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 VITS 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. It also provides guidelines VITS will use to administer these policies, with the correct procedure to follow.

VITS will keep all IT policies current 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

i) Develop IT infrastructure and services for laboratories, research, faculty, staff and students on 24 x 7 basis. and automation of information management systems

ii) Regular maintenance and upgradation of IT systems in line with their useful life and their obsolescence.

iii) Budget provisions to expand ever growing digital systems and services.

iv) Digitisation of general information and learning resources and access facility through internet and intranet.

v) Maintenance Firewall and Antivirus for Systems security and Cyber security.

vi) Maintenance of critical data and necessary backups.

vii) Maintenance of separate LAN for examinations systems for additional security.

viii) Use and promote opensource software and disposal of e-waste.

These policies and procedures apply to all employees.

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.

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.

Procedures

Purchase of Hardware

Guidance: The purchase of all desktops, laptops, servers, computer peripherals and mobile devices must adhere to this policy . The quotations are invited from minimum 3 vendors and one best quotation in terms of quality and cost is approved by Purchase committee.

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, IBM, Lenovo, Acer etc., .

The desktop computer system bundle must include:

□ Desktop tower
□ Monitor screen sizes
□ Keyboard and mouse
□ Windows/Linux based OS

The minimum capacity of the desktop must be:
□ 2 GHz Processor
□ 2 GB RAM
□ 3 USB ports
Any change from the above requirements must be authorised by SYSTEM ADMIN.

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 server systems
Procurement of Server systems through Dean, IT services by calling Quotations and release of Purchase Order based on recommendations of Purchase Committee.
Server systems purchased must be compatible with all other computer hardware in the Institute.
All purchases of server systems must be supported by 3 years warranty.
All purchases for server systems 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 systems manager authorised by Dean, IT Services with prior approval of Institute as per Institute purchase policy.

All purchases of computer peripherals must be supported by 6 months/1 year warranty and be compatible with the VITS's other hardware and software systems.

Any change from the above requirements must be authorised by Dean, IT Services.

All purchases for computer peripherals must be in line with the purchasing policy of the Institute as in manual.

Policy for Getting Software

Purpose of the Policy

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

Procedures

Request for Software

All software, including non-commercial software such as open source, freeware, etc. must be approved by IT services wing prior to the use or download of such software.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased through PC on recommendations on IT services office.

All purchased software must be purchased from authorised suppliers of companies.

All purchases of software must be supported by at least one-year onsite support and be compatible with the VITS's server and/or hardware system.

Any changes from the above requirements must be authorised by Dean, IT Services.

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 Dean, IT Services through from System Manager prior to the download or use of such software.

All open source or freeware must be compatible with the VITS's hardware and software systems.

Any change from the above requirements must be authorised by Dean, IT services.

Policy for Use of Software

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the VITS 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.

Procedures

Software Licensing

All computer software copyrights and terms of all software licences will be followed by all employees of the VITS.

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.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

VITS is to be the registered owner of all software purchased.

Only software obtained in accordance with the getting software policy is to be installed on the VITS's computers.

All software installation is to be carried out by Software Programmers

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the getting software policy is to be used within the VITS.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. 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 VITS's computer hardware.

Where an employee is required to use software at home, unless approval from Institute is obtained, software cannot be taken to home and loaded on employees' home computer.

Unauthorised software is prohibited from being used in the VITS. This includes the use of software owned by an employee and used within the VITS.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to Dean, IT Services for necessary action etc. The illegal duplication of software or other copyrighted works is not condoned within this VITS.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to committee for further action, reprimand action etc.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify

Systems Manager immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to committee for further consultation, reprimand action etc.

Bring Your Own Device Policy

At VITS we acknowledge the importance of mobile technologies in improving VITS communication and productivity. In addition to the increased use of mobile devices, staff members and students have requested the option of connecting their own mobile devices and laptops to VITS's network and equipment.

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 VITS purposes. All staff who use or access VITS's technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Current mobile devices approved for VITS use

The following personally owned mobile devices are approved to be used for VITS purposes:

□ All mobile devices such as notebooks, tablets, removable disks, mobile phones etc.,

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

□ Allowed to use services such as email access, VITS internet access, VITS intranet access, etc.,

Each employee who utilises personal mobile devices agrees:

□ Not to download or transfer VITS or personal sensitive information to personal devices. Sensitive information includes : Personal information that considered sensitive to the VITS, 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 VITS data access through the device

□ To abide by VITS's internet policy for appropriate use and shall access internet for academic and research related purpose only.

□ To notify VITS immediately in the event of loss or theft of the registered device

□ Not to connect USB memory sticks from an untrusted or unknown source to VITS's systems/ equipment.

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.

Indemnity

VITS 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 VITS against any and all damages, costs and expenses suffered by VITS 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 VITS.

Information Technology Security Policy

Purpose of the Policy

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

Procedures

Physical Security

The area used for all servers, blade servers and other network assets, must be secured appropriate access through secured locks and keys, such as keypad, lock etc., and provision of adequate ventilation and air circulation

System Manager will be responsible to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify to Dean, IT services immediately.

All security and safety of portable technology, such as laptops will be the responsibility of the employee who has been issued. Each employee is required to use such as locks, passwords, antivirus updates, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, system manager will assess the security measures undertaken to determine if the employee will be required to reimburse the VITS for the loss or damage.

Information Security

It is the responsibility of system manager to ensure that data back-ups are conducted {once in a week and the backed up data is kept in Dean, IT services office.

Anti-virus software need to be installed where ever necessary. It is the responsibility of systems manager to install anti-virus software and ensure that this software remains up to date on installed systems used by the VITS.

All information used within the VITS is to adhere to the privacy laws and the VITS's confidentiality requirements. Any employee breaching this will be treated seriously.

Intranet Management Information System Access and email access

Every employee will be issued with a unique identification code to access the VITS 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 VITS.

Where an employee forgets the password web developer/ software developer is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the Institute, referred to hereafter as "the Network", either through an authenticated network access connection, is governed under the Institute IT

Policy. The IT Services is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to ITS office.

IP Address Allocation: Any computer (PC/Server) that will be connected to the Institute network, should have an IP address assigned by the ITS office. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool using VLAN's with 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 (VITMS portal) for the purpose of new account creation and get the details from the ITS office.

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 ITS office. Even configuration of any computer with 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 which such computer is connected to the network. Connection will be re stored after receiving written assurance of compliance from the concerned department/

user.

Website Policy

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the VITS website.

Procedures

The web developer must record the following details:

- List of domain names registered to the VITS
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

{www.vignanits.ac.in.}

Keeping the Register up to date will be the responsibility of Web Developer.

System Manager will be responsible for any renewal of items listed in the Register.

Website Content

All content on the VITS 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 authorised to make changes to the VITS website: Web Developer

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the VITS.

IT Service Agreements Policy

Purpose of the Policy

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

Procedures

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

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

All IT service agreements must be reviewed by Dean, IT Services before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Institute.
All IT service agreements, obligations and renewals must be recorded in Institute Office and Dean, IT office.
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 authorised by Dean, IT Services.

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

Emergency Management of IT Services

Purpose of the Policy

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

Procedures

IT Hardware Failure

Where there is failure of any of the VITS's hardware, this must be referred to Systems Manager through service request form available in departments and also register request in online maintenance service portal.

It is the responsibility of Systems Manager to assign Hardware Technician to resolve the issue in the event of IT hardware/OS failure.

It is the responsibility of System Manger to undertake tests on planned emergency procedures semester wise to ensure that all planned emergency procedures are appropriate and minimise disruption to VITS operations.

Virus or other security breach

In the event that the VITS's information technology is compromised by software virus or such breaches are to be reported to Systems Manager immediately.

Dean, IT Services is responsible for ensuring that any security breach is dealt within 24 hours to minimise disruption to VITS operations.

Website Disruption

In the event that VITS 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.