VIGNAN'S
Foundation for Science, Technology & Research
(Deemed to be UNIVERSITY)
-Estd. u/s 3 of UGC Act 1956

Information Technology

Policy and Procedure Manual (Version -3)

Approved by

Dean - Technology Development

Prof. Dr. Y. RAVI SEKHAR
Dean-Technology Development
Vignan's Foundation for Science, Technology & Research
VADLAMUDI - 522 213
Guntur Dist., A.P., India.

VIGNAN'S
Foundation for Science, Technology & Research
(Deemed to be UNIVERSITY)
-Estd. u/s 3 of UGC Act 1956

Information Technology

Policy and Procedure Manual (Version -3)

Table of Contents

Introduction

IT policy ensures to maintain a secure, legal and appropriate use of IT infrastructure 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 VFSTR IT Policy and Procedure Manual provide the policies and procedures for selection and use of IT within the University, which must be followed by all staff. It also provides guidelines VFSTR will use to administer these policies, with the correct procedure to follow.

VFSTR 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 of networking, servers and computers required for laboratories, research, faculty, staff and automation of information management systems
ii) Access general information and learning resources from anywhere, any time through the internet and the intranet.
iii) Maintain confidentiality of certain areas like examinations.
iv) Provide security mechanism against Virus, Malware, Spyware, Denial of Service attacks, Hacking and Intrusions.
v) Maintenance of critical data backup
vi) Use and promote open source software

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Hardware Purchasing Policy

Policy Number: VFSTR\ITS\Policy\1

Policy Date: 01-06-2010

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 university to ensure that all hardware technology for the university is appropriate and value for money.

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, Acer etc.,}.

The desktop computer system bundle must include:

- Desktop tower
- Monitor screen sizes
- Keyboard and mouse
- Linux based 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 authorised by SYS ADMIN.

All purchases of desktops must be supported by3 Years warranty

All purchases for desktops must be in line with the purchasing policy of the University

Purchasing server systems

Procurement of Server systems through Dean, Technology Development 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 university.

All purchases of server systems must be supported by3 years warranty.

All purchases for server systems must be in line with the purchasing policy of the University 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, Technology Development with prior approval of Registrar as per university purchase policy.

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

Any change from the above requirements must be authorised by Dean, Technology Development.

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

Policy for Getting Software

Policy Number: VFSTR\ITS\Policy\2

Policy Date: 01-06-2010

Purpose of the Policy

This policy provides guidelines for the purchase of software for the VFSTR to ensure that all software used by the VFSTR is appropriate, value for money and where applicable integrates with other technology for the VFSTR. 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 Technology Development 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 CPC on recommendations of Technology Development 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 VFSTR's server and/or hardware system.

Any changes from the above requirements must be authorised by Dean, Technology Development.

All purchases for software must be in line with the purchasing policy of the University as per university 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 free-ware, software is required, the System Manager must obtain approval from Dean – TD prior to the department of use of such software.

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

Any change from the above requirements must be authorised by Dean, Technology Development.

Policy for Use of Software

: Policy Number: VFSTR\ITS\Policy\3

Policy Date: 01-06-2010

Purpose of the Policy

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

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.

VFSTR 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 VFSTR's computers.

All software installation is to be carried out by Software Programmes

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 VFSTR.

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 on 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 VFSTR's computer hardware.

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

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

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, Technology Development for necessary action etc. The illegal duplication of software or other copyrighted works is not condoned within this VFSTR.

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

Policy Number: VFSTR\ITS\Policy\4

Policy Date: 01-08-2010

At VFSTR, we acknowledge the importance of mobile technologies in improving VFSTR communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to VFSTR'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 VFSTR purposes. All staff who use or access VFSTR's technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Current mobile devices approved for VFSTR use

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

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

Registration of personal mobile devices for VFSTR use

Employees when using personal devices for VFSTR use will register the device with Technology Development wing.

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

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

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer VFSTR or personal sensitive information to personal devices. Sensitive information includes {Personal information that considered sensitive to the VFSTR, 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 VFSTR data access through the device
- To abide by VFSTR's internet policy for appropriate use and shall access internet for academic and research related purpose only.
- To notify VFSTR 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 VFSTR's systems/equipment.

All employees who have a registered personal mobile device for VFSTR use, acknowledge that the VFSTR:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data have held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can to take data backup.

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

VFSTR 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 indemnifies VFSTR against any and all damages, costs and expenses suffered by VFSTR 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 VFSTR.

Information Technology Security Policy

Policy Number: VFSTR\ITS\Policy\5

Policy Date: 01-08-2015.

Updated on:12-08-2018

Purpose of the Policy

The policy aims at providing secure and acceptable use of client systems.

Scope of the Policy

This policy is applicable to the employees, Students and Guest users of VFSTR for handling of unclassified information

Policy

(a) Acceptable Use of Client Systems.

(b) User shall be responsible for the activities carried out on the client system, using the network connection/accounts assigned to him/her.

(c) User's network access shall be subjected to monitoring / filtering for malicious / unauthorized activities

(d) For any administrative activities on the client system, user shall adhere to Security Policy for System Administrator.

(e) User shall use account with limited privileges on client system and shall not use administrator privileges.

(f) Backup of important files shall be taken by the user at regular intervals.

(g) System / media containing official information shall be physically secured.

(h) User shall not leave system unattended. The user shall lock out his / her system before leaving the system. Additionally, system idle timeout shall be configured on the client system.

(i) Maintenance or rectification of faults in the client system shall be carried out under close supervision of the user.

(j) User shall check that the system time is as per IST. Any variation shall be reported to the System Administrator / Network Security Administrator.

(k) User shall not engage in any of the following activities:

(i) Circumventing security measures.

(ii) Unauthorized access to Systems / Data / Programs.

(iii) Harassing other users by accessing or modifying their data / resources on the system.

(iv) Creating, accessing, executing, downloading, distributing, storing or displaying any form of anti-national, offensive, defamatory, discriminatory, malicious or pornographic material.

(v) Making copies of software / data for unauthorized use.

(vi) Impersonation.

(vii) Phishing

(viii) Social Engineering

(ix) Unauthorized use of software license

(x) Providing official e-mail address on Internet mail groups / bulletin boards for personal use

(xi) Any activity that is in violation of Central Civil Services (Conduct) rules

(l) User shall report security incident to the System Administrator / Network Security Administrator.

(m) User shall ensure that unauthorized Peer to Peer file sharing software is not installed.

(n) User shall ensure that the system is configured as follows:

i. User shall not share client system with anyone, by default. However, if necessary for any specific reason (such as client system used in shift-duty), following shall be ensured:

(a) Explicit approval of competent / designated authority is taken for each client system and every user accessing it

(b) Every user on the shared client system has a separate account.

(c) File / Folder access permission is limited to meet functional requirement of the user.

ii. User shall not share hard disk or folders with anyone, by default. However, if necessary, only the required folders shall be shared with specific user.

iii. Client System has Client System Security (CSS) implemented as per Client System Security Guidelines.

iv. By default, all interfaces on the client system are disabled and only those interfaces which are required are enabled. For configuration user shall contact the System Administrator.

(o) Virus and Malicious Code (adware, spyware, malware)

a) User shall ensure that client system is configured with the authorized anti-virus software.

b) User shall ensure that anti-virus software and the virus pattern files are up-to-date.

c) User shall ensure that anti-virus scan is configured to run at regular intervals.

d) In case a virus does not get cleaned, incident shall be reported to the System Administrator / Network Security Administrator.

(p) Hardware, Operating System and Application Software.

a) User shall use only the software / hardware which are authorized by the University/Department.

b) The following activities shall be carried out by the System Administrator. However, the User shall ensure the following:

i. Operating System and other software is installed using authorized source / Original Equipment Manufacturer (OEM) media with valid license.

ii. While installing the Operating System and other software packages, only the required utilities are installed / enabled.

iii. Latest available service packs, patches and drivers are installed.

iv. Booting from removable media is disabled.

v. Auto-run on all removable drives is disabled

(q) User shall allow the installation of service packs and patches provided by the patch server.

(r) E-mail Use

i) Only the E-mail account provided by the University shall be used for official communication.

ii) Official E-mail shall not be forwarded to personal E-mail account.

iii) E-mail password shall not be shared even for official purpose.

iv) User shall not attempt any unauthorized use of E-mail services, such as:

a) Distribution of messages anonymously

b) Misusing other user's E-mail address

c) Using a false identity

d) Sending messages to harass or intimidate others

e) Password used for online forms / services / registrations / subscriptions shall not be the same as the password of official E-mail account.

(s) Password Security

i) Selection of password shall be done as per the Password Management Guidelines.

ii) The following activities shall be carried out by the System Administrator. However, the User shall ensure the following:

a) Passwords are enabled on BIOS, System login and Screensaver levels. (refer: Password Enabling Procedure)

b) Auto-logon feature on the client system is disabled. (refer: Auto-Logon Disable Procedure)

c) User account is locked after a predefined number of failed login attempts.

iii) User shall not share or reveal passwords.

iv) Passwords shall be changed at regular intervals as per the Password Management Guidelines.

v) If a password is suspected to have been disclosed / compromised, it shall be changed immediately and a security incident shall be reported to the System Administrator / Network Security Administrator (refer: Security Incident Management Process).

(t) Portable Storage Media

a. User shall use officially issued portable storage media only.

b. User shall return the portable storage media, if it is no longer a functional requirement or in case of damage / malfunctioning.

c. User shall ensure that portable storage media used is free from virus.

d. User shall ensure that the execution of software from portable storage media is not done.

(u) Network Access Policy Applicable for the User

a. User shall take prior approval from the competent authority to connect the client system to the network.

b. A client system authorized to connect to one network shall not connect to any other network.

c. For wireless connectivity, user shall ensure the following:

i. By default, the wireless interfaces are disabled.

ii. Client system does not connect to wireless networks / devices without approval from the competent authority.

iii. If permitted, the wireless interface of the client system is enabled to connect to authorize wireless network only.

(v) Client System Log

a. User having administrative privilege shall not disable / delete the audit trails / logs on the client system.

Review

This Security Policy shall be reviewed at the time of any change in the IT environment or once every year, whichever is earlier. The review shall be carried out for assessing the following:

a) Impact on the risk profile due to, but not limited to, the changes in the deployed technology/ network security architecture, regulatory and / or legal requirements.

b) The effectiveness of the security controls specified in the policy. As a result of the review, the existing policy may be updated or modified.

Enforcement

Violation of this policy shall amount to misconduct under CCS Conduct rules

Password Policy

a) **Purpose:** The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

b) **Scope:** The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the NIC domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

Policy

Policy Statements

i) For users having accounts for accessing systems/services

a) Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

b) All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.

c) Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

d) Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.

e) All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

f) All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.

g) Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

h) Passwords shall not be revealed on questionnaires or security forms.

i) Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

j) The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected.

k) The "Remember Password" feature of applications shall not be used.

l) Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

m) First time login to systems/services with administrator created passwords, should force changing of password by the user.

n) If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

o) The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

ii) For designers/developers of applications/sites

a. No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter

b. The backend database shall store hash of the individual passwords and never passwords in readable form.

c. Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

d. Users shall be required to change their passwords periodically and not be able to reuse previous passwords.

e. For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

Policy for Constructing a password:

All user-level and system-level passwords must conform to the following general guidelines described below.

i) The password shall contain more than eight characters.

ii) The password shall not be a word found in a dictionary (English or foreign).

iii) The password shall not be a derivative of the user ID, e.g. 123.

iv) The password shall not be a slang, dialect, jargon etc.

v) The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.

vi) The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.

vii) The password shall not be based on birthdays and other personal information such as addresses and phone numbers.

viii) The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.

ix) The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).

x) The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., @# $%^&*() _+|~-=\` {}[]:";'<>?/).

xi) Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

Suggestions for Choosing passwords:

Passwords may be chosen such that they are difficult-to-guess yet easy-to-remember. Methods such as the following may be employed:

a) String together several words to form a pass-phrase as a password.

b) Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.

c) Combine punctuation and/or numbers with a regular word.

d) Create acronyms from words in a song, a poem, or any other known sequence of words.

e) Bump characters in a word a certain number of letters up or down the alphabet.

f) Shift a word up, down, left or right one row on the keyboard.

Responsibilities:

i) All individual users having accounts for accessing systems/services in the NIC domain, and system/network administrators of NIC servers'/ network equipment's shall ensure the implementation of this policy.

ii) All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

Compliance:

i) Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance

ii) Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

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 employees becoming aware of a breach to this security requirement is obliged to notify to Dean, Technology Development 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 VFSTR 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, Technology Development office.

Anti-virus software need to be installed wherever 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 VFSTR.

All information used within the VFSTR is to adhere to the privacy laws and the VFSTR'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 VFSTR technology (such as e-mail, university 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 VFSTR.

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 University, referred to hereafter as "the Network", either through an authenticated network access connection, is governed under the University IT Policy. The Technology Development is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to ITS office.

IP Address Allocation: Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the TD office. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. Therefore, 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 (VIMS portal) for the purpose of new account creation and get the details from the TD 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 university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by TD 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. Connections will be restored after receiving written assurance of compliance from the concerned department/user.

Website Maintenance Policy

Policy Number: VFSTR\ITS\Policy\6

Policy Date: 01-10-2010

Purpose of the Policy

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

Procedures

The web developer must record the following details:

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

{www.vignan.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 VFSTR 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 VFSTR website: Web Developer

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

IT Agreements Policy

Policy Number: VFSTR\ITS\Policy\7

Policy Date: 01-06-2015

Purpose of the Policy

This policy provides guidelines for all IT related agreements entered into on behalf of the VFSTR.

Procedures

The following IT related agreements can be entered into on behalf of the VFSTR:

- Provision of general Technology Development
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of VFSTR software
- Website design, maintenance etc.

All IT related agreements must be reviewed by Dean, Technology Development before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Registrar.

All IT related agreements, obligations and renewals must be recorded in Registrar Office and Dean, TD office.

Where a IT related 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, Technology Development.

Where a IT related agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, recommendation required from Dean, Technology Development before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Registrar.

Disaster Recovery Management of IT

Policy Number: VFSTR\ITS\Policy\8

Policy Date: 01-06-2015

Purpose of the Policy

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

Procedures

IT Hardware Failure

Where there is failure of any of the VFSTR'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 responsibilities 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 VFSTR operations.

Virus or other security breach

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

Dean, Technology Development is responsible for ensuring that any security breach is dealt within 24 hours to minimise disruption to VFSTR operations.

Disaster Recovery Policy for Vital VFSTR Data

- Periodic Backup of Vital data of VFSTR on to the NAS storage servers internally is performed daily.
- Periodic Backup (Weekly) of Vital data of VFSTR on to the Cloud Storage is performed weekly.

- In case of any disaster the data can be restored quickly depending the situation either form the NAS internal storage server (if available) or from the cloud storage server.

Website Disruption

In the event that VFSTR 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.

IT Maintenance Policy

Policy Number: VFSTR\ITS\Policy\7

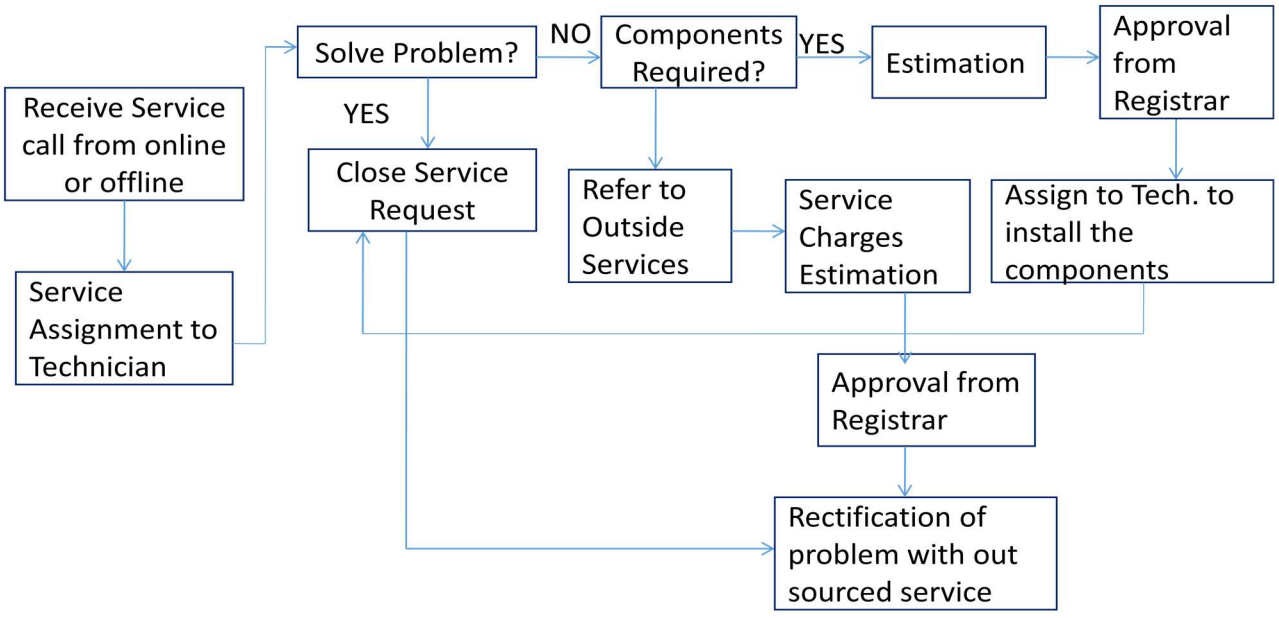
Policy Date: 01-08-2014

Purpose of the Policy

This policy provides guidelines for all IT Maintenance agreements entered into on behalf of the VFSTR.

Procedures

IT Service – Hardware Request Process Chart



The IT service request process flow mentioned above is to give the detailed description about the service request processing.

The IT Services department receives the service calls from online or offline. The received services are assigned to technician based on type of services related to network, systems, Internet access and software. The technician attends to solve the problem. If the problem gets solved, solve it and the service request is closed. If not, the required components are listed out and are estimated in all necessary aspects and submitted to indenter to take necessary approvals. Once approval is obtained from registrar, the service is attended by technician and service request is closed. In case

of unsolvable problems and if need of external service is required, estimate the cost of outsource service and submit to indenter. After getting approval If any outside services are considered service charges are estimated and an approval from registrar is taken and the problem is rectified with outsourced service.

The following Technology Development are provided

- Provision of general Technology Development
- Provision and maintenance of network, hardware and software
- Provision of VFSTR software
- Website design, maintenance etc.