VTM NSS
COLLEGE
DHANUVACHAPURAM
SINCE 1964
RE-ACCREDITED BY NAAC WITH B+

IT POLICIES & GUIDELINES

Table of Contents

1. Preface

The IT Policy aims to establish guiding principles for expanding and upgrading the IT infrastructure at Velu Thampi Memorial (VTM), NSS college. The policy is intended to support the educational, instructional, research, and administrative activities of the college. The primary objective is to promote and develop state-of-the-art IT infrastructure at VTM NSS College, Dhanuvacahpuram. This policy is being documented for academic purposes and is intended for use by students, faculty, staff, management, visiting guests, and research fellowship members.

Due to policy initiatives and academic drives, IT resource utilization in the campus has grown significantly over the past decade. The college has network connections to every computer system, covering more than two buildings across the campus. The Computer Centre is responsible for running the institute's intranet and internet services, including firewall security, DHCP, DNS, email, web and application servers, and managing the network of the institute. VTM is obtaining its internet bandwidth from BSNL, with a total bandwidth availability of 100 Mbps (leased line 1:1).

The widespread use of the internet has resulted in network performance issues in three ways: • The speed of Local Area Network (LAN) is affected when compared to internet traffic over the Wide Area Network (WAN).

- Free internet access for users leads to uncritical downloads that congest the traffic, affecting the Quality of Service (QoS) and impacting critical users and applications.

- When computer systems are networked, viruses that enter through the intranet/internet spread rapidly to all other computers on the network, exploiting the vulnerabilities of the operating systems.

The high number of concurrent users trying to access internet resources through a limited bandwidth creates stress on the available internet bandwidth. Every download adds to the traffic on the internet, which leads to higher costs and decreased Quality of Service and Experience. The solution is to reduce internet traffic.

Computer viruses are a significant threat to the network. They attach themselves to files and spread quickly when files are sent to others. Some viruses can damage files and reformat the hard drive, causing extensive losses to the enterprise. Others simply replicate themselves, taking up network space and slowing down the network. Emails, unsafe downloads, file sharing, and web surfing account for most of the virus attacks on networks. Once a virus gains entry into the network, it can slow down or even halt the network.

Containing a virus once it spreads through the network is challenging and can result in the loss of man-hours and data. Therefore, preventing viruses at the earliest stage is crucial. Computer Centre has taken appropriate steps to secure the network, including installing firewalls, access control, and virus checking and content filtering software at the gateway. However, in the absence of clearly defined IT policies, it is challenging to convince users about the steps taken to manage the network. Users may feel that such restrictions are unwarranted, unjustified, and infringe on their freedom.

Applies to Stake holders on campus or off campus

- Students: Diploma, 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

2. Vision, Mission and Objectives:

The vision and mission of an IT policy articulate the overarching goals and objectives of an organization's approach to managing information technology.

Vision: To create a secure, reliable, and innovative technology infrastructure that supports our organization's mission and enables us to meet the needs of our stakeholders.

Mission: Our IT policy is committed to:

- Ensuring the confidentiality, integrity, and availability of our information assets
- Implementing best practices for technology management, including risk assessment, incident response, and disaster recovery
- Encouraging innovation and collaboration across our organization through the use of technology
- Providing training and support to ensure that all employees have the skills and knowledge they need to use technology effectively
- Engaging with stakeholders to understand their technology needs and expectations, and delivering solutions that meet those needs

Through these efforts, we aim to create a technology environment that enables our organization to operate efficiently, make data-driven decisions, and achieve our strategic goals

Policy Objectives

IT (Information Technology) policy objectives typically aim to ensure the effective and efficient use of technology within an organization or government. Some common objectives include:

1. Security: Protecting sensitive data and systems from unauthorized access, theft, and other security breaches.

2. Accessibility: Ensuring that technology is accessible to all users, including those with disabilities.
3. Efficiency: Ensuring that technology is used efficiently to achieve the organization's goals, and avoiding wasteful or unnecessary spending on technology.
4. Innovation: Encouraging the development and adoption of new technologies that can help the organization be more productive, efficient, and competitive.
5. Interoperability: Ensuring that different technologies used within the organization can work together effectively, and avoiding silos and other barriers to collaboration.
6. Compliance: Ensuring that the organization is in compliance with relevant laws and regulations related to technology, such as data privacy laws or cybersecurity standards.
7. Sustainability: Encouraging the use of technology in a sustainable and environmentally friendly way, and minimizing the environmental impact of technology use.
8. Transparency: Ensuring that the organization's use of technology is transparent to stakeholders, including employees, customers, and the public.

3. Hardware Installation policy:

To minimise the inconvenience caused by hardware failures and interruptions in services, the user community of the institute network needs to follow certain precautions when installing their computers or peripherals

Some key components that should be included in an IT hardware installation policy:

1) Primary User: The individual who has their computer installed in their room and primarily uses it is considered the "primary user". If a computer has multiple users but none of them can be designated as the "primary user, the department head should appoint someone to be responsible for compliance.
2) End User Computer System: The institute considers computer systems, other than client PCs used by users, as end-user computers. This includes servers that are not directly managed by the Computer Centre. If a primary user cannot be identified, the department must take on the responsibilities assigned to the end-users. Even if registered with the Computer Centre, computer systems that function as servers providing services to other users on the Intranet/Internet are still considered end-user computers under this policy.
3) Warranty and Annual Maintenance Contract: For any Department/Cells purchasing computers, it is preferred that they come with a 3-year onsite comprehensive warranty. Once the warranty has expired, the Computer Centre or external Service Engineers can maintain the computers on a call basis. This maintenance should encompass OS re-installation and checking for virus-related problems.
4) Connecting Power t0 Computers and Peripherals: For optimal safety and performance, it is important to follow these guidelines when connecting computers and peripherals to electrical points:

- Connect all devices to the electrical point using a UPS.
- Do not switch off the power supply to the UPS as the battery requires continuous power to recharge.

- Make sure the UPS system is connected to an electrical point with proper earthing.
- Ensure that the electrical wiring at the point of connection is properly laid.

e) Network Cable Connection

To ensure smooth network communication when connecting a computer to the network, please keep in mind the following:

- The network cable used to connect the computer should be kept away from any electrical or electronic equipment, as these may cause interference.
- Additionally, do not share the power supply used for the computer and its peripherals with any other electrical or electronic equipment.

f) File and Print Sharing Facilities

Some guidelines to follow when setting up file and print sharing facilities on a computer over a network:

- Install these facilities only if they are absolutely necessary.
- If files are shared through the network, protect them with a password and set them to read-only access.

g) The Institute's Maintenance of Computer Systems

The Computer Centre is responsible for addressing any maintenance-related complaints for all computers that were centrally purchased by the institute and distributed to various locations. h) Non - compliance

Non-compliance with the computer hardware installation policy by VTM faculty, staff, and students can pose a risk to the network and result in damaged or lost files, inoperable computers, and loss of productivity. Additionally, non-compliant computers can negatively affect other individuals, groups, departments, and even the entire institute. Therefore, it is essential to bring all non-compliant computers into compliance as soon as possible to mitigate any potential adverse effects.

i) Computer Centre Interface

If the Computer Centre discovers a non-compliant computer that is affecting the network, they will contact the individual responsible for the system and request that it be brought into compliance. The notification will be sent via email or phone, and the individual user must follow up to ensure that their computer gains the necessary compliance. The Computer Centre will offer guidance as needed to assist the individual in becoming compliant.

4. Software Installation and Licensing Policy

When purchasing computer systems, individual department/cells must ensure that they are equipped with all licensed software, including the operating system, antivirus software, and necessary applications. The institute's IT policy prohibits the installation of any pirated or unauthorised software on computers owned by the institute or connected to the campus network, in accordance with anti-piracy laws. If any such instances are discovered, the Institute will hold the department/individual personally responsible for any pirated software installed on computers located in their department or personal rooms.

a) Operating System Updates and Maintenance

To ensure optimal performance and security of their computer systems, individual users are responsible for updating their operating system through the internet, regardless of their service packs, or parches. This is especially crucial for all Microsoft Windows-based computers, including PCs and servers. Regular updates help fix bugs and vulnerabilities in the operating system that are periodically detected by Microsoft, for which patches and service packs are provided to address them.

b) Updating Antivirus Software for Computer Systems"

To ensure optimal performance and security of computer systems, it is important to update antivirus software regularly. Users should make sure that their respective computer systems have current antivirus software installed and that it is updated on a regular basis to protect against new threats. The primary user of a computer system is responsible for ensuring compliance with this policy.

It is essential to note that any antivirus software that is not updated or renewed after its warranty period is of no practical use. Therefore, it is the responsibility of individual users to ensure that their antivirus software is up to date and properly maintained. If these responsibilities exceed the end user's technical skills, the end-user is responsible for seeking assistance from the Computer Centre.

c) Regular Backup of Data

It is important for individual users to perform regular backups of their vital data to prevent loss in case of virus infections or other issues that may destroy data on their computer. Ideally, at the time of OS installation, the computer's hard disk should be partitioned into multiple volumes, with the OS and other software on the C drive and user's data files on other drives such as D and E. This way, if only the C volume gets corrupted due to a virus problem, formatting only that volume will protect against data loss.

However, this is not a fool proof solution, and users should also keep their valuable data on other storage devices such as CDs, DVDs, pen drives, or external hard drives. Without proper backups, recovering destroyed files may be impossible. It is the responsibility of the individual user to regularly backup their data to prevent loss.

d) Noncompliance

Non-compliance with this computer security policy by VTM faculty, staff, and students puts themselves and others at risk of virus infections, leading to damaged or lost files, inoperable computers, loss of productivity, and the spread of infection to others. It also increases the risk of confidential data being revealed to unauthorized persons. Furthermore, non-compliant computers can have significant adverse effects on other individuals, groups, departments, or even the whole institute. Therefore, it is crucial to ensure all computers are compliant as soon as possible.

e) Computer Centre Interface

If Computer Centre detects a non-compliant computer, they will inform the responsible individual and request them to bring it into compliance. The notification will be sent through email or phone. The user should follow up on the notification to ensure that their computer becomes compliant. The Computer Centre will provide assistance if needed to help the user become compliant.

5. Network (Intranet & Internet) Use Policy

The institute's IT policy giverns network connectivity, including authenticated network access connections or WiFi. The Computer Centre is responsible for maintaining and supporting the network, except for local applications. If there are any issues with the institute's network, they should be reported to the Computer Centre.

a) IP Address Allocation

All computers (PCs/Servers) connecting to the institute network must be assigned an IP address by the Computer Centre following a systematic approach that allocates a range of IP addresses to each building/V LAN. This ensures that any computer connecting to the network from a building is allocated an IP address only from that address pool. Additionally, each network port in a room where a computer is connected is internally bound to the assigned IP address, preventing unauthorized usage of the IP address from any other location. When a new computer is installed, the user must obtain an IP address allocation from the Computer Centre or respective department. It is essential to note that IP addresses allocated to a particular computer should not be used on any other computer, even if that computer belongs to the same individual and connects to the same port, as IP addresses are assigned to computers and not to ports.

b) DHCP and Proxy Configuration by Individual Departments /Cells/ Users

To ensure compliance with the IP address allocation policy of the institute, the use of any computer as a DHCP server to connect to more computers via an individual switch/hub and distribute IP addresses (public or private) should be strictly avoided at end-user locations. Additionally, configuration of proxy servers should also be avoided to prevent interference with the services provided by the Computer Centre. Failure to comply with the IP address allocation policy will result in the disconnection of the port to which the non-compliant computer is connected. Reconnection will only be granted upon receiving written assurance of compliance from the concerned department or user.

c) Running Network Services on the Servers

Departments and individuals using the institute LAN to run server software, such as HTTP/Web server, SMTP server, FTP server, must notify the Computer Centre in writing and comply with the institute's IT policy for running such services. Failure to comply is a violation of the policy and may result in disconnection from the Network. The Computer Centre is not responsible for the content of any machines connected to the Network, whether they are Institute or personal property. If potentially damaging software is found on a client machine, it may be disconnected, and a client may also be disconnected if their activity affects the Network's performance. Institute network and computer resources are not for personal or commercial use. The Computer Centre will monitor Network traffic for security and performance reasons, and impersonating an authorized user while connecting to the Network is a violation that will result in disconnection.

d) Dial-up/Broadband Connections

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

e) Wireless Local Area Networks

This policy applies in its entirety to all departments or wireless local area networks. Each wireless access point must be registered with the Computer Centre, including Point of Contact (POC) information. Unrestricted access is not allowed; network access must be restricted either via authentication or MAC/IP address restrictions, and passwords and data must be encrypted. If an individual department wishes to have an inter-building wireless network, permission must be obtained from the institute authorities, with the application routed through the In Charge of the Computer Centre.

6. Email Account Use Policy

To ensure efficient communication of important information to all members of the institute, including faculty, staff, students, and administrators, it is recommended that the institute's email services be utilized for formal communication and academic and official purposes. This will facilitate the distribution of messages and documents to the campus community and beyond. Formal institute communications include official notices from the institute such as human resources information, policy messages, general institute messages, and official announcements. It is important to keep your email address active to receive these notices. Staff and faculty can access the email facility by logging onto https://gmail.com with their user ID and password. To obtain an institute email account, users can contact the Computer Centre and submit an application in a prescribed proforma to receive an email account and default password.

By using the email facility, users agree to follow certain policies. The facility should primarily be used for academic and official purposes and to a limited extent for personal use. Using the facility for illegal or commercial purposes, such as unlicensed and illegal copying or distribution of software, sending unsolicited bulk email messages, or generating threatening, harassing, abusive, obscene, or fraudulent messages or images, is a direct violation of the institute's IT policy and may result in withdrawal of the facility. Users should not open any mail or attachment from unknown or suspicious sources and should confirm the authenticity of any suspicious attachments even if they come from a known source. Users should not share their email account with others and should promptly close any email accounts left open on shared computers without peeping into their contents. Impersonating email accounts of others is a serious offense under the institute's IT security policy. Ultimately, it is each individual's responsibility to keep their email account free from violations of the institute's email usage policy.

These policies apply not only to the institute's email services but also to email services provided by other sources such as Hotmail.com and Yahoo.com as long as they are being used from the institute's campus network or by using the resources provided by the institute for official use even from outside

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

7. Web Site Hosting Policy

a) The official web site of the institute, which can be accessed at http://, is currently maintained by the Computer Centre. Departments, Cells, and central facilities may have their own pages on the site.

b) Faculty members may request to have their personal pages linked to the official web site of the institute by sending a written request or email to the Computer Centre. However, any illegal or improper usage will result in the termination of the hyperlink. The contents of personal pages must comply with all applicable laws and regulations, including export laws, copyright and trademark laws, and government laws. Personal pages should not be used for commercial purposes or political lobbying, nor should they host pages for other individuals or groups. Faculty members should explicitly state that any views expressed on their personal pages are their own and not those of the institute.

c) Departments, Cells, and individuals are responsible for updating their own web pages and must send updated information to the Computer Centre on a regular basis.

8. Institute Database Use Policy

The following policy pertains to the databases maintained by VTM, which are crucial resources for providing valuable information. While data may not always be confidential, its use must be safeguarded. VTM has specific policies governing the creation and access of databases, as well as a more comprehensive policy on data access. Together, these policies provide guidance on how to access and utilize this institute resource. VTM is the owner of all institutional data generated within the institute. Certain officers in each department may be responsible for data administration activities. The Management Information System of VTM includes the following components: Employee Information Management System, Student Information Management System, Financial Information Management System, Library Management System, and Document Management & Information Retrieval System. To ensure the proper use of data by departments, cells, and administrative departments, the following general policy guidelines and parameters must be followed:

1. Institute data policies prohibit the distribution of data that can identify individuals outside of the institute.
2. Data from the institute's database, including data collected by departments, faculty, and staff, is intended solely for internal use within the institute.
3. Data resources required to carry out official responsibilities/rights are determined by one's role and function. The institute provides access to information based on these responsibilities/rights.
4. Data containing personal information must not be disseminated in any form to external individuals or agencies, including government agencies and surveys. All such requests must be directed to the Office.
5. All requests for information from the courts, attorneys, etc., should be handled by the Office, and departments must not respond, even if subpoenaed. All requests from law enforcement agencies must also be directed to the Office.
6. Tampering with the database by departments or individual users is a violation of the IT policy. Such actions include modifying/deleting data items or software components through illegal access methods or with ulterior motives, intentionally causing a database/hardware/system software crash, or attempting to breach the security of database servers. Any member who engages in such activities will face disciplinary action by the institute, and law enforcement agencies may become involved if the matter involves illegal action.

9. Responsibilities of Computer

Campus Network Backbone Operations:

a) The Computer Centre administers, maintains, and controls the campus network backbone and its active components to ensure that service levels are maintained as required by the Institute Departments and hostels served by the campus network backbone within operational best practices.

b) The Computer Centre is responsible for maintaining the institute-owned computer systems and peripherals that are under warranty or out of warranty.

c) Computer Centre receives complaints from users regarding maintenance problems with the computer systems or peripherals that are under its maintenance. The designated person in Computer Centre coordinates with service engineers of respective brands of the computer systems to resolve the problem within a reasonable time limit. Complaints related to networks can also be made through email or phone, and Computer Centre coordinates with the internal technical team or service engineers of network hardware to resolve the issue.

d) Computer Centre is responsible for solving hardware-related problems, operating systemrelated problems, application software-related problems legally purchased by the institute and loaded by the company, and network-related problems or services related to the network.

e) Computer Centre or its service engineers should not encourage the installation of any unauthorized software on the computer systems of users.

f) Physical connectivity of campus buildings already connected to the campus network backbone and physical demarcation of newly constructed buildings to the backbone are the responsibility of Computer Centre. Computer Centre consults with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.

g) Major network expansion is the responsibility of Computer Centre, which reviews the existing networking facilities every three to five years to determine possible expansion.

h) Computer Centre considers providing network connection through wireless connectivity in locations where access through Fibre Optic/UTP cables is not feasible. Computer Centre is authorized to consider the applications of Departments or divisions for the use of radio spectrum from Computer Centre prior to implementation of wireless local area networks. Computer Centre is also authorized to restrict network access to the Cells, departments, or hostels through wireless local area networks either via authentication or MAC/IP address restrictions.

i) Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

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

k) Computer Centre provides Net Access IDs and email accounts to individual users upon receiving requests from the individuals on prescribed proforma to enable them to use the campus-wide network and email facilities provided by the institute. l) Disconnect Authorization

Computer Centre has the authority to disconnect any Department, or cell from the campus network backbone if their traffic violates the policies set forth in this document or any other network-related policy. If a department, cell, or hostel machine or network causes severe degradation to the normal flow of traffic, Computer Centre will strive to solve the issue in a way that minimizes the negative impact on other members of the network. In the event of disconnection, Computer Centre will provide the criteria that must be met to regain network access.

10. Responsibilities of Department

a) User Account:

- A legitimate user account (Net Access/Captive Portal ID) is required for entities to connect to the Institute network and verify affiliation with the Institute.

- The user account is provided by Computer Centre after submission of the application form.
- The user is personally responsible for all actions performed using the account and is advised to take measures to prevent unauthorized use.
- Users must know and follow the IT policy of the Institute.

b) Supply of Information by Department or Cell for Publishing on/Updating the VTM Web Site:

- Departments or Cells must provide updated information periodically to Computer Centre.
- Hardcopy or softcopy should be sent to Computer Centre for advertisements/tender notifications published in newspapers or events organized by departments or cells.
- Links to web pages can be provided upon written requests.
- Soft copy of the contents and necessary content pages (and images, if any) should be provided in advance.

c) Security:

- Departments must abide by the Network Usage Policy under the Institute IT Security Policy.
- Network security incidents are resolved by coordination with the POC in the originating department.
- If a POC is not available, the offending computer is disconnected until compliance is met.

d) Preservation of Network Equipment and Accessories:

- Routers, switches, cabling, connecting inlets, racks, and batteries are the property of the Institute and maintained by Computer Centre and respective departments.
- Tampering with these items violates the IT policy.

e) Additions to the Existing Network:

- Adherence to the Institute network policy is required for any addition to the network.
- Prior permission from the competent authority and information to Computer Centre is necessary.
- The internal network cabling should be CAT 6 UTP and follow structured cabling standards.
- Only managed switches should be used, and the hardware maintenance of the network segment is the responsibility of the department/individual member.
- Managed switches should be web-enabled, and IP address allocation can be obtained from Computer Centre on request.

f) Campus Network Services Use Agreement:

- All members seeking network access must read the “Campus Network Services Use Agreement” found on the Institute website.
- All provisions of this policy are considered a part of the Agreement, and users are responsible for being aware of the IT policy.

g) Enforcement:

- The Computer Centre enforces the Network Use Policy by conducting regular scans of the Institute's network. Non-compliance with the policy may lead to the suspension of service for the person responsible for the violation.

11. Responsibilities of the Administrative Department

The Computer Centre requires up-to-date information from various Administrative Departments in order to provide network and IT facilities to new members of the institute and withdraw facilities from those who are leaving. Additionally, the Computer Centre needs this information to keep the VTM website current with its content. This information could include details about new appointments, termination of services, new enrolments, expiry of studentship, removal of names from the rolls, important events/achievements, rules, procedures, and facilities.

Departments running application or information servers are responsible for maintaining their own servers. To ensure proper server maintenance, they should follow these guidelines:

1. Obtain an IP address from the Computer Centre for the server.
2. Add the server hostname to the DNS server for IP address resolution.
3. Enable only the essential services required for the intended purpose of the server.
4. Protect the server against virus attacks and intrusions by installing appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam, etc.
5. Regularly update the operating system and security software.

12. Guidelines for Desktop Users

These guidelines apply to all members of the VTM Network User, as the Institute IT Policy has released recommendations to improve desktop security in response to increasing hacker activity on campus. The following recommendations should be followed:

1. Install the latest version of antivirus on all desktop computers and keep the setting that schedules regular updates of virus definitions from the central server.
2. Apply all operating system updates and patches when installing a desktop computer, and regularly apply updates and patches to maintain security. The frequency of updates should balance productivity loss and security needs, and security policies should be set at the server level and applied to the desktop machines whenever possible.
3. Use a difficult-to-break password.

4. Disable the guest account.
5. Computer Centre also suggests implementing a regular backup strategy to reduce the impact of machine loss due to virus infection or hacker compromise. Daily and/or weekly backup of data is recommended, as following all the procedures listed above does not guarantee complete protection against cyber attacks

13. Video Surveillance Policy

The institute has implemented a system consisting of fixed position cameras, monitors, digital video recorders, storage, and public information signs. The cameras will be strategically placed throughout the campus, mainly at the entrances and exits of buildings and sites. These cameras will not be hidden and will not be allowed to focus on private residential areas. Signs will be prominently displayed to inform individuals that CCTV cameras are in use. Although the system aims to be as effective as possible, it cannot guarantee the detection of every incident within the coverage area.

The primary purpose of the system is to reduce crime, protect institute property, and ensure the safety of staff, students, and visitors while respecting their privacy. The system will achieve these goals by deterring potential criminals, assisting in crime prevention and detection, and aiding in the identification, apprehension, and prosecution of offenders. Additionally, it will help identify any activities or events that may warrant disciplinary proceedings against staff or students and provide evidence to managers or individuals facing disciplinary or other action.

The institute acknowledges that some individuals may have concerns or complaints about the system's operation, and any complaints should be directed to the Computer Centre. Individuals may request CCTV footage from the institute upon completing a prescribed proforma.

14. Web Application Filter

Default Block Category in Firewall

- Weapon
- Phishing and fraud
- Militancy and Extremist
- Gambling
- Pro-Suicide and self-Harm
- Criminal Activity
- Intellectual Piracy
- Hunting and Fishing
- Legal highs
- Controlled substances
- Anonymizers
- Sexually Explicit

- Nudity
- Advertisement

Campus Network Services Use Agreement

Before applying for a user account or email account, it is important to read the IT policies and guidelines of VTM. By signing the application form, the user agrees to comply with these policies and failure to do so may result in account/IP address termination. A Net Access ID is a combination of a username and password used to gain access to Institute computer systems, services, campus networks, and the internet.

The policies are summarized as follows:

a) Accounts and Passwords: Users must not share their Net Access ID or password with anyone, use it for educational/official purposes only, and will not be allowed more than one ID at a time. Computer Centre may delete accounts of those who leave the Institute.

b) Limitations on the use of resources: Computer Centre reserves the right to close the Net Access ID of any user deemed to be using excessive storage space or limiting computing resources for other users.

c) Data Backup, Security, and Disclaimer: The User is responsible for backing up files and Computer Centre is not liable for loss or corruption of data or security/privacy of electronic messages. The User is held liable for any improper use of equipment or software.

d) Account Termination and Appeal Process: Accounts may be terminated with little or no notice for inappropriate use of computing and network resources. Users may approach the In Charge, Computer Centre, to justify their actions if they feel such termination is unwarranted.

Users can obtain a detailed document of these policies from the website or various intranet servers. It is important to understand and follow these policies to avoid account termination or other consequences.

Principal
V.T.M.N.S.S. College
Dhanuvachapuram

V.T.M.N.S.S. COLLEGE
DHANUVACHAPURAM P.O.