SREE SANKARACHARYA UNIVERSITY OF SANSKRIT, KALADY

(Abstract)

Pl.D- Implementation of IT Policy in the University - Sanctioned-orders issued.

PLANNING AND DEVELOPMENT SECTION

No. Pl.D/2607/SSUS/2014 (subfile) Dated, Kalady, 16.02.2018

Ref: Minutes of the 09/10(165th) Meeting of the Syndicate held on 24.11.2017 (Item No. 7)

ORDER

Vide reference listed above 9/17(165th) meeting of the Syndicate after considering the recommendations of the standing committees on planning & Development held on 15.11.2017 and Accounts Audit & Legal held on 21.11.2017 resolved to accept the IT Policy .It is also resolved to incorporate a sub-clause 4 in clause 5.2 that "The university shall make use of free software as far as possible". Further resolved to constitute an Expert Committee under the Chairmanship of the Registrar to implement IT Policy and manage all IT related affairs in this University. Considering the above sanction has been accorded by the Hon'ble vice Chancellor to implement the afore said resolution of the Syndicate. Orders are issued accordingly.

Sd/-
Dr T.P. Raveendran
Registrar

Copy to :

PS to VC/ PVC/Regr
Director-Planning and Development / System Analyst / ITI/c
IA/Accounts/Bill/Cash/LFA/SF/FC/IQAC

Forwarded/By Order

Section Officer

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

IT SECURITY & AUDIT POLICY

For

Sree Sankaracharya University
ICT Division

Reference

- ✓ Guidelines from Department of Information Technology, Government of Kerala
- ✓ Guidelines from Department of Information Technology, Government of India
- ✓ Indian Computer Emergency Response Team(CERT-In), Ministry of Electronics and Information Technology, Government of India
- ✓ Minutes of the 154th meeting of the Syndicate dated 20.07.2016 - Item no.36 - Establishment of ICT Division in the University

[1] Introduction

Information Security Policies are the cornerstone of information security effectiveness. The Security Policy is intended to define what is expected from the University with respect to security of Information Systems. The overall objective is to control or guide human behavior in an attempt to reduce the risk to information assets by accidental or deliberate actions.

Information security policies underpin the security and well-being of information resources. They are the foundation, the bottom line, of information security within the institution. It should practice the elements of data security that deeds and insurance assets are kept safely so that they are available when it required.

As per the recommendations from IT policy and audit security, the ICT peripherals/assets are to be maintained and managed properly with an organizational manner under technical supervision in terms of confidentiality, integrity and availability.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[2] Objective

The IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business which must be followed by all staff. It also provides guidelines for the institution which will use to administer these policies, with the correct procedure to follow.

The main benefits to having this policy and procedure manual can be majorly enlisted as follows;

[2.1] Ensures all staff are aware of obligations in relation to selection, use and safety when utilising information technology within the business

[2.2] Proven and scientific way to help administrative entities to make consistent and reliable decisions

[2.3] Helps give each employee a clear understanding as to what you expect and allow.

These policies and procedures apply to all the employees in the institution.

[3] Technology Hardware Purchasing Policy

Computer hardware refers 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.

[3.1] Purpose

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money and where applicable integrates with other technology for the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

[3.2] General Conditions for the policy

[3.2.1] The detailed specifications must be prepared by the University ICT Division for the area/purpose/system specific as far as the requirement concerned.

[3.2.2] All purchases of ICT peripheral must be supported by maximum possible guarantee and/or warranty requirements.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

9. Necessary supporting documents
10. Necessary supporting softwares

[3.5] Purchasing server systems

The server system is a device that provides functionality for other programs or devices, called "clients" normally knows client-server model/architecture, and a single overall computation is distributed across multiple processes or devices.

[3.5.1] Minimum items/specification

1. Open source operating system wherever possible
2. Minimum 4 USB ports
3. Minimum 4 network(RJ45) ports
4. Necessary data cables
5. Necessary power cables
6. Necessary supporting documents
7. Necessary supporting softwares

The detailed specification of the server system including processor, memory, storage, architecture must be prepared by the University ICT Division for the area specific.

[3.6] Purchasing computer peripherals

The Computer system peripherals include add-on devices such as 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.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

[3.6.1] Minimum items/specification

1. Necessary data cables
2. Necessary power cables
3. Necessary supporting documents
4. Necessary supporting soft wares

[3.7] Purchasing mobile phones

A mobile phone is a portable telephone that can make and receive calls over a radio frequency carrier while the user is moving within a telephone service area.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT
KALADY-683574

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

3.7.1] Minimum items/specification

1. Necessary data cables
2. Necessary power cables
3. Necessary supporting documents
4. Necessary supporting softwares

A mobile telephone will only be purchased once the eligibility criteria is met.

The purchase of a mobile phone must be ensured the business takes advantage of volume pricing based discounts provided by the authorised suppliers. Such discounts should include the purchase of the phone, the phone call and internet charges etc.

The request for accessories (a hands-free kit etc.) must be included as part of the initial request for a phone.

[4] Policy for Getting Software

Computer software, is that part of a computer system that consists of encoded information or computer instructions, in contrast to the physical hardware from which the system is built.

[4.1] Purpose

This policy provides guidelines for the purchase of software for the business to ensure that all software used by the business is appropriate, value for money and where applicable integrates with other technology for the business. This policy applies to software obtained as part of hardware bundle / pre-loaded software / developed by the University ICT Division / developed from third party sources/ purchased from third party sources.

[4.2] Getting software by developing in-house

1. Open source platform should be used wherever it possible
2. Developing should be monitored by the Project Leader who is authorized by the ICT Division in time to time
3. Industry standard steps / procedures must be followed throughout the SDLC (Software Development Life Cycle)
4. The following systematic development process must be followed
   a. Creating detailed System Requirement Specification(SRS)
   b. Design and Coding of the Application Software
   c. User Acceptance Testing(UAT)

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[4.3] Getting software by developing through outsourcing

1. Open source platform should be used wherever it possible
2. Developing should be monitored by the Project Leader who is authorized by the ICT Division in time to time
3. Industry standard steps / procedures must be followed throughout the SDLC (Software Development Life Cycle)
4. The following systematic development process must be followed
    a. Creating detailed System Requirement Specification(SRS)
    b. Design and Coding of the Application Software
    c. User Acceptance Testing(UAT)
5. The deliverable shall be:
    a. System Requirement Specifications(SRS)
    b. Application Software
    c. Fully documented Source Code (Hard Copy as well as Soft copy)
    d. All necessary licenses wherever applicable
    e. User Manuals
    f. Training materials
    g. Detailed Acceptance Test Plan based on the SRS with test date
6. Necessary training should be ensured
7. Necessary AMC may be procured

[4.4] Getting software by purchasing

1. All software, must be approved by University ICT Division prior to the use / download / purchase of such software.
2. All purchased software must be purchased from authorized dealers / suppliers
3. All purchases of software must be supported by maximum possible guarantee and/or warranty and be compatible with the business's server and/or hardware system.
4. Any changes from the above requirements must be authorised by University ICT Division
5. All purchases for software must be in line with the purchasing policy in the Financial policies and procedures manual in the University.
6. Obtaining open source or freeware software wherever possible
7. Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT
KALADY-683574

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683574

8. In the event that open source of freeware software is required, approval from University ICT Division must be obtained prior to the download or use of such software.
9. All open source or freeware must be compatible with the business's hardware and software systems.
10. Any change from the above requirements must be authorized by University ICT Division.

[5] Policy for Use of Software

[5.1] Purpose

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

[5.2] Software Licensing

1. All computer software copyrights and terms of all software licenses will be followed by all employees of the University.
2. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of University ICT Division to ensure these terms are followed.
3. University ICT Division is responsible for completing a software audit of all hardware to ensure that software copyrights and license agreements are adhered to.
4. The University shall make use of free software as far as possible.

[5.3] Software Installation

1. All software must be appropriately registered with the supplier where this is a requirement.
2. Only software obtained in accordance with the getting software policy is to be installed on the business's computers.
3. All software installation is to be carried out by the University ICT Division
4. 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.

[5.4] Software Usage

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

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

2. 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.
3. All employees within the University must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This ensuring will be the responsibility of respective heads in the business areas.
4. Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.
5. Unless express approval from University ICT Division is obtained, software cannot be taken home and loaded on a employees' home computer
6. Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from University ICT Division is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the business and must be recorded on the software register by University ICT Division
7. Unauthorised software is prohibited from being used in the business. This includes the usage of open source, freeware and commercial, which is owned by an employee and used within the business.
8. 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 University ICT Division for consequences, further consultation, reprimand action etc. The illegal duplication of software or other copyrighted works is not condoned within this business and University ICT Division is responsible to recommend disciplinary action where such event occurs.

[5.5] Breach of Policy

1. Where there is a breach of this policy by an employee, that employee will be referred to business heads for consequences, further consultation, reprimand action etc.
2. Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT ★ KALADY-683574

DR. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

to notify respective business heads or University ICT Division 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 business heads for consequences, further consultation, reprimand action etc.

[6] Policy for Own Device

For all business it is acknowledged that the importance of mobile technologies in improving business 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 University Network and business equipment.

[6.1] Purpose

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and any kind of mobile devices for business purposes. All staff who use or access the University Network / Business Technology equipment and/or services are bound by the conditions of this Policy.

[6.2] Mobile devices approved for business use

1. The following personally owned mobile devices are approved to be used for business purposes:
   a. Notebooks,
   b. Smart phones,
   c. Tablets,
   d. Removable media

[6.3] Registration of personal mobile devices for business use

1. Employees when using personal devices for business use will register the device with University Network / Business Technology Equipment.
2. University ICT Division will record the device and all applications used by the device.
3. Personal mobile devices can only be used for the following business purposes:
   a. email access
   b. business internet access
   c. business telephone calls
   d. business portals
   e. e-Governance application

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

4. Each employee who utilizes personal mobile devices agrees:
   a. Not to download or transfer business or personal sensitive information to the device.
   b. Not to download or transfer sensitive / confidential information such as intellectual property, other employee details etc.
5. Not to use the registered mobile device as the sole repository for Business Information. All business information stored on mobile devices should be backed up
6. Make every reasonable effort to ensure that {Business Name}'s information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected
7. Maintain the device properly with its maintenance requirements of mobile devices such as current operating software, current security software etc.
8. Not share the device with other individuals to protect the business data access through the device
9. Abide by Business Internet Policy for appropriate use and access of internet sites etc.
10. Notify to Business Head and University ICT Division immediately in the event of loss or theft of the registered device
11. Not to connect USB memory sticks from an untrusted or unknown source to University Network / Business Technology Equipment
12. All employees who have a registered personal mobile device for business use acknowledge that the business:
    a. Owns all intellectual property created on the device
    b. Can access all data held on the device, including personal data
    c. Will regularly back-up data have held on the device
    d. Will delete all data held on the device in the event of loss or theft of the device
    e. Has first right to buy the device where the employee wants to sell the device
    f. Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
    g. Has the right to deregister the device for business use at any time.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

DR. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[6.4] Keeping mobile devices secure

1. The following must be observed when handling mobile computing devices (such as notebooks, tablets and smart phones):
   a. Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
   b. Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
   c. Mobile devices may be carried as hand luggage when travelling by aircraft.

[6.5] Exemptions

This policy is mandatory unless University ICT Division grants an exemption. Any requests for exemptions from any of the business directives, should be referred to the University ICT Division.

[6.6] Breach of this policy

Any breach of this policy will be referred to University ICT Division who will review the breach and determine adequate consequences, which can include such as confiscation of the device and or termination of relevant services.

[6.7] Indemnity

University ICT Division 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 the business process against any and all damages, costs and expenses suffered by the business area 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 University ICT Division.

[7] Information Technology Security Policy

Information Technology Security also known as, IT Security is the process of implementing measures and systems designed to

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT KALADY-683574

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

securely protect and safeguard information (business and personal data, voice conversations, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information against any unauthorized access misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions.

[7.1] Purpose

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

[7.2] Physical Security

[7.2.1] All servers, mainframes and other principal network assets for any kind of business in the University must be installed in the University Data Centre.

[7.2.2] University Data Centre will act as a principal physical location of all University Business Technology Equipment and its management and appropriate user access privileges rules will be created, monitored and maintained by the University ICT Division in time to time by using its constituents and will be treated its proprietaries with University ICT Divisior itself.

[7.2.3] It will be the responsibility of University ICT Division 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 University ICT Division/Administration immediately.

[7.2.4] All security and safety of all portable technology (such as notebook, tablet/pads, smartphones) will be the responsibility of the employee who has been issued with. Each employee is required to use such devices and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

[7.2.5] In the event of loss or damage, University ICT Division will assess the security measures undertaken to

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683574

determine if the employee will be required to reimburse the business for the loss or damage.

[7.2.6] All portable devices when kept at the office desk is to be secured by relevant security measure such as keypad, lock etc. provided by the University ICT Division

[7.3] Information Security

[7.3.1] All the issued business devices (servers, computers, laptops/notebooks, tablets/pads, smartphones etc.) for Business Purposes must be administrated by the University ICT Division using necessary User Access Controls / Privileges

[7.3.2] All the users must keep a check list of relevant data to be backed up either general such as sensitive, valuable, or critical business data in the issued business devices issued with.

[7.3.3] It is the responsibility of employee to ensure that daily data back-ups are conducted

[7.3.4] All technology that has internet access must have anti-virus software installed. It is the responsibility of University ICT Division to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

[7.3.5] All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be suffering from relevant consequences.

7.4] Server Operating System Security Guidelines

efore installation of server one should first identify role of he server. The server role means applications running on the erver. The server can be deployed as a file server, print erver, mail server, web server or database server. Based on the erver role or applications running on it, System Administrator SA) can categorize the server under low, medium or high threat erception. In all cases the SA have to plan for adequate server ecurity to ensure confidentiality, integrity and availability f data.

7.4.1] Identification of network services /

etwork services will depend upon the role of the server like ccount server, Web server, Mail server, Database server etc. As

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

a general rule, a network server should be dedicated to a single service. This usually simplifies the configuration, which reduces the likelihood of configuration errors. It also eliminates unexpected and unsafe interactions among the services that present opportunities for intruders. In some cases, it may be appropriate to offer more than one service on a single host computer. For example, the server software from many vendors combines the file transfer protocol (FTP) and the hypertext transfer protocol (HTTP) services in a single package. For some organizations, it may be appropriate to provide access to public information via both protocols from the same server host, but it is not recommended since it is a less secure configuration.

[7.4.2] Physical security

Access to a server is very important, physical access to a server should be limited to only administrator and other server operators for backup etc. There should be no free access to servers. In general, following guidelines should be adhered to

1. Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office
2. Keep portable equipment secure—
3. Position monitor and printers so that others cannot see sensitive data
4. Keep floppy disks and other media in a secure place
5. Seek advice on disposing of equipment
6. Report any loss of data or accessories to the SA
7. Keep the system and sensitive data secure from outsiders
8. Get authorization before taking equipment off-site
9. Take care when moving equipment
10. Log out, shut down or lock the system when leaving office
11. Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure

[7.4.3] Methods of authentication

Depending on the level of threat exposure to the server, authentication method should be chosen

1. For Low Threat Exposure in build user/password mechanism available with the OS is an acceptable practice.
2. For Medium Threat Exposure a choice could be made from user/password combination implemented by sever only with strong password policy or an external

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

authentication server like TACKAC, RADIUS or KERBOUS may be implemented. For example, an external POP mail server may have radius server authenticating the user access.

3. For High Threat Exposure a choice could be made from tokens, smart cards and biometrics devices (devices that recognize a person based on biological characteristics such as fingerprints or patterns of the retinal blood vessels.

[7.4.4] Account Policy

[7.4.4.1] User privileges & rights

Document the categories of users that will be allowed access to he provided services. Categorize users by their organizational department, physical location, or job responsibilities. A category of administrative users who will need access to administer the network server and a category for backup operators needs to be created. Normally, access to network servers should be restricted to only those administrators responsible for operating and maintaining the server. Determine he privileges that each category of user will have on the omputer. To document privileges, create a matrix that shows the sers or user categories cross-listed with the privileges they ill possess. The privileges are customarily placed in groups hat define what system resources or services a user can read, rite, change, execute, create, delete, install, remove, turn n, or turn off. For many resources, such as program and data iles, the access controls provided by the OS are the most vious means to enforce access privileges. Also, consider using ncryption technologies to protect the confidentiality of nsitive information.

.4.4.2] Passwords

ere should be password policy in the organization. The most mmon method of authentication is password. The responsibility selecting a password that is hard to guess generally falls on ers. To decrease the chances of guessing password, user must lect a hard-to-guess, or strong password.

trong password must:

1. Be as long as possible
2. Include mixed-case letters.
3. Include digits and punctuation marks.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

4. Not be based on any personal information.
5. Not be based on any dictionary word, in any language.

While most shared systems can enforce at least some of these rules, almost none have features to enforce all of them. Despite all these efforts the passwords could be guessed given enough time. Thus a user must also:

1. Change his/her password regularly, in order to limit the amount of time available to persons to guess it.
2. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed regularly.
3. Never use the same password twice.

Some systems have a password expiry feature, which forces user to change his password periodically. Some systems incorporate a password history feature, which disallows user from reusing one of his last n passwords. When faced with a password history mechanism, some users may change their password n times, and return it to its original value, so as to avoid having to remember a new password value. To prevent this, systems should either have an unlimited-length password history, or prevent users from changing their password more than once daily.

[7.5] Workstation Operating System Security Guidelines

The word "workstation" is used in this module to mean the combination of the hardware, operating system, application software, and network connection.

[7.5.1] User Categorisation

For workstations, the categories of users should be defined. The categories should be based on user roles that reflect their authorised activity. The roles are often based on similar work assignments and similar needs for access to particular information resources-system administrators, software developers, data entry personnel, etc. If appropriate, remote users should be categorised as temporary or guest users.

[7.5.2] User Privileges

Create a matrix that shows the users or user categories cross-listed with their privileges. The privileges are customarily placed in groups that define what system resources or services a user can read, write, change, execute, create, delete, install, remove, turn on, or turn off.

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[7.5.3] Configure multiple computers using a tested model replication procedure

When deploying several computers, especially desktop workstations, across an organisation, it is better to configure one appropriately and then propagate that configuration to all the others. It should be ensured that this is done in a secure manner, especially if a network is used for propagation. This helps in establishing a consistent level of security on all the computers to LAN. It also facilitates consistent updating of all computers as and when necessary.

[7.6] Web Server Security Guidelines

web server is a program, which listens for http requests on a TCP/IP port (normally either port 80 or port 443) and serves html pages in response.

[7.6.1] The essential way to secure a Web Server through the following steps

1. Installing a Secure Server
2. Configuring Web Server Software and the underlying Web Server host operating system
3. Maintaining the Web Server's Integrity

[7.6.2] Practices that should be adopted by business technology for installing and configuring web server are as follows:

1. Isolate the Web server from public networks and the organization's internal networks.
2. Care must be taken while placing a public Web server on University network. It is highly recommended that the server be placed on a separate, protected subnetwork. This will ensure that traffic between the Internet and the server does not traverse any part of the private internal network and that no internal network traffic is visible to the server.

   To accomplish this, following steps may be taken:
   a. Place the web server on a subnet isolated from public and internal network.
   b. Use firewall technology to restrict traffic between a public network and the web server and between the web server and the internal network.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

c. Place the servers providing email, directory and database services in support of the web site on a protected subnetwork.
d. Disable all source routing functions in the firewalls and routers protecting the public web server.
e. Disable IP forwarding and source routing on the web server and the server hosts that provide supporting services.

[7.6.3] Configure the Web server with appropriate object, device, and file access controls. This is necessary for the following reasons

a. To limit access to the Web server software
b. To apply access controls specific to the Web server where more detailed levels of access control are required

To configure this, following steps may be taken:

a. The web server should be configured to execute under a unique individual user and group identity. This is important for implementing access controls on various files, viz. Server log files, system software and configuration files, password files etc.
b. The protection needed for various files, devices and objects specific to the web server should be identified.
c. Time-outs and other controls to mitigate the effects of DOS attacks should be configured.
d. The file serving of web server file listings should be disabled.

[7.6.4] Configure the Web server to use authentication and encryption technologies, where required.

Without strong user authentication, one may not be able to restrict access to specific information by authorized users. Before placing any sensitive or restricted (i.e. not for public consumption) information on a public Web server, one needs to determine the specific security and protection requirements and confirm that the available technologies, like SSL (Secure Socket Layer), S/HTTP (Secure Hypertext Transport Protocol), and SET (Secure Electronic Transaction) can meet these requirements.

[7.7] Firewall Security Guidelines

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

This provides introductory information about firewalls and firewall policy primarily to assist those responsible for etwork security. It addresses concepts relating to the design, election, deployment, and management of firewalls and firewall nvironments. This document is not intended to provide a ndatory framework for firewalls and firewall environments, but ther to present suggested approaches to the topic.

.7.1] General Guidelines

1. Business processes should view firewalls as their first line of defense from external threats; internal security must still be a top priority. Internal systems must be patched and configured in a timely manner.
2. Organizations should use firewalls to secure their Internet connections and their connections to other networks. Proper Firewall should be framed and followed
3. At remote locations, users should use personal firewalls and firewall appliances to secure their connections to the Internet and Internet Service Providers
4. Organizations must monitor incident response team reports and security websites for information about current attacks and vulnerabilities. The firewall policy should be updated as necessary. A formal process should be used for managing the addition and deletion of firewall rules.
5. Organizations should recognize that all system administration, especially firewall administration, requires significant time and training. Organizations should ensure that their administrator receive regular raining so as to stay current with threats and .lnerabilities.
6. nsure that the Firewall and the network cabling related to t are physically secured. Physical access to the firewall the related network cabling provides opportunities for intruder to bypass the firewall itself

echnology Access

.8.1] Every employee will be issued with a unique ication code to access the business technology and will ired to set a password for every single access of the with University Network

8.2] Each password is to be set by the employee es with at least one capital letter, one small letter,

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

one digit, one special character and in total of 8 characters which is not to be shared with any employee within the business.

[7.8.3] University ICT Division is responsible for the issuing of the identification code and initial password for all employees.

[7.8.4] Where an employee forgets the password or is 'locked out' after three wrong failure attempts, then recovering of the same be done by direct contacting the University ICT Division or by using recovery procedures available in the work flow. The University ICT Division 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.

[7.8.5] Employees are only authorised to use business computers for personal use and will be possible only with permission from University ICT Division.

[7.8.6] Internet policy will be applicable in time to time as per direction from the University administration.

[7.8.7] It is the responsibility of University ICT Division to keep all procedures for this policy up to date.

[7.9] Password Policy

The following policy should be considered as the minimum baseline password policy for implementation across all business process systems in the University. More stringent criteria for setting and usage of passwords could be followed (which should be considered as above the baseline) for any business process based on the need.

1. Passwords should be changed every 45 days
2. Passwords should be minimum of 8 characters
3. Passwords should be alphanumeric characters with a minimum of 2 numeric characters.
4. Blank passwords should not be permitted.
5. The minimum password age should be 1 day. There should be no immediate changes of passwords at least on a daily basis.
6. Guest accounts should be removed immediately on installation of systems.
7. Default system accounts provided by vendor/service provider should be renamed immediately upon installation of new systems.

KALADY-683574 ★ SREE SANKARACHARYA UNIVERSITY OF SANSKRIT

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit

8. Last 5 passwords should not be reused for any reasons. After 5 unsuccessful attempts, account should be locked until the system administrator reactivates the account.
9. Users should be required to change their passwords immediately after their first logon to their applications/IT systems for first time logons.
10. Password should strictly be kept private and confidential. Passwords should not be shared, coded into programs, stored in an unprotected form in any IT systems including mobile and wireless devices inclusive. Password should not be written down.
11. Password should not be displayed in plain text while logging in. Passwords must be masked.
12. Passwords should be changed immediately in case of a suspected compromise or a wrongful disclosure scenario.
13. Responsibility of maintaining confidentiality of User passwords should rest with the User.
14. Passwords should be communicated securely to the Users. Temporary secure passwords should be informed to Users first time, enabling IMMEDIATE change over to passwords of User's choice, as per the policy.
15. There should be a process to verify the identity of the User prior to communicating the password for a new user, while resetting password or in case of issue of a temporary password. For example, IT Service Desk or System Administrators should communicate passwords to identified users only after confirming certain user details like Employee number, Date of joining etc.
16. Initial temporary user passwords should be linked with unique identifiers of a user and should not be guessable.
17. Users should refrain from using any option which helps "Remember Passwords" in any application at the end user machine or at application level itself for convenience purposes.
18. Users should be held responsible for every transaction being carried out using their login account.
19. Screen saver password should be enabled by Users on their own desktops/laptops to prevent unauthorized access.
20. Any employee/contractor/partner/vendor/service provider or supplier knowing critical system passwords for business purposes should be bound by standard Non-Disclosure Agreements (NDA).
21. Whenever key personnel administering or having privileged access to the system leaves the business or changes role

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

within the business. The System passwords should be changed immediately

22. Users should refrain from using same passwords for business and non-business purposes.

[7.10] Additional Policies for Website Policy

Reference: *System Security Guidelines by Indian Computer Emergency Response Team*

[8] Information Technology Administration Policy

Administration involves the IT asset management which normally is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.

[8.1] Purpose

This policy provides guidelines for the administration of information technology assets and resources within the business.

[8.2] General procedures / guidelines

[8.2.1] All software installed and the license information must be registered on the University ICT Division. It is the responsibility of the division to ensure that this register is maintained. The register must record the following minimum information:

1. Device ID
2. Si No, Model and Device Type
3. What software is installed on every machine
4. What license agreements are in place for each software package
5. Renewal dates if applicable.
6. Location and User of the device
7. Details regarding AMC /Warranty etc.

[8.2.2] University ICT Division is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by the Division.

[8.2.3] University ICT Division is responsible for maintaining adequate technology spare parts and other requirements on the basis of the analysis of necessities.

KALADY-683574 * SREE SANKARACHARYA UNIVERSITY OF SANSKRIT *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
University of Sanskrit

[8.2.4] A technology audit may be conducted by the University ICT Division in suspected situations to ensure that all information technology policies are being adhered to.

[8.2.5] Any unspecified technology administration requirements should be directed to University ICT Division

[9] Website Policy

Recommended guidelines applies for the development and management of University web portal and its child websites. The primary objectives of the guidelines are to ensure that belonging to any constituent of the University, at any level, are visitor friendly.

[9.1] Purpose

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website which are to be followed while developing or managing any websites, web portal or web application under the perspective of University.

[9.2] General Guidelines

[9.2.1] All the websites should be hosted in the University Data Centre

[9.2.2] A Website Register is to be followed which must record the following minimum details:

1. List of domain names registered to the business
2. All the domain names should be in the format of *{name}.ssus.ac.in*
3. Super user credentials

[9.2.3] The keeping the register up to date will be the responsibility of University ICT Division.

[9.2.4] All content on the business website must be provided by respective business areas from the University in time to time through any University Administrative Cell (such as IQAC - Internal Quality Assurance cell) or from the authorized nodes/points which are directed by the University Administration. Relevant communication must be made by the University Administration to such Business Nodes.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

within the business. The system passwords should be changed immediately

22. Users should refrain from using same passwords for business and non-business purposes.

[7.10] Additional Policies for Website Policy

Reference: *System Security Guidelines by Indian Computer Emergency Response Team*

[8] Information Technology Administration Policy

Administration involves the IT asset management which normally is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.

[8.1] Purpose

This policy provides guidelines for the administration of information technology assets and resources within the business.

[8.2] General procedures / guidelines

[8.2.1] All software installed and the license information must be registered on the University ICT Division. It is the responsibility of the division to ensure that this register is maintained. The register must record the following minimum information:

1. Device ID
2. Si No, Model and Device Type
3. What software is installed on every machine
4. What license agreements are in place for each software package
5. Renewal dates if applicable.
6. Location and User of the device
7. Details regarding AMC /Warranty etc.

[8.2.2] University ICT Division is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by the Division.

[8.2.3] University ICT Division is responsible for maintaining adequate technology spare parts and other requirements on the basis of the analysis of necessities.

SREE SANKARACHARYA U. SANSKRIT KALADY-683574

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[9.2.5] The content of the website is to be reviewed by respective business areas before submitting into authorized cells in University

[9.2.6] The University ICT Division is responsible for making necessary changes and uploading data to the business websites

[9.3] Additional Policies for Website Policy

Reference: *Guidelines for Indian Government websites – An Integral Part of Central Secretariat Manual of Office Procedure*

[10] E-Mail Policy

These are the recommended guidelines for the usage and management of e-mail system for business process.

[10.1] Purpose

This policy provides guidelines for the maintenance of all relevant technology issues related to the business e-mail system.

[10.2] General Guidelines

[10.2.1] All the business entities must be provided with email accounts with the domain name *ssus.ac.in*

[10.2.2] For statutory officers an additional *gov.in* email accounts must be used for confidential and government communications

[10.2.3] The following are the e-mail accounts for statutory officers provided by Government of India (@gov.in)

Vice- Chancellor:	vc.ssu-ker@gov.in
Pro Vice- Chancellor:	pvc.ssu-ker@gov.in
Finance Officer:	fo.ssu-ker@gov.in
Registrar:	registrar.ssu-ker@gov.in

[10.2.4] All the business area must be used e-mail accounts for business process provided by University ICT Division(@ssus.ac.in)

[10.2.5] It is the responsibility of University ICT Division to create, manage and maintain the user credentials for each email accounts

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[10.2.6] The user credentials must be stored with in the University Data Centre in its electronic form with necessary security features like encryptions

[10.2.7] A register is to be kept update for the list of e-mail accounts issued from University ICT Division.

[10.3] Additional Policies for E-Mail Policy

Reference: *E-mail Policy of Government of India, Department of Electronics and Information Technology, Ministry of Communications and Information Technology*

[11] Electronic Transactions Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the business.

[11.1] Purpose

The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

[11.2] Electronic Funds Transfer (EFT)

[11.2.1] It is the policy of Business Process that all payments and receipts should be made by EFT where appropriate.

[11.2.2] All EFT payments and receipts must adhere to all University Financial policies.

[11.2.3] All EFT arrangements, including receipts and payments must be submitted to relevant Business Area of the business.

[11.2.4] EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy in the University Financial Policies.

[11.3] Electronic Purchases

[11.3.1] All electronic purchases by any authorised employee must adhere to the University Purchasing Policy.

[11.3.2] Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe, and be able to demonstrate that this has been reviewed.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT ★ KALADY-683574 ★

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[11.3.3] All electronic purchases must be undertaken using business credit cards only and therefore adhere to the business credit card policy in the University Financial Policy.

[12] IT Service Agreements Policy

Information Technology Service agreements is the service level documents prepared at any interaction / usage of third party services for the business.

[12.1] Purpose

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

[12.2] General Guidelines

[12.2.1] The following IT service agreements can be entered into on behalf of the business:

1. Provision of general IT services
2. Provision of network, hardware and software
3. Repairs and maintenance of IT equipment
4. Provision of business software
5. Provision of mobile phones and relevant plans
6. Website design, maintenance etc.

[12.2.2] All IT service agreements must be reviewed by University ICT Division and Legal Section before the agreement is entered into.

[12.2.3] All IT service agreements, obligations and renewals must be recorded with University Administration

[12.2.4] 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 {insert relevant job title here}.

[12.2.5] Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, University ICT Division and Legal Section must be reviewed before the renewal is entered into.

[13] Emergency Management of Information Technology

[13.1] Purpose

This policy provices guidelines for emergency management of all information technology within the business.

KALADY-683574 * SREE SANKARACHARYA UNIVERSITY OF SANSKRIT *

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-68

[13.2] IT Hardware Failure

[13.2.1] Where there is failure of any of the business's hardware, this must be referred to University ICT Division immediately.

[13.2.2] It is the responsibility of technical assistants or similar nature of job designations to undertake tests on planned emergency procedures to ensure that all planned emergency procedures are appropriate and minimise disruption to business operations.

[13.2.3] When a hardware failure cannot be recovered or solved in any manner it should be entered into a condemn list and kept in place with necessary entries by the technical assistants. This must be done only after the confirmation and certification from the head of the Division

[13.2.4] All such failures must be registered with University ICT Division

[13.2.5] The signature for solved issues must be obtained and recorded from the end users

[13.3] Software Disruptions

[13.3.1] Where there is failure of any of the business's software or business's information technology is compromised by software virus or such noticed breaches, this must be referred to University ICT Division immediately.

[13.3.2] All such disruptions must be registered with University ICT Division

[13.3.3] The signature for solved issues must be obtained and recorded from the end users

[13.4] Website Disruption

[13.4.1] In the event that business website is disrupted, the following actions must be immediately undertaken:

[13.4.2] All such disruptions must be registered with University ICT Division

[14] General guidelines for IT security & Audit Policy

[14.1] Applicable

Policies for All Users of the Business Process

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

[14.1.1] Using CD/ Flash Drives

1. Flash drives should be used in consultation with system administrator/ Controlling Officer (IT) and should be scanned before use.
2. Unofficial CDs or Flash Drives should not be used on office systems.

[14.1.2] Password

1. Administrative password of all PC, Laptops etc shall be managed by the System Administrator/ Controlling Officer (IT).
2. Keep the system screen saver enabled with password protection.
3. Don't share or disclose your password.
4. A strong password must be as long as possible, and must include mixed-case letters, numbers, punctuation marks, and avoid any personal information, or any of the words in the dictionary.
5. Change password at regular intervals.

[14.1.3] Backup

1. Normal backups from business computers is the responsibility of the users themselves
2. Backup should be maintained regularly on the space provided on central server of the department or on the storage media as per department policy.
3. Always backup the data before leaving the workstation.

[14.1.4] Email Accounts

1. New email accounts for all the departments of the Business shall be processed through Controlling Officer (IT).
2. The administrative password/ account of all official emails shall be managed by the Controlling Officer (IT).

[14.1.5] Safety of System

1. Protect the system from unauthorized use, loss or damage, e.g. the cabin/ door should be locked when not in the office.
2. Store portable equipment issued to you securely.

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

5. General Interest, Personal such as Advertising, Brokerage and Trading, Games, Social Networking, Real Estate, News and Media etc.
6. General Interest – Business such as Finance and Banking, Business, Armed Forces etc.

[14.1.11] Audit Policy

Purpose of the audit policy is to provide the guidelines to security audit team to conduct a security audit on IT based infrastructure system at various departments of the business. Security Audit is done to protect entire system from the most common security threats which includes the following:

1. Access to confidential data
2. Unauthorized access of the department computers.
3. Password disclosure compromise
4. Virus infections.
5. Denial of service attacks.

Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and resources
2. Monitor all security measures to ensure conformance with business security policies.
3. Investigate security incidents recorded in security log book

The Controlling Officer (IT) or system administrator or a nominated person from the IT division will be responsible for internal Audit within the department and operations of their sub dept. When requested and for the purpose of performing an audit, any access needed will be provided by the end users to the internal audit team.

This access may include:

1. User level and/or system level access to any computing or communications device.
2. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective Dept. equipment or premises.
3. Access to work areas (offices, cubicles, storage areas, etc.).
4. Access to official email accounts.

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *

Dr. DHARMARAJAN P.K
Vice-Chancellor
Sree Sankaracharya University of
Kalady, Ernakulam, Kerala-6

b. Access to interactively monitor and log traffic on networks.

[15] Conclusion

The ICT Division and the IT Policy may be managed by the existing administrative hierarchy of the University.

The IT Policy described above is to be modified as per the regulations, reforms, directions etc., may be undertaken by the Government of Kerala, Central Ministry and other Government Agencies.

30.09.16
Director
Planning and Development

Law

SUBMITTED

Dr. DHARMARAJAN P.K.
Vice-Chancellor
Sree Sankaracharya University of Sanskrit
Kalady, Ernakulam, Kerala-683 574

SREE SANKARACHARYA UNIVERSITY OF SANSKRIT * KALADY-683574 *