

SRI RAMACHANDRA
INSTITUTE OF HIGER EDUCATION AND RESEARCH
(DEEMED TO BE UNIVERSITY)
PORUR, CHENNAI

Information Technology and Security
– Policy and Procedure Manual

TABLE OF CONTENTS

SL. NO.	SECTION	CONTENT	PAGE NO.
1		Introduction	1
2		Information Technology and Security Policy Statement	2
3		Information Technology and Security Objectives	3
<hr/>			
4	Section 1	Asset Management	
		1.1 Responsibility for Assets	4
		1.2 Information Classification	5
		1.3 Media Handling and Security	7
<hr/>			
5	Section 2	Access Control	
		2.1 Business Requirement for Access Control	9
		2.2 User Access Management	10
		2.3 User Responsibilities	11
		2.4 System and Application Access Control	13
<hr/>			
6	Section 3	Mobile Devices, Teleworking & Cryptography	
		3.1 Mobile Devices and Teleworking	15
		3.2 Cryptographic Controls	16
		3.3 Key Management	16
<hr/>			
7	Section 4	Physical and Environmental Security	
		4.1 Secure Areas	17
		4.2 Equipment Maintenance and Security	17
<hr/>			
8	Section 5	Operations Management	
		5.1 Operational Procedures And Responsibilities	19
		5.2 Protection From Malware	20
		5.3 Back-up	20
		5.4 Logging and Monitoring	22
		5.5 Control of Operational Software	23
		5.6 Technical Vulnerability Management	24
		5.7 Information Systems Audit Consideration	25
		5.8 Compliance with Legal and Contractual Requirements	26




9	Section 6	Communications Management	
		6.1 Network Security Management	28
		6.2 Information Transfer	29
		6.2.1 Information Transfer Policies and Procedure	29
		6.2.1.1 Electronic Messaging & E-mail policy	30
		6.2.1.2 Credit card payment services security	36
		6.2.2 Agreements on Information Transfer	36
		6.2.3 Confidentiality or Non-disclosure Agreements	37
<hr/>			
10	Section 7	System Acquisition, Development and Maintenance	
		7.1 Security Requirements of Information Systems	38
		7.1.1 Information Security Requirements Analysis and Specifications	38
		7.1.2 Securing Application Services on Public Networks	38
		7.1.3 Protecting Application Services Transactions	39
		7.2 Security in Development and Support Process	39
		7.2.1 Secure Development Policy	39
		7.2.2 System Change Control Procedures	39
		7.2.3 Technical Review of Applications after Operating Platform Changes	40
		7.2.4 Restrictions on Changes to Software Packages	40
		7.2.5 Secure Development Environment	40
		7.2.6 Outsourced Development	40
		7.2.7 System Security Testing	41
		7.2.8 System Acceptance Testing	41
		7.3 Test Data	
		7.3.1 Protection of Test Data	41



INTRODUCTION

The Sri Ramachandra Institute of Higher Education & Research (Deemed to be University) Information Technology and Security Policy and Procedure Provides the policies and procedure for selection and use of Information Technology within the organization, which covers entire organisation and must be followed by all staff. It also provides guidelines which the organisation will use to administer these policies and procedures.

Sri Ramachandra Institute of Higher Education & Research (Deemed to be University) will keep all Information Technology and Security 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

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



INFORMATION TECHNOLOGY AND SECURITY POLICY STATEMENT

Sri Ramachandra Institute of Higher Education & Research (Deemed to be University) is committed to Information Technology and Security in terms of Protecting the organisation's information technology assets against unauthorised use, modifications, disclosure either accidental or intentional.

Responsibility for protecting these assets through designated faculty / employees who will be responsible for identifying and protecting the assets in their respective process areas.



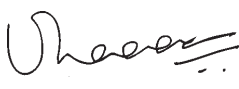
Ensuring that the Students, Faculty and all other persons working in the organisation use the assets only for the intended purpose and adhere to laid down policies and procedures.

Ensuring compliance with applicable legal or regulatory requirements and contractual obligations.

Scope

1. Covers all departments within the organization.
2. It covers all those entities to whom activities of the organisation is outsourced and they must comply with the same requirements.

This policy shall come into force from October 2018

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



INFORMATION TECHNOLOGY AND SECURITY OBJECTIVES

Establish and maintain an effective information technology and security system in the organization.

Promote and install Information Technology and security as a culture in the organisation through appropriate training and motivation methods.

Create awareness on information technology and security among third party/external party service providers and ensure their adherence to the information technology and security policy of the organization.

Maintain high professional standard of information technology and security with regular reviews to maintain excellence, adhering to statutory and regulatory requirements.

Keep abreast of latest developments related to information technology and security.



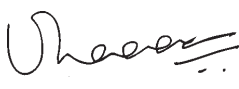
Ensure the security and confidentiality of Students', Faculties' and Patients' related information.

Protect against any anticipated threats or hazards to the integrity of Students', Faculties' and Patients' related information.

Protect against unauthorised access to or use of such information that could result in substantial harm or inconvenience to any Student, Faculty and patient.

Ensure availability of all relevant information to authorised users.

Ensure the proper disposal of Students', Faculty's and Patients' information, which are outdated.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



SECTION 1



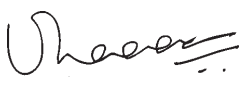
Asset Management

1.1 Responsibility for assets

1. An inventory of all the assets of the Organisation relating to information technology should be prepared and held in the Organization. Examples of assets are:
 - Information assets: (e.g. databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, archived information etc.)
 - Software assets: (e.g. application software, system software, development tools and utilities etc.)
 - Physical assets: (e.g. computer equipment (desktops, servers, laptops, printers, scanners etc.), communications equipment (routers, switches, hubs, modems, PABXs, Fax machines etc), magnetic media (e.g. External drives , CDs, tapes, disks etc.), other technical equipment (power supplies, air-conditioning etc.), Other Equipment which are used for day-to –day operations of the organisation
 - Human Resources
 - Paper Assets like Agreements, SLAs, Students and faculty related documents, Patient case sheets / Medical Records, etc.
 - Commercial equipment
 - Other Technical equipment

Responsibility: Process Heads / HODs / System Administrator

2. Department Head should be responsible for the protection of such assets at each office/ Department of the Organization.
3. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned to the respective owners. The following table gives the details of the owners/custodians for all the assets in respective departments.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



LIST OF ASSETS:

SL. NO.	USER	DEPARTMENT	ASSET DETAILS	LOCATION OWNER	ASSET	CUSTODIAN

Department Heads should identify one of the staff for nominating as Custodian. In the event of transfer of the Custodian, Department Head should identify another Staff.

Where there is no Staff other than the Department Head, he / she will be both Owner and Custodian.

1.2 Information Classification

Procedures

1. Information in the Organisation should be classified into two types as defined below as per the sensitivity of the information content. The classifications are – CONFIDENTIAL, and UNCLASSIFIED. This standard data sensitivity classification system should be used throughout the Organization. These classifications are defined as follows:

CONFIDENTIAL: This classification applies to sensitive Student information, Faculty / Employee information, patient information which is nonetheless intended for use within the Organization. Its unauthorised disclosure could adversely impact the Organization, its stakeholders, its associates, and/or its students, employees and patients.



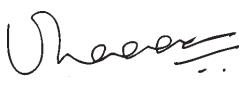
Example : Personal information of employees / faculty (such as salary details, security verification details, an enquiry, disciplinary proceedings, etc) is confidential in nature, disclosure of which could lead to some unwarranted and unpleasant situation to the Organization

Personal information of students such as their grades, marks, various assessments, etc.

Patient records with various personal details of the patients.

All documents, manuals, software licenses and software in various media in the IT department and in other departments.

UNCLASSIFIED: This classification applies to all other information which is not confidential. While its unauthorised disclosure is against policy, it is not expected to seriously or adversely impact the Organization, its employees / faculty, students, its stakeholders, its associates, and/or its patients.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



2. All confidential should be labeled confidential . Information that does not fall into this category need be marked “unclassified”. These markings should be maintained whatever technology is used to capture, store, or process the information.
3. If known, the data that was labeled as confidential information will no longer be sensitive, then it should be indicated as part of the information classification. This policy also applies in those circumstances where sensitive information will be downgraded to a less sensitive classification.
4. Information owners should review the sensitivity classifications assigned to information for which they are responsible.
5. If necessary, Information owners should determine whether sensitive information may be declassified or downgraded.
6. The roles and responsibilities of all participants in the information classification program should be defined as Owner, Custodian and Users.
7. A key element of the classification scheme is the role of the users, owners, or custodians of the data play in regard to the data. The roles that owner, custodian, and user plays in information classification are described here under:

Owner : HODS of Department



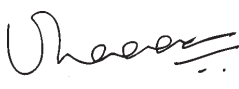
An information owner is responsible for the information assets under their control that must be protected. An owner is different from a custodian. The owner has the final responsibility of data protection, and under the concept of due care, the owner may be liable for negligence because of the failure to protect this data. However, the actual day-to-day function of protecting the data may be delegated to a custodian.

The responsibilities of an information owner could include the following:

- Making the original determination to decide what level of classification the information requires, which is based upon the business needs for the protection of the data.
- Reviewing the classification assignments periodically if necessary and making alterations as the business needs change.
- Delegating the responsibility of the data protection duties to the custodian.

Custodian

An information custodian is delegated the responsibility of protecting the information by its owner. This role is commonly executed by IT systems personnel and for paper documents, it could be the staff of the concerned department / section. The duties of a custodian include the following:

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



- Running regular backups, safe custody, and routinely testing the validity of the backup data
- Performing restoration from the backups when necessary
- Maintaining those retained records (both paper and electronic media) in accordance with the established information classification policy

In addition, the custodians also have additional duties, such as being the administrator of the classification scheme.

CUSTODIAN – Systems Department, Designated personnel of the concerned departments.

User

In the information classification scheme, an end user is considered to be anyone (such as an operator, employee / faculty, student or external party) that routinely uses the information as part of their job. They can also be considered a consumer of the data, who needs daily access to the information to execute their tasks. The following are a few important points to note about end users:

- Users should follow the operating procedures that are defined and they should adhere to the published guidelines for its use.
- Users should take ‘due care’ to preserve the information’s security during their work. They should prevent easy access to information to persons who are not authorised to know.



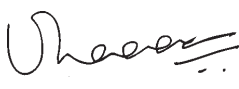
1.3 Media handling and Security

1. Employees / faculty/ should not store confidential information on Desktop or workstation hard disk drives unless authorised.
2. When not being used by authorised employees / faculty or where an authorised person working in a closed area, all hard copy confidential information should be locked in file cabinets, desks, safes, or other furniture. Likewise, when not being used, or when not in a clearly visible and attended area, all computer media (External drives, hard disks, CDs, DVDs, etc.) containing confidential information should be locked in similar enclosures.

Responsibility – Respective HODs / process owners

3. If confidential information should be stored on the hard disk drive or other internal components of a personal computer, it should be protected by either a password access control or by following guidelines of Access Control Policy.

Responsibility – Respective Users.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



4. When confidential Organization's information is erased from a disk, tape, or other magnetic storage media, it should be followed by format operation to prevent the data from later being retrieved. In addition data erase by special software should be used.

Responsibility – IT DEPARTMENT / Respective HODs.

5. When disposed of, all confidential information in hardcopy form (paper, microfilm, microfiche etc.) should be burnt / shredded

Responsibility - Respective HODs.

6. Confidential information when not required should not be discarded in trash bins, recycle bins or other publicly accessible locations.

Responsibility – Respective HODs.

After it becomes no longer needed as per record retention policy, all confidential information should be destroyed either by burning or shredding.



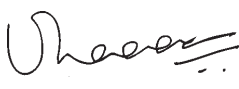
Responsibility – Respective HODs.

7. Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal of condemned e waste, all confidential information should be formatted and / or Erased using a special software . In addition, in case of disposal, the vendor should be an authorised person for handling e waste.

Responsibility – IT DEPARTMENT

8. All confidential information in any form should be protected. Responsibility – Respective HODs / Process Owners
9. When confidential information is written to a External drive, Hard disk, magnetic tape, smart card, or other storage media, the media should be suitably marked with the relevant classification. Unless encrypted, this media should be securely stored.

Responsibility – Respective HODs / Process Owners

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



SECTION 2

Access Control

2.1 Business Requirement For Access Control

Procedures

Areas are categorized into High Risk and Low Risk Areas for the purpose of Access Control.



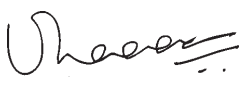
High Risk Area

1. Access to High Risk Area should be authorised by the Head of the Department concerned. Entry should also be supervised and date and time of entry should be recorded.
2. Access to the network, servers, systems and applications should be achieved via logical controls like passwords, which are unique to each individual user. Additional precautions should be taken while allowing access to information systems in the high-risk area. Any access should be assessed prior to giving approval. It should be monitored whether the access is within the defined boundary.

Responsibility– IT Department/ Manager IT /System Administrator / Concerned HOD Or Process Owner

3. Allocation of privileges to access network, servers, systems and applications should be recommended by the officer In-charge of the group concerned and approved by the head of the Department concerned. Additional precautions should be taken while allocation of privileges to access information systems in the high risk area. Any access should be assessed prior to giving approval. It should be monitored whether the access is within the defined boundary. All these privileges should be removed immediately after the set job is completed. Privileges accorded should be clearly recorded in the Log Book. Some of the key privileges should not be granted to the temporary users and if required the necessary things should be carried out by the authorised employee / faculty of the Organization.

Responsibility– IT Department/ Manager IT /System Administrator / Concerned HOD Or Process Owner

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---





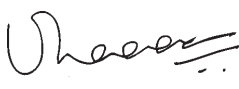
Low Risk Area

Common area where visitors / patients will be visiting regularly. Authentication is not required for their visits to Low Risk areas

2.2 User Access Management

Procedures

1. The Head of the department concerned should authorize the creation of User Ids. These User Ids should be unique, so that user can be linked to and be made responsible for their actions.
2. Check that the user has authorization from the system owner for the use of the information systems and /or services.
3. Check that the level of access granted is appropriate to the business purpose and is consistent with the policy of the organisation.
4. Requirement for the users to sign statements indicating that they understand the conditions of access.
5. Ensure that no access id provided, until the authorization procedure has been completed.
6. Maintenance of a formal record of all persons registered to use the information systems and /or services.
7. Immediate removal of access rights of the users who have changed jobs or left the organization.
8. Periodic checking for the redundant User Ids and Accounts and removal thereof.
9. Ensure that the redundant User Ids are not issued to the other users.
10. Privileges should be allocated to the individuals on a need to Use (do) basis and on an event-by-event basis, i.e. the minimum requirement for performing their functional role only, when needed.
11. An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.
12. Privileges should be assigned to a different User Id from those used for normal business use.
13. System users should sign a statement to keep personal passwords confidential.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



14. Whenever users are required to maintain their own passwords, they may be provided initially with a temporary password, which they should be forced to change immediately on getting access to the resources.
15. User access rights should be reviewed periodically and after any change.
16. Authorization for the special privileged access rights should be reviewed atleast once in a year separately.
17. Privilege allocations should be checked once in a year to ensure that unauthorised privileges have not been obtained.
18. The Head of the department concerned should authorize the creation of User Ids subject to justification by the concerned. Number of such user Ids shall be to the bare minimum and to be monitored with regard to its usage. These User Ids should be unique, so that user can be linked to and be made responsible for their actions.
19. Access / privilege rights should be given with prior authorisation and should be on need basis. Details of which should be given to the concerned user in writing with the user acknowledging the receipt.
20. User should safeguard the details of the access and privilege rights provided and in case of its loss he should change his / her password immediately and should report the matter to his / her superior.
21. User ids not used owing to transfer / change of department / resignation and so on should be disabled at once the information reaches the IT department.
22. Every year, user access should be reviewed by the custodian and remove / change the unwanted ones.



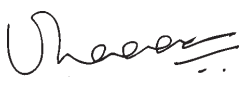
Responsibility: HODs / Manager IT /System Administrator / IT Department

2.3 User Responsibilities

Procedures

1. All users of workstations, PCs / laptops should ensure that their screens are clear / blank when not being used.
2. All unused workstations should be powered off. Responsibility – Respective Users.
3. All network wiring should be fully documented. All unused network points should be de-activated. Redundant cabling schemes should be used where possible.

Responsibility – IT Department

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



4. The use of removable media disks, e.g. External drives, hard disks, and CDs, DVDs, etc., should not be permitted except when specifically authorised.

Responsibility – IT Department/ System Administrator

5. The naming of the Organization's data files should be meaningful and capable of being recognized by its intended users.



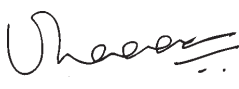
Responsibility – System Administrator

6. Users should delete the temporary files present on their PCs and laptops regularly to prevent possible misuse by unauthorised users.
7. All users of information systems whose job function requires them to create or amend data files, should save their work on the system regularly to prevent corruption or loss through system or power malfunction.
8. User should safeguard the details of the access and privilege rights provided and in case of its loss he should change his / her password immediately and should report the matter to his superior.
9. All employees should treat passwords as private and highly confidential. Non-compliance with this policy could result in disciplinary action. Each individual is accountable for:
 - Providing protection against loss or disclosure of passwords in his or her possession.
 - All activities that occur as a result of deliberately revealing his or her user ID and password.
10. Confidential information should be shared only with authorisation by HODs of the respective Department / Section.
11. The use of removable media disks, e.g. External Drives, hard disks, CD-ROMS should not be permitted except when specifically authorised.
12. Users should logout / lock their workstations or invoke screen savers when they leave their workstation for any period of time.
13. Any unused network wall sockets should be sealed-off and their status should be formally noted. The security of network cabling should be reviewed during any upgrades or changes to hardware or premises.

Responsibility – IT Department.

14. Data directories and structures, and their access privileges should be established by the owner of the information system. Access restrictions to such directories should be applied as necessary to restrict unauthorised access.

Responsibility – Respective Owners.



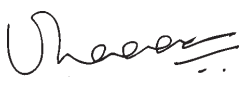
<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



15. Password which can be guessed easily like spouse name, pet name, children name, friends name and those which just change based on month, department name, project name should be avoided. For example, users must not employ passwords like “21Aug” “August29” “abcGM” etc.
16. All user-chosen passwords should contain alphanumeric combination characters or at least one lower case and one upper case alphabetic character and should be Five to eight characters minimum length. Passwords should be changed once in six months.
17. After three unsuccessful attempts to enter a password, the User-ID should be locked until reset by the Administrator.
18. Super / Admin Users should always keep the written down passwords in a sealed envelope. In case the system is down and the concern administrator is not available the sealed envelope should be opened in the presence of two authorised personnel. once the problem is resolved, existing password should be changed and the new password should be written and should be kept in a sealed envelope under lock and key .
19. All users should be made aware of the security requirements and procedures for protecting unattended equipment.
20. An automatic password protected *screen saver* should run after a fixed time period of inactivity .
21. A clear screen policy should be implemented throughout the organisation to avoid opportunistic shoulder surfing.
22. The workstation should be moved to a secure area if its primary function is to process data while unattended.
23. The software programs and network sessions should be configured to ‘timeout’ after a reasonable period of inactive session.

2.4 System And Application Access Control

1. In order to support access restriction requirements, the following controls should be implemented.
 - Providing menus to control access to application system functions;
 - Restrict users’ knowledge of information on application system functions which they are not authorised to access.
 - Controlling the access rights of users, e.g. read, write, delete and execute;

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



- Ensuring that outputs from application systems handling sensitive information contain only the information that is relevant to the use of the users and is sent only to authorised terminals and locations.
2. The sensitivity of an application system should be explicitly identified and documented by the application owner.
- When a sensitive application is to run in a shared environment, the application systems with which it will share resources should be identified and agreed with the owner of the sensitive application.
 - Procedures suggested by the owner shall be followed strictly Responsibility: Respective Users /HODs /System Administrator

Operating System Access Control Policy



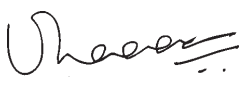
1. To access the Operating System, all users should use their personal User Id only
2. In case of sensitive applications it should be run from a specific terminal.
3. System Utilities like fdisk, fsck, format etc. should be restricted to the IT Department.

Responsibility – IT Department/ System Administrator

Network over WAN should be through dedicated lines or through dedicated telephone line(s)

1. Network services should be made to connect to appropriate ports of the application systems and/or firewalls. Unwanted network services/ ports should be disabled and it has to be periodically checked for any loopholes.
2. Unlimited network roaming should be prevented on the organization's network.
3. Network over locations should be through dedicated lines with backup line as well.

Responsibility – IT Department

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



SECTION 3

Mobile Devices, Teleworking & Cryptography

3.1 Mobile Devices and Teleworking

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.



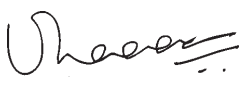
When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices should consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

A policy and procedure supporting security measures should be implemented to protect information accessed, processed or stored at Teleworking sites.

Laptop Security Policy – Procedures: (For laptop owned by the organization)

1. Install OS with advanced security features and latest service packs
2. Update the laptop with latest windows update
3. Use only secure NTFS file system:
 - Windows NTFS file alone provide file and folder level security.
4. Secure Internet Explorer Settings:
 - Some website may have dangerous scripting and ActiveX controls which may damage the Laptop.
5. Disable non-essential Services:
6. Password Management (Refer: User Responsibility - Section 2 , SUB CLAUSE 2.3 ; Points: 14, 15 & 16)
7. Secure the Sharing of Laptop resources
8. Personal firewall should be installed
9. Antivirus software should be installed and should be updated with latest virus definitions

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



10. Wireless LAN should be secured (Refer Section 3, Sub Clauses: 3.2 , 3.3 Cryptographic Controls and Key Management respectively)

Responsibility – IT Department



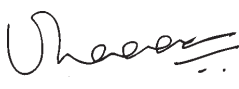
3.2 Cryptographic Controls

1. The appropriate Key should be selected based on the identified wireless devices.
2. IT Department is responsible to ensure that the Key is changed periodically
3. The length of Key selected should be as per the guidance laid down by the regulator or as per the Government's restriction if any.

3.3 Key Management

1. Key should be generated for the use of wireless equipment
2. The Key generated should be noted in a log file .
3. Whenever the Key is modified or replaced, it should be duly approved .
4. Provision of Key to the users should be recorded and authorised.

Responsibility – IT Department

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



SECTION 4

Physical and Environmental Security

4.1 Secure areas

Procedures

1. Organisation should use security perimeters to protect areas which contain information processing facilities. The following controls to be implemented where deemed fit:
 - The security perimeter should be clearly defined
 - The perimeter of a building or site containing information should be physically sound
 - A manned reception area or other means to control physical access to the site or building should be in place

Responsibility : HODS / CHIEF SECURITY OFFICER

2. Secure areas should be protected by appropriate entry controls. The following controls should be implemented in the secure areas:
 - Visitors to secure areas should be supervised
 - Access to sensitive information should be controlled and restricted to authorised persons only.



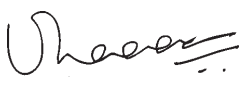
Responsibility: HODS / CHIEF SECURITY OFFICER

4.2 Equipment Maintenance And Security

Procedures

Responsibility for points 1, 2, & 3 : Projects / Electrical Department

- 1 All PCs / Servers / Communication equipment and workstations should be powered with Uninterrupted Power Supply (UPS) systems.
2. If generators are used, they should be regularly tested in accordance with the manufacturer's instructions.
3. Power cables should be segregated from communications cables to prevent interference.
4. Repairs and servicing of all information systems equipment should be performed only by qualified and authorised maintenance personnel
5. Network cabling should be protected from unauthorised interception or damage, for example by using conduit or by avoiding routes through public areas.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



Responsibility - Third party Service Provider / Network Engineer / System Administrator / Manager IT

6. All information systems equipment used for production processing should be maintained in accordance with the supplier's recommended service intervals and specifications.

Responsibility - Third party Service Provider / Network Engineer / System Administrator/ Manager IT

7. Manufacturer's instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields

Responsibility - Third party Service Provider / Network Engineer / System Administrator / Manager IT

8. Adequate insurance cover should be in place to protect all information systems equipment

Responsibility – Network Engineer / System Administrator / Manager IT

9. If Information not required, Storage devices containing sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function.

Responsibility - Third party Service Provider / Network Engineer / System Administrator/ Manager IT

- 10 All items of equipment containing storage media, e.g. fixed hard disks and medical equipments should be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal.



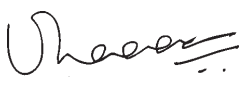
Responsibility - i) IT Assets: IT Department

ii) Medical Equipment: Bio-medical Engineering Department.

- 11 Damaged storage devices containing sensitive data should be sent for destruction to Information Technology Department in case of IT Assets. In case of Medical Equipments, damaged storage devices should be sent to Bio-medical Engineering Department.

Responsibility - i) IT Assets: IT Department

ii) Medical Equipment: Bio-medical Engineering Department.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



SECTION 5

Operations Management

5.1 Operational procedures and responsibilities

1. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. The following process should be considered:
 - Identification and recording of significant changes
 - Assessment of the potential impact of such changes
 - Formal approval procedures for proposed changes.
 - Communication of change details to all relevant persons
 - Procedures identifying responsibilities for aborting and recovering from unsuccessful changes.
2. The concerned head of the department should adopt segregation of duties for reducing the risk of accidental or deliberate system misuse.
3. A formal change control process should be established to move application software from development to production environment. This movement should be approved by HOD of IT Department /Manager IT and Concerned HODs.
4. The separation of business application software in development from business application software in use and business application software in testing should be achieved via physically separated computer systems.



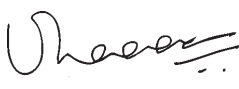
Responsibility – Manager IT / Network Engineer / System Administrator

5. Software features which could be used to compromise security, and which are clearly unnecessary in the Organisation's computing environment, should be disabled at the time of installation of software on multi-user systems.

Responsibility – Manager IT / Network Engineer / System Administrator

6. Editors and other system utilities should not be accessible/available from/ in production/ Business systems.

Responsibility – Manager IT / System Administrator

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



5.2 Protection from malware



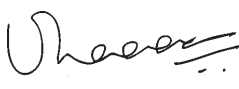
1. If users suspect infection or warned about an attack by a malicious software they should report it to the IT Department / Head of the Department / Network Engineer / System Administrator / Manager IT
2. Employees should not download software from the Internet, or any other systems using the system provided by the organisation.
3. The only exception to the use of externally provided software is when such software has first been tested by Network Engineer / System Administrator / Manager IT and approved by the HOD of IT Department
4. Network Engineer / System Administrators / Head of the Departments should ensure that Anti-Virus software is installed and continuously enabled on all local area network (LAN) servers and personal computers (PCs) of their respective departments.
5. Employees should not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any Organisation's computer, network, or information.

5.3 Back-up

1. Backup processes should be performed periodically, and with sufficient frequency. Using Quest Software and EMC storage for applications .
2. Data backups should be taken and maintained.
3. Backups should be taken on daily basis where data is critical to the business.
 - Server anti-virus updating log should be maintained in the server.
 - Server Back-up logs detail should be maintained in the server.

Responsibility: IT Department/ Network Engineer / System Administrator /Manager IT

4. When software environment is created or changed, including change of version.
 - A backup on the new software environment has to be taken. The backup should include application software, operating system, configuration details and databases. The implementation document and the procedures should specify these details also.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



5. Recovery and restoring of data files.

- It should be ensured that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files. Restoration procedures should be well tested and scripts should be available.

6. Restarting or recovering your system.

- Information system owners should ensure that adequate backup and system recovery procedures are in place and working satisfactorily.

Following process should be followed :



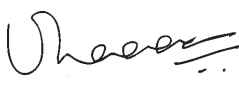
- i) Log of contents should be stored in the system in an identifiable manner
- ii) A backup register should be maintained with details in the system such as :
 - A) Backup date/time
 - B) Place of storage
- iii) Periodic testing of backup for its readability and usability
- iv) Backup of the prior versions of production systems software and production application software should be maintained to quickly revert back in case of updated software has some problem.

Responsibility: IT Department/ Network Engineer / System Administrator /Manager IT

OFFSITE BACK UP / DISASTER RECOVERY MANAGEMENT

It is recommended to have off-site backup and should be stored in a place away from main building / hospital where Data centre is located, as part of disaster recovery management and business continuity plan (BCP) . It is recommended to conduct periodical BCP drills .

Responsibility: IT Department/ Network Engineer / System Administrator /Manager IT

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



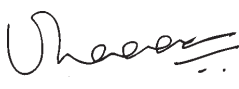


5.4 Logging and Monitoring

Procedures

Responsibility: IT Department/ Network Engineer / System Administrator /Manager IT

1. Systems should be monitored to detect deviation from access control policy by using event logging and recording monitor able events in Audit Logs to provide evidence in case of security incidents.
2. Audit logs, recording exceptions and other security-level events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs should also include:
 - a. User Ids;
 - b. Dates and times for log-on and log-off;
 - c. Terminal identity or location, if possible;
3. The following areas should be monitored:
 - a) Authorised access, including details such as:
 - The user ID;
 - The date and time of key events;
 - The type of events;
 - b) All privileged operations such as:
 - Use of Administrator / supervisor account;
 - c) Unauthorised access attempts, such as;
 - Failed attempts;
 - d) System alerts or failures, such as:
 - Console alerts or messages;
4. The result of the monitoring activities should be reviewed regularly.
5. System logs should be reviewed regularly.
6. System logs should be secured so as to prevent any alteration. It should be noted that tampered system logs give a false sense of security. Controls should aim to protect against unauthorised changes and operational problems including:
 - i. The logging facility being disabled;



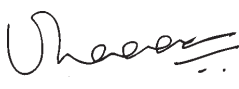
<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



- ii. Alterations to the message types that are recorded;
 - iii. Log files being edited or deleted;
- 7 Sufficient disk space should be provided on the system to prevent overwriting of logs frequently.
 8. Backup of system logs should be taken when the log size touches earmarked limit.
 9. Designated Personnel of IT Department should review settings on a periodical basis.
 10. In the case of Linux, Copying sensitive system commands into unsecured directories provides an easy access to unauthorised users. These files should be immediately removed or moved to an appropriate directory. “var/adm/message” file can be reviewed both for identifying security problems and for identifying valid executable programs.
 11. In the case of Linux, Unauthorised changes to the system files like etc/passwd, protected password, /etc/group, /etc/inetd.conf files, the “r” (remote) commands, cron files and the kernel may compromise system integrity. Personnel of IT Department should review for unauthorised changes to the files at least once in a year. By turning on /etc/inet/ inetd.conf by using inetd-t flag, logs of access attempts to the file can be compiled and reviewed.
 12. System Administrator should periodically review to ensure that the server configuration and other files provided alone are on the system.
 13. A full system partition may result in the denial of processing provided by the host. System Administrator should review disk space utilization periodically, and format / re-partition all disks installed on the system prior to use.
 14. Disable any service that does not serve a strong business need.
 15. TCP ports are popular back door for attackers to install on TCP port. The risk of transferring unauthorised files across the network is very high. Services approved only should run on TCP ports (Transport Control Protocol Ports).

5.5 Control of operational software

1. Ensure that the users give complete requirements regarding the changes requested and these requests are authorised prior to taking them for consideration.
2. Changes in application systems should be implemented with prior review by designated personnel In IT Department / Manger IT and approval from HODs / Head Of IT
3. Support programmers should be given access only to those parts of the system necessary for their work, for which change has been approved.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



4. Wherever changes are to be carried out, all computer software, information, database entities and hardware should be identified for carrying out the changes.
5. Staff responsible for development of application systems is also responsible for developing necessary security controls into the project and support environment. Existing controls and integrity procedures should ensure that application systems and operating systems should not be compromised by the changes.
6. Designated personnel of IT department / Manager IT should review the change control request proposals and approved by concerned HODs / Head of IT.
7. Implementation of changes should be carried out at suitable time so as to minimize business disruption.
8. System documentation should be updated with all changes after the old documentation is archived. User procedures /manuals, operational instructions should be updated or written to reflect the changes carried out.



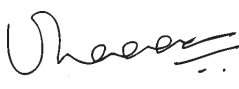
Version Control:

9. Version control or history should be maintained for all software updates.
10. All change requests should be serially numbered.
11. Development / Testing and production environment should be segregated.
12. Changes should be submitted and accepted prior to implementation by authorised users.
13. Formal version control procedures should be used for maintaining versions of the application.
14. Backup of the prior versions of production systems software should be Taken and maintained.
15. All historic versions of each source code should be retained.
16. The changes made in the application systems should not adversely impact the existing controls and integrity.

Responsibility: Third Party Service provider / Designated Individual In IT Department / Manager IT

5.6 Technical Vulnerability Management

1. Periodical vulnerability assessment of network to be done
2. Vulnerability assessments should be planned in such a way that it does not affect the Organization's day-to-day operations.
3. Procedures for testing should be discussed and clearly documented.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



4. Responsible personnel should be identified to co-ordinate the assessment and take necessary remedial actions either with the help of the IT department or with vendors as the case may be.
5. All test results, recommendations and actions taken should be documented.
6. After addressing the issues, if any a subsequent assessment should be undertaken to ensure effectiveness.
7. The results should be communicated to the respective information owners and Custodians
Responsibility: Third Party Service Provider /Designated Individual / Manager IT

Restriction on software installation

Rules governing the installation of software by users should be established and implemented
The organization should define and enforce strict policy on which types of software users may install.

The principle of least privilege should be applied. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted having regard to the roles of the users concerned.

Responsibility: Network Engineer / Designated Individual / Manager IT

5.7 Information systems audit considerations

Information systems audit controls



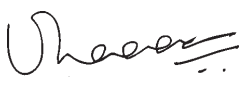
Audit / Review requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

Implementation guidance

The following guidelines should be observed:

- a) Audit/Review requirements for access to systems and data should be agreed with Management;
- b) The scope of technical audit /Review tests should be agreed and controlled;
- c) Audit /Review tests that could affect system availability should be run outside Business hours;

Responsibility: Network Engineer / Manager IT / Head - IT / System Auditors

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



1. An internal pool of Auditors/ Information Technology & Security professionals Having adequate knowledge and training should be engaged.
2. HOD - IT Department / Internal Auditors / Manager IT / should prepare an Annual Audit / Review Plan.
3. Based on the Audit /Review Report, Audit Team should suggest modifications if any, in the Information Technology And Security Policy & Procedure and action should be initiated.

5.8 Compliance with Legal and Contractual Requirements Procedures

1. Employees of the Organisation should not attempt activities (like hacking, port scanning) prohibited by the Information Technology Act, 2000.
2. Whenever it is planned to outsource penetration testing, a formal agreement should be entered into with the consultants authorizing them to conduct the test
3. The system of storage and handling should ensure clear identification of records and of their statutory or regulatory retention period. It should permit appropriate destruction of records after that period if they are not needed by the Organization.
4. When records are converted from paper to non-paper form, the following controls should be in place.
 - Master creation details sheet authenticated by the HODsExample:- Account-wise balance are listed and tallied



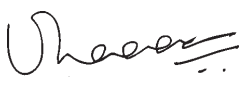
Whenever the underlying paper documents are subsequently destroyed and the converted format becomes the prime record a certificate of authenticity should be made at the time of conversion and is signed by the official responsible for overseeing the conversion process.

Identification of applicable legislations

Relevant statutory, regulatory and contractual requirement and the organizations approach to meet these requirements should be explicitly defined, documented and kept up to date for the areas covered by this policy and procedure

Intellectual Property Rights (IPR)



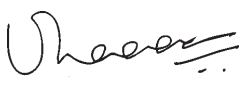
Appropriate Procedure should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



Following Process Should Be Followed :

- i) List of software assets should be maintained
- ii) Training and awareness on IPR should be conducted
- iii) Unauthorised coping of software should be prohibited.
- iv) Coping of software should be done for backup purpose as permitted by copyright law

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---





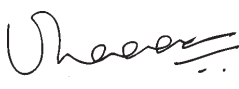
SECTION 6

Communications Management

6.1 Network Security Management

Network Controls

1. Any direct connection between the Organization's systems and computers at an external location / organizations, via the Internet or any other public network should be established after proper approval .
2. Organisation computers or networks may only be connected to third party computers or networks after proper approval, so that the connected system will be in compliance with Organization's security requirements.
3. Network Engineer / System Administrator should maintain the inventory of communication equipment / lines and should be updated periodically. Inventory should have complete details on the make, model, manufacturer, contact address of the manufacturer /dealer, contact center details for problem resolution
4. Movement of equipment across the locations should be authorised by the HOD of the concerned department / Manager IT / HOD - IT Dept. and entry to be made in the inventory list.
5. Configuration of the network equipment should be done in accordance with the recommended methodology as suggested by the equipment vendor and as per the standards relating to Router Security , Firewall Security , and organisation's Access control policy in such a way that the security of information system is not compromised.
6. Patches should be applied periodically to the communication equipment based on the recommendations of the equipment vendor. These should address the latest security risks and requirements of Access Control Policy in such a way that the security of information system is not compromised.
7. Configuration changes and application of patches should be carried out with prior approval after assessing the need for such a change. All these request / approval should be preserved for future reference.
8. Network Engineer / Manager IT / HOD - IT Dept. should propagate the details of new technology, safe techniques to handle the net, need for not tampering with the settings and so on through the normal training programs of the Organization.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



9. Network Engineer / Manager IT should be responsible for the detection and reporting of dropped communication links, termination of the associated computer services when the line drops and re-authentication when the link is restored.
10. Network Engineer / Manager –IT should be responsible for enabling the network services for business reasons only and for removing /disabling the unused/unwanted network services.
11. Network Engineer / Manager IT should maintain the master documents supplied by the network equipment vendors, parameter setting details, scripts, configuration files used for installation and operation of the network OS.
12. HOD - IT Dept. / Manager IT / System Administrator should initiate a process to procure a Network Management Software / Remote Management Software for managing the distributed network infrastructure in terms of monitoring, configuring and maintaining the availability of network devices and the associated services.
13. Groups of information services, users and information systems should be segregated on networks. Virtual Private Networking (VPN) can be used to segregate users such as users in Various Colleges , buildings, Clinics , doctors, administration, outsourced vendor, etc. Agreements with vendors providing network services should include IS combinations such as Non-Disclosure agreements, etc.



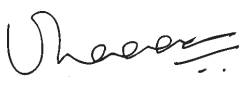
Responsibility : Manager IT / Network Engineer

6.2 Information Transfer

Exchange of information and software between and within organizations should be based on formal exchange policy, carried out in live exchange agreements and should be compliant with any relevant legislation.

6.2.1 Information transfer policies and procedures

- 1) Employees, third party / external parties and any other user should not compromise the Organisation's Interest, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorised purchasing, etc.
- 2) Procedures should be followed for detection of and protection against malicious code that may be transmitted through the use of electronic communications.
- 3) Procedures should be followed for protecting communicated sensitive electronic information that is in the form of an attachment; (Refer E-mail Policy).
- 4) Procedures should be followed regarding the use of wireless communications, taking into account the particular risks involved.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---





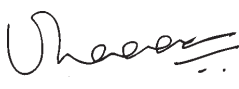
- 5) Retention and disposal guidelines for all business correspondence, including messages should be followed
- 6) Users should not leave sensitive or critical information on printing facilities, e.g. copiers, printers, and facsimile machines, as these may be accessed by unauthorised personnel;
- 7) Personnel should take appropriate precautions, e.g. not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by:
 - i) People in their immediate vicinity particularly when using mobile phones;
 - ii) Wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers;
 - iii) People at the recipient's end;
- 8) Personnel should be aware of the problems of using facsimile machines, namely:
 - 1) Unauthorised access to built-in message stored to retrieve messages;
 - 2) Deliberate or accidental programming of machines to send messages to specific numbers;
 - 3) Sending documents and messages to the wrong number either by misdialing or using the wrongly stored number.
- 9) Personnel should not register demographic data, such as the e-mail address or other personal information in any software.
- 10) Personnel should be aware that facsimile machines and photocopiers have page caches and store pages in case of a paper or transmission fault, which will be printed once the fault is cleared.

6.2.1.1 Electronic messaging & E-mail policy

Electronic messaging

Security considerations for electronic messaging such as e-mail should include the following:

- 1) Protecting messages from unauthorised access, modification or denial of service;
- 2) Ensuring correct addressing and transportation of the message;
- 3) General reliability and availability of the service;
- 4) Legal considerations, for example requirements for electronic signatures;

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



- 5) Obtaining approval prior to using external public services such as instant messaging or file sharing;
- 6) Stronger levels of authentication controlling access from publicly accessible networks.

E-mail policy

Objective of the policy.

To ensure that emails (electronic mails) stored or transmitted using the organisation's facilities should be used only in accordance with the need for business communication and based upon criterion defined from time to time by the management.

Procedures:

1. To enhance productivity, information sharing and reduce paper cost, the organisation has procured an **internet based email service** that is meant to be used for effective communication with other organization's staff, business partners and others.

To facilitate this, the organization has allowed staff to get an email id that consists of a User Id chosen by them or allotted prefixed to the words "**@sriramchandra.edu.in** " thus signifying that the mail and all contents are dealing with matters pertaining to the organisation. In addition, every department can have a generic e-mail id for the general use of that department's operational needs.

The organisation has also provided facility to post mail to recipients and receive mail from other sources.



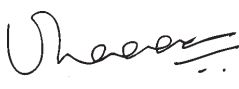
2. All persons who have a need on access to e-mail services of the organisation can ask for and should be shown a "read only" copy of the policy. In addition, for discussion or information, extracts can be provided.

The organisation encourages persons to be conversant with the policy and apply relevant portions in their daily work.

3. Legal obligations

By using the e-mail services, infrastructure and equipment, Faculties / employees are automatically deemed to have agreed not to violate the policy or guidelines or norms.

It should be noted that Faculties / employees don't have the right to deviate from the policy or not use the e-mail services etc just because they may or may not agree with some parts of or the whole policy.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



In the case of outside persons (other than faculties /employees), the department responsible for inducting them should inform them about the existence of the policy and doubts and clarifications about the obligations and rights should be provided.

However, once they begin to use the services, infrastructure or equipment, they are also deemed to have agreed to go by the policy guidelines.

4. Related to the user.

Who can have an account.

Any employee /faculty / consultant authorised to use the official mail is eligible to have an e-mail account. Account Opening has to be approved.

Note however that eligibility for an e-mail account doesn't automatically qualify the user for a desktop or access to computer resources.

Account opening.

Submit a requisition mail / letter to Web administrator for account opening.

It should be authorised by the HOD of the concerned employee / faculty of the department for whom Email account has to be opened.

Confirm that the e-mail id you have asked for is available.

Web administrator needs one working day to register and energize the new account.



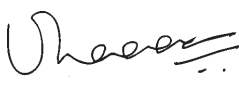
Change the password during first time access of the email after obtaining the access permission to operate an official email account.

5. Organisation's property.

As a productivity enhancement tool, organization encourages the business use of electronic communications. Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Sri Ramachandra Institute of Higher Education & Research (Deemed To Be University), and are not the property of users of the electronic communications services.

6. Authorised usage.

Organization's electronic communications systems generally should be used only for official activities.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



The policy provides for storage of mail and attachments upto a reasonable volume and all associated services like personalised address books, folders and mail classification. The structure is standard, is based on the priority assigned and it is not possible to exceed it. Once the data storage limit is exceeded, a cautionary notice is issued to the user to purge the data.

Employees are reminded that the use of organization's resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

7. Unauthorised usage.



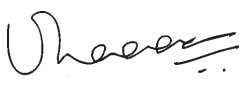
Users are forbidden from using organization's electronic communications systems for personal purposes - however good or popular the endeavor may be. Following constitutes unauthorised use :

- Messages and attachments of a denominational nature,
- Unofficial circulars or chain mail of any content
- Managing the affairs of professional bodies or societies to which users may belong,
- Private business activities,
- Amusement/entertainment purposes,
- Forwarding/attaching software - specially pirated software,
- Attempting to know others' passwords,
- Inappropriate written or graphic material.
- Using the email to originate and spread hate against groups, communities and genders,
- Violating any applicable state, central government or common law.

8. It is forbidden for anybody to communicate patient related information / student related information /faculty related information in individual form or as aggregate information for any reason whatsoever without the explicit written consent on a case by case basis by the concerned authority .

9 All malicious acts or deliberate attempts to deviate from normal e-mail use are forbidden. Examples could be:

- Using the e-mail handle (myid@sriramachandra.edu.in) provided to misrepresent yourself as somebody you are not. This is like a visiting card.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



- Using the e-mail to communicate with external parties and committing the organisation to inappropriate effort and cost .
- Using someone else's e-mail account either by misusing the password or finding a desktop with an open e-mail session.
- Discussing password or related installation and facility details with friends or former colleagues or business partners.

10. Account closure or suspension.

Accounts are normally closed (retired) when the employee / faculty leaves the services of the organization. However in exceptional cases - usually as a disciplinary measure - the organization may suspend or close the account of an existing employee / faculty

11. Privileges for operating the department's mail account.

Employee privileges for using electronic communications systems should be assigned only to those persons necessary to perform a job using the mailing system . With the exception of emergencies and regular system maintenance notices, broadcast facilities should be used only after the permission of the concerned authority.

12. User separation.



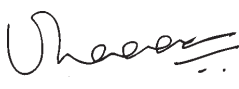
These facilities should be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems should employ user IDs and associated passwords to isolate the communications of different users. All faculty and employees authorised should have unique usernames and passwords to access the e-mail system.

13. User accountability.

Regardless of the circumstances, individual passwords should never be shared or revealed to anyone else besides the authorised user.

The user in whose name the account is opened is always responsible for all mail that originates from or is transmitted by or stored from his / her mail account.

If users need to share computer resident data, they should utilise message forwarding facilities, public directories on local area network servers, and other authorised information-sharing mechanisms. To prevent unauthorised parties from obtaining access to electronic communications, users should choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



14. No special protection.

Employees / faculty are reminded that organization's e-mail data is not specially protected or encrypted. If sensitive information should be sent by electronic communications systems, encryption or similar technologies to protect the data should be employed.

15. Respecting privacy rights.

Except as otherwise specifically provided, employees / faculty may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. Organisation is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

However, Organisation also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

16. No guaranteed message privacy.

Organisation does not guarantee that electronic communications will be private. Employees / faculty should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

17. Regular message monitoring.



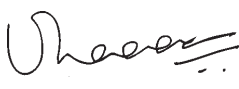
It is the practice of the organization not to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities.

18. Statistical data (of e-mail usage).

Consistent with generally accepted business practice, organisation authorises the IT Department to collect statistical data about electronic communications. Using such information, Information Technology (IT) staff can monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.

19. Incidental disclosure.

It may be necessary for support staff to review the content of an individual employee's communications during the course of problem resolution. Support staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



20. Message forwarding.

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive information should not be forwarded to any party outside the organization without the prior approval. Blanket forwarding of messages to parties outside the organization is prohibited.

21. Attachments.

Users of the e-mail system should send attachments only as related to the needs of the assignment.

22. Purging electronic messages.

Messages no longer needed for business purposes should be periodically purged by users from their personal electronic message storage areas. It should not be used as a permanent data / information backup area.

23. Information movement.

All attachments downloaded from non- organisational sources should be screened with virus detection software prior to being opened or run.

Users should not place organisation's internal information in any location, on machines connected to organization internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.



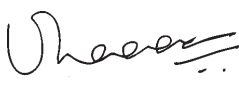
6.2.1.2 Credit card payment services security

The Authorization slip, which contains the credit card no. should be protected, since it is confidential

6.2.2 Agreements on Information Transfer

The security content of any agreement should reflect the sensitivity of the business information involved.

Agreements may be electronic or manual, and may take the form of formal contracts or conditions of employment. For sensitive information, the specific mechanisms used for the exchange of such information should be consistent for all organizations and types of agreements.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



Exchange Agreements Should Consider The Following Security Conditions:

- 1) Responsibilities for controlling and notifying transmission, dispatch, and receipt;
- 2) Procedures for notifying sender of transmission, dispatch, and receipt;
- 3) Procedures to ensure traceability and non-repudiation;
- 4) Minimum technical standards for packaging and transmission;
- 5) Escrow agreements;
- 6) Courier identification standards;
- 7) Responsibilities and liabilities in the event of information security incidents, such as loss of data;
- 8) Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; (Refer Information Classification under Asset Management)
- 9) Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations (Refer IPR, Data Protection and Personal Information)



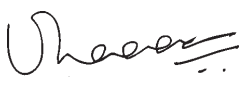
6.2.3 Confidentiality or non-disclosure agreements

Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, regularly reviewed and documented.

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties and employees of the organization. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



SECTION 7

Systems Acquisition, Development and Maintenance

7.1 Security Requirements of Information Systems

7.1.1 Information Security requirements analysis and specification

1. Statements of business requirements for new systems, or enhancements to existing systems should specify the requirements for controls.
2. Specifications should consider the automated controls to be incorporated in the system, and the need for implementing manual controls.
3. Security requirements and controls should reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security.
4. Controls should be identified at the design stage. Controls at the design stage are cheaper to implement and maintain than those included during or after implementation.
5. User department management should consider security requirements early in the systems development life cycle (SDLC).
6. It is the information owner who is responsible for incorporating relevant controls into a system.



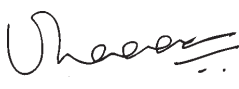
Responsibility : HODs / IT Department

7.1.2 Securing application services on public networks

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls should be followed. Controls required often include cryptographic methods for authentication and securing data transfer.

Application services should use secure authentication methods, e.g. using public key cryptography and digital signatures to reduce the risks. Also, trusted third parties can be used, where such services are needed. Proper Service level agreements(SLAs) from such third parties should be obtained. SLAs should include Non-Disclosure & confidentiality clause.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



7.1.3 Protecting application services transactions

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

The extent of the controls adopted should be commensurate with the level of the risk associated with each form of application service transaction.

Transactions should comply with legal and regulatory requirements in the jurisdiction which the transaction is generated from, processed via, completed at or stored in.

7.2 Security in development and support processes

7.2.1 Secure development policy

Rules for the development of software and systems should be established and applied to developments within the organization.

Secure development is a requirement to build up a secure service, architecture, software and system.

Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use.



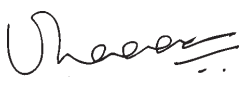
7.2.2 System change control procedures

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Formal change control procedures should be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts.

Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, and quality control and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised. Support programmers are given access only to those parts of the system necessary for their work and that formal agreement and approval for any change is obtained.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



7.2.3 Technical Review Of Application After Operating Platform Changes

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

This process should cover:

- review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes;
- ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation;
- ensuring that appropriate changes are made to the business continuity plans

Operating platforms include operating systems, databases and middleware platforms. The control should also be applied for changes of applications.

7.2.4 Restrictions on changes to software packages

Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.

If changes are necessary, the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorised software. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades.

7.2.5 Secure Development Environment



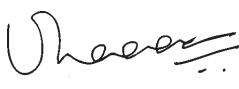
Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

A secure development environment includes people, processes and technology associated with system development and integration.

7.2.6 Outsourced development

The organization should supervise and monitor the activity of outsourced system development given to a third party contractor / vendor

Licensing arrangements, code ownership and intellectual property rights related to the outsourced content should be established.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---



Acceptance testing for the quality and accuracy of the deliverables should be carried out to ensure that the delivered product confirms to the specifications approved and accepted . Such acceptance test should be carried before deploying it in the production environment

Arrangements for continuous support for the developed product should be established by entering into product support agreements with the third party contractor / vendor . Such support agreements should include non –disclosure and confidentiality clause.

The organization remains responsible for compliance with applicable laws and control efficiency verification.

7.2.7 System security testing

Testing of security functionality should be carried out during development.

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. The extent of testing should be in proportion to the importance and nature of the system.

7.2.8 System acceptance testing

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

System acceptance testing should include testing of information security requirements along with the testing of completeness of user specifications / requirements . The testing should also be conducted on received components and integrated systems.

Testing should be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization’s environment and that the tests are reliable.



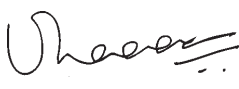
7.3 Test data

7.3.1 Protection of test data

Test data should be selected carefully, protected and controlled.

The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data. Such test data should be protected and controlled.

<p>Prepared By</p>  <p>Mr. Balaji Srinivasan Head-Information Technology</p>	<p>Reviewed By</p>  <p>Dr. S.P. Thyagarajan Prof. of Eminence & Dean (Research)</p>	<p>Approved By</p>  <p>Dr. P.V. Vijayaraghavan Vice Chancellor</p>
---	--	---