taken and will be informed the Department / School about the obsolete assets.
- ❖ CTS will look for information on the catalogue with the product for end-of-life equipment handling.
- ❖ CTS will communicate about the obsolete assets with recyclers to quote. Also we will ensure that only Authorized Recyclers/Dismantler handle the electronic (i.e. LED TV's and accessories) products.
- ❖ E-Waste will awarded to highest quoted recyclers/dismantler and form-6 will be collected from the vendor.
- ❖ CTS will maintain a stock book for all E-Waste items gets disposed.
- ❖ Annual return of e-waste disposed will be submitted to Tamil Nadu Pollution Control Board in the prescribed format (Form-3) every June.


REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Laptop Policy for faculty during Foreign Trip

Purpose

Laptops provide important functionality, allowing faculty to have their computing resource at hand in meetings/workplace or even at home in certain time pressing situations so as to enable faculty to be maximally functional and productive while away from VIT premises.

Policy and Guideline

- ❖ A faculty can make a request to Centre for Technical Support for availing a Laptop for his Foreign Trip. Based on their request, CTS will facilitate the laptop based on the availability.
- ❖ In case of the loss of laptop be it on, or off VIT premises, due to negligence of the faculty, VIT may recover the cost of the laptop from the faculty.
- ❖ The laptop issued to be returned to CTS on the day of their reporting to the Institution after the foreign trip in good working condition.
- ❖ Faculty members to take the data backup before handing over the laptop to CTS.
- ❖ If there is damage on account of the above the faculty may be liable to pay the damages at cost to the VIT/the same may be deducted from their monthly salary.
- ❖ In case of any failure, faculty are required to report the same to the Centre for Technical Support.
- ❖ Faculty may not take the laptop for repair to any external agency or vendor at any point of time.

Physical Security & Theft protection

To ensure physical security of laptops and data therein, all faculty are required to undertake the following actions:

T. Jayar

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

- ❖ The physical security of VIT provided laptops is the faculty personal responsibility. He/she is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.
- ❖ Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
- ❖ Never leave a laptop visibly unattended in a vehicle. If necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.

Additional Recommendations

- ❖ Set Wi-Fi to “do not automatically connect to Wi-Fi” on all devices capable of wireless connections.
- ❖ **DO NOT** update your computer while connected to a public or hotel wireless network.
- ❖ Disable Bluetooth on your laptop, mobile phone, and other devices.
- ❖ Tape over any integrated laptop cameras, or disable them to prevent a hacker from viewing you while you use your laptop.
- ❖ Ensure host based firewalls are configured and enabled on Windows and Mac laptops.



REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Google Workspace Policy for Faculty & Staff

Purpose

Vellore Institute of Technology (VIT) has collaborated with Google to bring Google Workspace for Education Plus, a cloud-based collection of applications that will help enhance teaching, learning and research within the Institutions. The applications includes all the products you already use, like **Google Classroom, Google Meet, Gmail, Google Calendar, Google Drive, Google Docs, Google Sheets, Google Slides and many more**. Everything you need to teach, learn, connect and share will remain all in one place, accessible from anywhere on any device.

Policies

Google Workspace is made available to all Faculty, Staff & Students under the terms of a contract between VIT and Google, which must be agreed to by each VIT user. Email users should use primarily for academic and official purposes and to a limited extent for personal purposes. The following are the quota of storage allocated to email users.

1. Core Group – **Unlimited**
 2. Deans & Directors – **50 GB**
 3. All Faculty – **20 GB**
 4. All Staff – **10 GB**
 5. All Students – **10GB**
- ❖ Keep it legal. Don't use VIT Email account to promote, organize, or engage in unlawful activities.
 - ❖ The termination or suspension of email accounts, which are in individual names, should be executed based on the instruction from HR Department.
 - ❖ While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
 - ❖ 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.

T. Jayar
REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)⁴³
Vellore-632 014, Tamil Nadu, India



- ❖ User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
- ❖ 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.
- ❖ Impersonating email account of others will be taken as a serious offence under the VIT IT policy.
- ❖ Any spam mail received by the user into INBOX should not be forwarded to anyone and could be deleted.
- ❖ Students are given VIT mail ID under the domain “**vitstudent.ac.in**” hosted in Google Workspace. Students will be able to use all the features offered by google.
- ❖ All the alumni’s are given with a lifetime mail ID to interact with their classmates or college mates or with VIT. Once the student becomes alumni, the mail id will be moved from the “**vitstudent.ac.in**” to “**vitalum.ac.in**” without losing any mails. A prior notification will be sent to student well in advance before the migration.

Email Data Backup

Google Workspace includes built-in redundancy and recovery features, but it does not provide comprehensive backup against today’s disasters. The default protection is designed to only prevent Google customer data loss due to a Google infrastructure failure. Google’s native backup options, include Google Vault, Google Takeout and Google Workspace Migrate. Faculty & Staff members should take the periodical backup of Email & Drive data using Google Takeout feature.

Spam and Bulk Mail

- Don’t use VIT Gmail to distribute spam or unsolicited commercial mail.
- You are not allowed to use VIT Gmail to send email in violation of the CAN-SPAM Act or other anti-spam laws; to send unauthorized email via open, third-party servers; or to distribute the email addresses of any person without their consent.
- You are not allowed to automate the Gmail interface, whether to send, delete, or filter emails, in a manner that misleads or deceives users.

T. Jayar
REGISTRAR



- Please keep in mind that your definition of “unsolicited” or “unwanted” mail may differ from your email recipients’ perception. Exercise judgment when sending email to a large number of recipients, even if the recipients elected to receive emails from you in the past. When Gmail users mark emails as spam, it increases the likelihood that future messages you send will also be classified as spam by our anti-abuse systems.

Malware

- Don’t use Gmail to transmit viruses, malware, worms, defects, Trojan horses, corrupted files, or any other items of a destructive or deceptive nature.
- In addition, don’t distribute content that harms or interferes with the operation of networks, servers, or other infrastructure belonging to Google or others.

Fraud, Phishing, and other Deceptive Practices

- You may not access another user’s Gmail account without their explicit permission.
- Don’t use Gmail for phishing. Refrain from soliciting or collecting sensitive data, including but not limited to passwords, financial details, and Social Security numbers.
- Don’t send messages to trick, mislead, or deceive other users into sharing information under false pretenses. This includes impersonating another person, company, or entity with the intent to deceive or mislead.

Harassment

- Don’t use VIT Gmail to harass, intimidate or threaten others. Anyone found to be using Gmail for these purposes may have their account disabled.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India

Internet Usage Policy

The institute shall provide superior connectivity and adequate bandwidth across the campus that includes Administrative building, Department Buildings and student Hostels through Wi-Fi.

- Internet usage policy must ensure high availability of bandwidth through a proper bandwidth allocation plan for its optimum utilization.
- Total Bandwidth used in the campus is 13Gbps which being shared and access across the academic and Hostels of the Institute.
- Internet speed of 6Mbps has been provided to the Hostellers to access the bandwidth.
- Allot equal bandwidth to two hostels (Boys & Girls) as per their requirements.
- Adequate bandwidth must be allocated for usage by students across the Hostels and Hot Spots in the academic Area through Wi-Fi
- The library should be allocated adequate bandwidth all through its operational time.
- An authentication mechanism must be deployed to monitor unproductive and illegal usage of the internet facility.

User responsibilities

- There shall be restricted usage of internet, limiting it to Gmail, You Tube, Wiki and other educational websites within the campus.
- Any usage of applications like Torrents/Proxy/Tunnels are not allowed. If found a serious action will be taken.
- It may be clearly conveyed to all stakeholders that such IT facilities are provided only for academic, official purposes only and not for personal or commercial use.
- All users must abide by the laws, regulations of the IT act of the Government of India, and any violation must be firmly dealt with by the authorities.

T. Jayar
REGISTRAR

Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



- Users shall be held responsible for any undesirable content sharing, abuse or storage while using the campus network. They are responsible for the content stored in the designated workspace allocated to them (example: file storage area, webpages, stored/archived emails, on Computer Centre or Department machines).
- Users are responsible for all the network traffic generated by their computer. Physically tampering with network connections/equipment(s), connecting additional (personal) network devices like Routers and Switches, or making exclusive use of network resources is **STRICTLY NOT ALLOWED** in hostels and academic buildings.
- Users are not allowed to set up his/her own Wi-Fi network, which is connected to the campus backbone using routers or software like Connectivity/Hotspot etc. Users are not permitted to install proxy / torrent download / games download / direct download etc. Users are not allowed to engage in any activity with intent of degrading the performance of the network.
- Use of network for creating, sending, storing, uploading, accessing, using, soliciting, publishing, or linking offensive, obscene, profane, or indecent images or material is **STRICTLY NOT ALLOWED**.
- Users are not allowed to download pirated software or any suspect malware from the internet and spread the same among other users.
- Users are not allowed to do security related misuse which includes attempting to bypass firewalls and access rules in place, breaking security of the systems, trying to capture passwords of other users, Damaging / Gaining access to the data of other users etc.
- Users are not allowed to cause physical damage to compute or networking facility or property of the Institute.
- Users are not allowed to install personal software for use on Institution computer systems except the ones leased to the user. Users are not allowed to download/install unauthorized/pirated software.

T. Jayar

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India



Deactivation of IT services

Purpose: When the Employee get relived on the basis of retirement, resignation and termination, similarly when the student Discontinue his/her studies, this policy provides the guidelines to deactivate the IT services acquired while studying/working in this Institution.

Policy:

1. The employee or student details will be verified and the Laptop/tablet/Mobile will scanned manually to understand the services available for them.
2. The endpoint security-K7 provided to the employee or student Laptop/tablet will removed and refreshed so that the details of the devices will be removed.
3. The internet access provided to the employee or student Laptop/tablet will be removed in the Web security Appliances /Firewall so that the internet access will be no longer available for the Laptop/tablet.
4. The Domain Name Service – DNS had been enabled in the DNS secured service – Cisco Umbrella. The Name and the IP will be removed and refreshed and to verify the details are no longer available to Employee or Student Laptop/tablet.
5. The Wireless Access of the Employee or Student Laptop will verified in the DHCP and the Wireless controller. The Mac address of the Laptop will be removed in the DHCP Scope and in the Wireless Controller. All the SSID will be removed and refreshed to verify the details of the Laptop are no longer available for they employee.
6. Other deactivating IT service including E-Mail and MS-Teams are followed based on the Email Use policy and Online delivery of classes and Exams & Meeting.

REGISTRAR
Vellore Institute of Technology (VIT)
(Deemed to be University under section 3 of UGC Act, 1956)
Vellore-632 014, Tamil Nadu, India