VIGNAN'S INSTITUTE OF INFORMATION TECHNOLOGY
(AUTONOMOUS)
(Approved by AICTE - New Delhi & Affiliated to JNTUK, Kakinada)
Beside VSEZ, Duvvada, Vadlapudi Post, Gajuwaka, Visakhapatnam - 530 049.

Information Technology Services Policy and Procedure Manual

(Version -2)

Prepared by

IT Infrastructure Development Committee

Version-1 dated, 01-06-2010

Version-2 dated, 14-08-2018

Approved by

Governing Body

Information Technology Services Policy and Procedure Manual

(Version -2)

Table of Contents

Introduction

IT policy ensures to maintain a secure, legal and appropriate use of IT infrastructure for free flow of information and maintenance of confidentiality and integrity of the same. Access to information assets are created, managed, and regulated with the help of IT infrastructure. The VIIT(A) IT Services Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the Institute which must be followed by all staff and students. It also provides guidelines to administer these policies, with the correct procedure to follow. All IT policies updated and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

The main aspects of the IT policy are to

1) Develop IT infrastructure and services for laboratories, research, faculty, staff and students on 24 x 7 basis. and automation of information management systems
2) Regular maintenance and up gradation of IT systems in line with their useful life and their obsolescence.
3) Budget provisions to expand ever growing digital systems and services.
4) Digitization of general information and learning resources and access facility through internet and intranet.
5) Maintenance Firewall and Antivirus for Systems security and Cyber security.
6) Maintenance of critical data and necessary backups.
7) Maintenance of separate LAN for examinations systems for additional security.
8) Use and promote open-source software and disposal of e-waste.

These policies and procedures apply to all employees and students.

1. Technology Hardware Purchasing Policy

Computer hardware refers whole or to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

1.1 Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the institute to ensure that all hardware technology for the institute is appropriate and value for money

1.2 Procedures

Purchase of Hardware Guidance: The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy.

- **Purchasing desktop computer systems**

  The desktop computer systems must be purchased as standard desktop system bundle and must be from reputed companies such as HP, Dell, Lenovo etc..}.

The desktop computer system bundle must include:

- Desktop tower
- Monitor screen sizes
- Keyboard and mouse
- Windows OS

The minimum capacity of the desktop must be:

- 2 GHz–Gigahertz processor
- 2GB RAM
- 3 USB ports

Any change from the above requirements must be verified by system administrator and authorized by Dean Infrastructure. All purchases of desktops must be supported by 3 Years warranty. All purchases for desktops must be in line with the purchasing policy of the Institute.

Purchasing servers

- Procurement of Servers by calling Quotations and release of Purchase Order based on recommendations of CPC.
- Server systems purchased must be compatible with all other computer hardware in the institute.
- All purchases of server must be supported by 3 years warranty.
- All purchases for server must be in line with the purchasing policy of the Institute manual.

- **Purchasing computer peripherals**

  Computer system peripherals include printers, scanners, external hard drives etc. Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals or when need to be replaced with defect/damaged for the systems under service/repair.

  - The purchase of computer peripherals will be through system cell in-charge authorized by Dean Infrastructure with prior approval of Principal as per institute purchase policy.
  - All purchases of computer peripherals must be supported by 6 months/1 year warranty and be compatible with the VIIT(A)'s other hardware and software systems.
  - Any change from the above requirements must be authorized by system cell in charge.
  - All purchases for computer peripherals must be in line with the purchasing policy of the Institute as in manual.

2. Policy for Getting Software

2.1 Purpose of the Policy

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

2.2 Procedures

Request for Software: All software, including non-commercial software such as open source, freeware, etc. must be approved by system cell prior to the use or download of such software.

2.3 Purchase of software

The purchase of all software must adhere to this policy.

- All purchased software must be purchased through CPC on recommendations of system cell department.
- All purchased software must be purchased from authorized suppliers of companies.
- All purchases of software must be supported by at least one-year onsite support and be compatible with the institute server and/or hardware system.
- Any changes from the above requirements must be authorized by system cell in-charge.
- All purchases for software must be in line with the purchasing policy of the Institute as per institute manual.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet. In the event of open source or freeware software is required, approval must be obtained by System cell in-charge through from system admin prior to the download or use of such software. All open source or freeware must be compatible with the VIIT(A)'s hardware and software systems. Any change from the above requirements must be authorized by system cell in-charge.

3. Policy for Use of Software

3.1 Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the institute to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

3.2 Procedures

3.3 Software Licensing

All computer software copyrights and terms of all software licenses will be followed by all employees of the VIIT(A). Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of respect department software programmers to ensure these terms are followed.

3.4 Software Installation

All software must be appropriately registered with the supplier where this is a requirement. institute has to registered as owner of all software purchased. Only software obtained in accordance with the software policy are to be installed on the VIIT(A)'s computers. All software installations are to be carried out by system cell staff. Software upgrade shall not be installed on a system that does not support the original version of the software loaded on it.

3.5 Software Usage

The software that is purchased in accordance with software policy is used in the institute. Prior to the use of any software, the user must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

In order to use the existing software appropriately, it is mandatory to train on all software's.

Employees are prohibited from bringing software from home and loading it on to the institute computer hardware.

Unless approval from, the principal is obtained. Software cannot be taken to home and loaded on employees' personal computer.

Unauthorized software is prohibited from being used in the institute. This includes the use of software owned by an employee within the institute.

The unauthorized copying of software is prohibited. Any employee who violates will be referred to System cell in-charge for necessary action etc. The illegal duplication of software or other copyrighted works is not condoned within this institute.

4. Bring Your Own Device Policy

At institute we acknowledge the importance of mobile technologies in improving institute communication and productivity. In the view of increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to institute network and equipment.

4.1 Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile devices for institute purposes. All staff who use or access institute's technology equipment and/or services are bound by the conditions of this Policy.

4.2 Procedures

Current mobile devices approved for VIIT(A) use The following personally owned mobile devices are approved to be used for institute purposes:

- {All mobile devices such as notebooks, tablets, removable disks, mobile phones etc..}

Personal mobile devices can only be used for the following institute purposes:

- {Allowed to use services such as email access, institute internet access, institute intranet access, etc..}

Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer institute personal sensitive information to personal devices. Sensitive information includes {Personal information that considered sensitive to the institute for example intellectual property, confidential project files, yet to publish research findings, other employee details, student details etc.}
- Not to share the device with other individuals outside the institution to protect the institute data access through the device
- To abide by institute's internet policy for appropriate use and shall access internet for academic and research related purpose only.
- To notify institute immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an un trusted or unknown source to institute's systems/equipment.

4.3 Breach of this policy

Any breach of this policy will be referred to Committee who will review the breach and determine adequate consequences, which can include such as confiscation of the device and barring from usage of service.

4.4 Indemnity

The Institute bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify institute against any and all damages, costs and expenses suffered by institute arising out of any

unlawful or improper conduct and activity, and in respect of any action. settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by institute.

5. Information Technology Security Policy

5.1 Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the institute to ensure integrity, confidentiality and availability of data and assets.

5.2 Procedures

5.3 Physical Security

The location of servers and other network assess to be in a secured room with a proper locking and also in an Air condition environment. System cell in-charge is responsible to take care of the all-hard works. If any are breeching Is liable for action. Security and safety of portable technology, such as laptops will be the responsibility of the employee to where it has been issued. Each employee is required to use security measures such as locks, passwords, antivirus updates, to ensure security of the asset issued to them. In the event of loss or damage, system cell in-charge will assess the extent of damage. If the damage is caused by an employee or student, the whole expenditure to incurred to repair is to bare.

5.4 Information Security

It is the responsibility of system admin to ensure that data back-ups are conducted once in a week and the backed-up data is kept in System cell department. Anti-virus software is to be installed where ever necessary. It is the responsibility of system Admin to install anti-virus software and ensure that this software remains up to date on installed systems used by the institute. All information used is to adhere to the privacy laws and institute's confidentiality requirements of the institute. Any employee breaching this will be treated seriously.

5.5 Intranet Management Information System Access and email access

Every employee will be issued with a unique identification code to access the institute Technology (such as e-mail, institute information system) and will be required to set a password for access. Each password is to be at-least ten characters and is not to be shared with any employee within the institute. In case if an employee forgets the password, web developer/ software developer is authorised to reissue a new initial password with which the employee logs in.

5.6 Network (Intranet & Internet) Use Policy

Network connectivity provided through the Institute, referred to hereafter as "the Network", Is provided through an authenticated network access connection i.e governed under the Institute IT Policy. The IT Services is responsible for the ongoing maintenance and support other Network, exclusive of local applications. Problems within the Institute's network should be reported to system cell.

IP Address Allocation: Any computer (PC/Server) that will be connected to the institute network, should have an IP address assigned by the system cell. Based on a systematic approach, the range of IP addresses that will be allocated to each department is decided. So, any computer connected to the network from that department will be allocated IP address only from that Address pool using DHCP.

Internet Access (wired or Wi-Fi): As and when a new user(faculty/staff/student) want to access internet, user can make request over maintenance service (VIMS portal) for new account creation and get the details from the system cell.

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 absolute violation of IP address allocation policy of the institute. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by system cell. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration. on- compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

6. Website Policy

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the VIIT(A) website.

Procedures

The web developer must record the following details:

- List of domain names registered to the institute.
- Dates of renewal for domain names
- List of hosting service providers

- Expiry dates of hosting {www.vignaniit.edu.in}
- Keeping the Register up to date will be the responsibility of Web Developer.
- System cell in charge will be responsible for any renewal of items listed in the Register.

Website Content

All content on the VIIT(A) website is to be accurate, appropriate and current. This will be the responsibility of Web Developer. All content on the website must follow proper authentication channel in updating of information. The content of the website is to be reviewed daily. Persons authorized to make changes to the institute website: Web Developer Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institute.

7. IT Service Agreements Policy

7.1 Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the institute.

7.2 Procedures

The following IT service agreements can be entered into on behalf of the institute:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of institute software
- Website design, maintenance etc.

All IT service agreements must be reviewed by System cell in charge before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution is received, then the agreement must be approved by Principal. All IT service agreements, obligations and renewals must be recorded in Principal Office and System cell department. Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorized by System cell in-charge.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, recommendation required from System cell in-charge before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Principal.

8. Emergency Management of IT Services

8.1 Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the institute.

8.2 Procedures

8.3 IT Hardware Failure

When there is failure of any of the institute's hardware, this must be referred to System admin through service request form available in departments and also register request in online maintenance service portal. It is the responsibility of System admin to assign Hardware Technician to resolve the issue in the event of IT hardware/OS failure. It is the responsibility of System admin to undertake tests on planned emergency procedures semester wise to ensure that all planned emergency procedures are appropriate and minimize disruption to institute operations.

Virus or other security breach

In the event that the institute's information technology is compromised by software virus or such breaches are to be reported to System admin immediately. System cell in-charge is responsible for ensuring that any security breach is deal within 24 hours to minimize disruption to institute operations.

Website Disruption

In the event that institute website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- Web Developer must be notified immediately
- Correspondence with Web service provider (vender hosting website) to restore immediately.
- Data back-up to be maintained regularly (at-least once in a week) to restore immediately in case of hardware failure also.

Principal

PRINCIPAL
VIGNAN'S INSTITUTE OF
Information Technology (A)
Beside: VSEZ, Duvvada, Visakhapatnam-49