VISHNU
UNIVERSAL LEARNING

Vishnu Institute of Technology

Bhimavaram 534202

West Godavari District, Andhra Pradesh

IT Policy

VISHNU INSTITUTE OF TECHNOLOGY (AUTONOMOUS) ★ BHIMAVARAM PIN:534 202 ★ VISHNUPUR-KOVVADA

PRINCIPAL
Vishnu Institute of Technology
(Autonomous)
Vishnupur, BHIMAVARAM-534 202

Contents

1 INTRODUCTION

The VITB Information Technology (IT) Policy sets forth the central policies that govern the responsible usage of all users of the VITB's information technology resources. This comprises the IT facilities allocated centrally or by individual departments. Every member of the VITB is expected to be familiar with and adhere to this policy. Users of the campus network and computer resources are responsible to properly use and protect information resources and to respect the rights of others.

2 OBJECTIVE

The objective of this policy is to ensure proper access to and usage of VITB's IT resources and prevent their misuse by the users. Use of resources provided by VITB implies the user's agreement to be governed by this policy.

- VITB IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the VITB on the campus.
- This policy establishes college-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the VITB.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

3 POLICY FOR PURCHASING SOFTWARE

This policy provides guidelines for the purchase of software for the institution to ensure that all software used by the institution is appropriate, value for money and where applicable integrates with other technology for the institution. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

The following are the steps for software purchasing

- ✓ Request for Software
- ✓ All software's must be approved prior to the purchase of software's.
- ✓ Purchase of software

The purchase of all software must adhere to this policy. All purchases of software must be compatible with the institution's server and/or hardware system.

Obtaining open source software

Open source software can be obtained without payment and usually downloaded directly from the internet. In the event that open source software is required, approval from principal must be obtained prior to the download or use of such software. All open source must be compatible with the institution's hardware and software systems.

4 POLICY FOR PURCHASING HARDWARE

This policy provides guidelines for the purchase of hardware for the institution to ensure that all hardware used by the institution is appropriate, value for money and where applicable integrates with other technology for the institution. All hardware's must be approved prior to the purchase of hardware's and then purchase of hardware's will be done

5 POLICY FOR HARDWARE INSTALLATION

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

5.1 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.

5.2 What are End User Computer Systems

Apart from the client PCs used by the users, VITB will consider servers not directly administered by internet unit, 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 internet unit, are still considered under this policy as "end-users" computers.

5.3 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. Such maintenance should include OS re-installation and checking virus related problems also.

5.4 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 earthling and have properly laid electrical wiring.

5.5 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.

5.6 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.

5.7 Maintenance of Computer Systems provided by VITB

Computer Maintenance Cell will attend to the complaints related to maintenance of all the computers that were purchased by the VITB.

6 POLICY FOR SOFTWARE INSTALLATION

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

6.1 Operating System and its Updating

- Individual users should make sure that respective computer systems have their OS updated in respective of their service packs through Internet. This is particularly important for all MS Windows based computers. 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 service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.
- College 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.

6.2 Antivirus Software and its updating

- Computer systems used in the college 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.

6.3 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.

7 POLICY FOR USE OF SOFTWARE

Only software purchased in accordance with the getting software policy is to be used within the institution. Prior to the use of any software, the employee will receive

instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees will receive training for all new software's. This includes new employees to be trained to use existing software appropriately. Employees are prohibited from bringing software from home and loading it onto the institution's computer hardware. The unauthorized duplicating, acquiring or use of software copies is also prohibited. Further unless approval, software cannot be taken home and loaded on an employees' home computer.

8 POLICY FOR USE OF HARDWARE

Only Hardware purchased in accordance with the getting hardware policy is to be used within the institution. Prior to the use of any hardware, the employee will receive instructions on any licensing agreements relating to the hardware, including any restrictions on use of the hardware. All employees will receive training for all new hardware. This includes new employees to be trained to use existing hardware appropriately. Employees are prohibited from bringing hardware from home. Further unless approval, hardware cannot be taken home and use it.

9 POLICY FOR IT ASSET MANAGEMENT

Asset Management: The institute shall lay down processes for the management of hardware and software assets that facilitates the usage of IT resources in the business. This shall include procedures for managing the purchase, deployment, maintenance, utilization, energy audit, and disposal of software and hardware applications within the business.

Copying and Distribution: The institute shall ensure that there is no violation in the copying and distribution of proprietary and licensed software's.

Risks: The business shall emphasize on managing the risks involved for the usage of IT resources. This shall include standard procedures for identification, minimization and monitoring of risk impact by preventive and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate internet connectivity for a fail-safe internet access.

Open Source Asset: The institute shall endeavour towards the promotion and effective usage of open source software's.

The Academic Advisory Committee of VITB periodically reviews the IT infrastructure and recommends the necessary up-gradation as per the requirements. The IT infrastructure strategies are developed as per the guidelines of AICTE & University from time to time.

10 POLICY FOR INFORMATION SECURITY

VITB provides necessary and sufficient education and training to the users of the computing and networking recourses so that they can understand the importance of information security in general and exercise appropriate care while handling confidential information in particular. To achieve this, for example, the proxy servers are configured to block spam messages and malicious attachments.

11 POLICY FOR NETWORK SECURITY

VITB follows appropriate safety standards for protecting information against generic threats posed by computer hackers and intruders. Remote access to the computing facilities is limited only to authentic users. Appropriate Firewall settings are done and used for securing data transmission and restricting intrusion.

12 POLICY FOR USE OF EMAIL ACCOUNT

VITB provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email with VITB's domain.

In an effort to increase the efficient distribution of critical information to all faculty, students, and the Institute's administrators, it is recommended to utilize the Institute's e-mail services, for formal Institute communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it

regularly. Staff and students may use the email facility by logging on to http://gmail.com with their User ID and password. For obtaining the Institute's email account, user may contact dean statutory bodies for email account and default password by submitting an application in a prescribed proforma.

13 POLICY FOR BRING YOUR OWN DEVICE

This policy provides guidelines for the use of personally owned laptops, notebooks, smart phones and tablets for institution purposes. All staff or students who use or access technology equipment and/or services are bound by the conditions of this Policy. Employees or students when using personal devices for institution use will have to register the device with the institution. Each employee or student who utilizes personal devices agrees not to download or transfer institution or personal sensitive information to the device.

14 POLICY FOR IT SERVICE MANAGEMENT

VITB adopts best practices for scalable and sustainable implementation of its IT services. It provides computing and networking services such as desktops, laptops, Wi-Fi based Internet to all departments, library and offices. Appropriate standards are followed for selection, purchase, setup and maintenance of all computing and networking equipment. In addition the industry recommended protocols to securely store and transmitting the data are followed.

15 POLICY FOR DISPOSAL OF IT EQUIPMENT

The disposal of IT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the institute.