

4.3.2

INFORMATION TECHNOLOGY POLICY



VIKRAMA SIMHAPURI UNIVERSITY
NELLORE – 524324
ANDHRA PRADESH, INDIA

CONTENTS

1	Introduction
2	Scope
3	Objective
4	Roles and Responsibilities
5	Acceptable Use
6	Access to the Network
7	Monitoring and Privacy
8	E-Mail Access
9	Access To Social Media Sites
10	Security Incident Management Process
11	Intellectual Property
12	Enforcement
13	Deactivation
14	Audit of Network Infrastructure
15	Hardware Installation
16	Software Installation and Licensing
17	Use of IT Devices
18	Network (Intranet & Internet) Usage
19	Email Account Usage
20	Revisions to Policy


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324

1 INTRODUCTION

- a. Vikrama Simhapuri University (VSU), Nellore provides IT resources to its employees, students and other stakeholder to enhance their efficiency and productivity.
- b. Support the teaching & learning, research, and administrative activities to enhance the efficiency and productivity of the employees. **IT Resources** includes desktop computers, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.
- c. Misuse of these resources can result in unwanted risk and liabilities for the university. It is, therefore, expected that these resources are used primarily for university related purposes and in a lawful and ethical way.

2 SCOPE

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/ users/ entities.

3 OBJECTIVE

- a. The objective of this policy is to ensure proper access to and usage of Government's IT resources and prevent their misuse by the users. Use of resources governed by the by this policy.
- b. Maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- c. Establishes strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.

4 ROLES AND RESPONSIBILITIES

The following roles and responsibilities:

- 1) Computer Centre shall implement appropriate controls to ensure compliance with this policy by their users. The centre shall be the primary Implementing Agency and shall provide necessary support in this regard.
- 2) Computer Centre shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.
- 3) Use VSU's IT resources for those activities that are consistent with the academic, research and public service mission of the University and are not "Prohibited Activities".
- 4) All users shall comply with existing national, state and other applicable laws.
- 5) Abide by existing telecommunications and networking laws and regulations.
- 6) Follow copyright laws regarding protected commercial software or intellectual property.
- 7) As a member of the University community, VSU provides use of scholarly and/or work-related tools, including access to the Library, certain computer

systems, servers, software and databases and the Internet. It is expected from University Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of nonelectronic communication.

- 8) Users of VSU shall not install any network/security device on the network without consultation with the IA.
- 9) It is responsibility of the University Community to know the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
- 10) As a representative of the VSU community, each individual is expected to respect and uphold the University's good name and reputation in any activities related to use of ICT communications within and outside the university.
- 11) Competent Authority should ensure proper dissemination of this policy.

5 ACCEPTABLE USE

- A. An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.
- B. A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the University for all use of such resources. As an authorized VSU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of VSU or a personal computer that is connected to the VSU campus wide Local Area Network (LAN).
- C. The university is bound by its End User License Agreement (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.
- D. Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
- E. No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- F. Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.
- G. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

6 ACCESS TO THE NETWORK

A. Access to Internet and Intranet

- a. A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus wide LAN.


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324

- b. VSU shall maintain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.
- c. Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

B. Access to VSU's Wireless Networks

For connecting to a VSU's wireless network, user shall ensure the following:

- a. A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the VSU's wireless network.
- b. Wireless client systems and wireless devices shall not be allowed to connect to the VSU's wireless access points without due authentication.
- c. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

C. Filtering and blocking of sites

- a. Computer Centre or any other Implementing Agency (IA) may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
- b. Computer Centre or any other Implementing Agency (IA) may also block content which, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.

7 MONITORING AND PRIVACY

- A. All users are expected to respect the privacy and personal rights of others.
- B. Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
- C. While the University does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.
- D. Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.
- E. IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
- F. IA may monitor user's online activities on University network, subject to such Standard Operating Procedures of Government of India norms.


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324

8 **E-MAIL ACCESS**

- A. E-mail service authorized by VSU and implemented by the Computer Centre shall only be used for all official correspondence.
- B. More details in this regard are provided in the "E-mail Usage Policy of VSU".

9 **ACCESS TO SOCIAL MEDIA SITES**

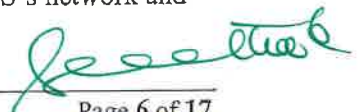
- A. Use of social networking sites by VSU users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".
- B. User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.
- C. User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
- D. User shall report any suspicious incident as soon as possible to the competent authority.
- E. User shall always use high security settings on social networking sites
- F. User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
- G. User shall not disclose or use any confidential information obtained in their capacity as an employee of the university.
- H. User shall not make any comment or post any material that might otherwise cause damage to VSU's reputation.

10 **SECURITY INCIDENT MANAGEMENT PROCESS**

- A. A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of University's data.
- B. IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the university.
- C. Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.
- D. Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.
- E. IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

11 **INTELLECTUAL PROPERTY**

Material accessible through the VSU's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use VUS's network and



Page 6 of 17

RÉGISTRAR

VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324.

resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights

12 **ENFORCEMENT**

- A. This policy is applicable to all the users of VSU as specified in **Section 2** of this document. It is mandatory for all users to adhere to the provisions of this policy.
- B. Each entity of VSU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.

13 **DEACTIVATION**

- A. In case of any threat to security of VSU's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the Computer Centre.
- B. Subsequent to such deactivation, the concerned user and the competent authority of the university shall be informed.

14 **AUDIT OF NETWORK INFRASTRUCTURE**

The security audit of the network infrastructure shall be conducted periodically by an organization approved by the university

15 **HARDWARE INSTALLATION**

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

A. Who is Primary User

An individual 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

B. What are End User Computer Systems

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

C. Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

D. Power Connection to Computers and Peripherals


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324

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, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

E. Network 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.

F. 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

G. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the University attached with Computer Centre will attend to the complaints related to any maintenance related problems

16 SOFTWARE INSTALLATION AND LICENSING

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

A. Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so.

University 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

B. Use of software on Desktop systems

- a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.
- b. Any software installed should be for activities of the university only.

C. Antivirus Software and its updating

Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

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

D. Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

17 USE OF IT DEVICES

IT devices issued by a user shall be primarily used for academic, research and any other university related purposes and in a lawful and ethical way and shall be governed by the practices defined in this Section. Use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners as

A. Desktop Devices

a. Use and Ownership

Desktops shall normally be used only for transacting university's works. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

b. Security and Proprietary Information

- i. User shall take prior approval from the Computer Centre to connect any access device to the network.
- ii. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy of the application.
- iii. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.
- iv. Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.
- v. User shall report any loss of data or accessories to the competent authority.
- vi. User shall obtain authorization from the competent authority before taking any issued desktop outside the premises of the university.
- vii. Users shall properly shut down the systems before leaving the office/ department.



REGISTRAR

VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324

- viii. Users shall abide by instructions or procedures as directed by the Computer Centre from time to time.
- ix. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the Computer Centre for corrective action.

B. Sharing of data

Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which are used for identification and authorization purposes.

C. Use of Portable Devices

Use of the **Portable Devices** shall be governed by the following:

- a. User shall be held responsible for any unauthorized usage of their issued access device by a third party.
- b. Users shall keep the issued devices with them at all times or store them in a secured location when not in use.
- c. User should not leave the devices unattended in public locations (e.g. classrooms, meeting rooms, restaurants etc.).
- d. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.
- e. The Computer Centre shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.
- f. Users shall wipe or securely delete data from the device before returning/ disposing it off.
- g. Lost, stolen, or misplaced devices shall be immediately reported to the Computer Centre/ and the competent authority.
- h. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

18 NETWORK (INTRANET & INTERNET) USAGE

Network connectivity provided through the University, referred to hereafter as "the Network", an authenticated network access connection is governed under the University IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network. Problems within the University's network should be reported to the Computer Centre.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the Computer Centre. Following a systematic approach, the range of IP addresses that will be allocated. Any device connected to

the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location. As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.

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

B. DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered an absolute violation of IP address allocation policy of the university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the services run by the Computer Centre.

Even configuration of any computer with an additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Non-compliance to the IP address allocation policy will result in disconnecting the port from the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user

C. Running Network Services on the Servers

- a. Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Centre in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.
- b. The Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.
- c. Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

- d. Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.
- e. Network traffic will be monitored for security and for performance reasons at the Computer Centre.
- f. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection

D. Internet Bandwidth obtained by Other Departments

- a. Internet bandwidth acquired by any department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource.
- b. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.
- c. IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to Computer Centre.
- d. Non-compliance to this policy will be direct violation of the university's IT security policy.

19 EMAIL ACCOUNT USAGE POLICY

The University provides official email accounts with **vsu.ac.in** domain access privileges to its users for effective information dissemination and formal communication. Staff and faculty may use the email facility by logging on to **GSuite Mail Service** with their given User ID and Password. For obtaining the university's email account, users may contact Computer Centre for an email account and default password by submitting an application in a **prescribed proforma as given in the ANNEXURE -1.**

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

- a. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- b. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy. The illegal use includes, but is not limited to, the


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324.

unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages, generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

- c. While sending large attachments to others, user should make sure that the recipient has an email facility that allows him to receive such large attachments.
- d. User should keep the mailbox used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- e. User should not open any mail or attachment that is from an unknown and suspicious source. Even if it is from a known source, and if it contains any attachment that is of suspicious in nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
- f. User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- g. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
- h. 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.
- i. Impersonating the email account of others will be taken as a serious offence under the IT security policy.
- j. It is ultimately each individual's responsibility to keep their email account free from violations of university's email usage policy.
- k. All the mails detected as spam mails go into the SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.

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

20 REVISIONS TO POLICY

The University reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the University website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy

CONTACT ADDRESS

If you have any queries in relation to this policy, please contact:

COMPUTER CENTRE
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324
ANDHRA PRADESH, INDIA
Phone:
Email: computercenter@vsu.ac.in


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324

ANNEXURE – I

REQUISITION FORM FOR OFFICIAL E-MAIL ID FOR STAFF

1.	Name	:	
2.	Father's Name	:	
3.	Gender	:	
4.	Department	:	
5.	Date of Joining	:	
6.	Date of Birth	:	
7.	Email address	:	
8.	Mobile Number	:	
DECLARATION			
I am hereby declare that the above details are true for the best of my knowledge.			
Date			
Place			Signature of the Staff


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324.

ANNEXURE – II

WI-FI ACCESS REQUISITION FORM FOR STUDENTS

9.	Name	:	
10.	Admission Number	:	
11.	Hall Ticket Number	:	
12.	Programme	:	
13.	Year of Admission	:	
14.	Department	:	
15.	Year	:	
16.	Father's Name	:	
17.	Gender	:	
18.	Date of Birth	:	
19.	Email address	:	
20.	Mobile Number	:	
DECLARATION			
I am hereby declare that the above details are true for the best of my knowledge.			
Date			
Place			Signature of the Student


 REGISTRAR
 VIKRAMA SIMHAPURI UNIVERSITY
 NELLORE - 524 324.

ANNEXURE - III

WI-FI ACCESS REQUISITION FORM FOR EMPLOYEES

1	Name	:	
2	Father's Name	:	
3	Gender	:	
4	Date of Birth	:	
5	Department/ Section	:	
6	Designation	:	
7	Email address	:	
8	Mobile Number	:	
DECLARATION			
I am hereby declare that the above details are true for the best of my knowledge.			
Date			
Place			Signature of Employee


REGISTRAR
VIKRAMA SIMHAPURI UNIVERSITY
NELLORE - 524 324.