SRI DEVARAJ URS ACADEMY OF HIGHER EDUCATION AND RESEARCH

A Deemed to be University
Tamaka, Kolar, Karnataka.

Declared under Section 3 of the UGC Act, 1956
vide MHRD, Government of India Notification
No.F-9-36/2006-U.3 (A) dated 25th May 2007

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

SRI DEVARAJ URS ACADEMY OF HIGHER EDUCATION & RESEARCH

A DEEMED TO BE UNIVERSITY, (DECLARED UNDER SECTION 3 OF THE UGC ACT, 1956)

TAMAKA, KOLAR 563101, KARNATAKA, INDIA

Name of the Policy/ Guidelines	Information and Communication Technology Policy	
Short Description	The policies and procedures pertaining to information systems	
Scope	This policy is applicable to all the administrative officers, faculty and non- teaching staff of the constituent colleges and departments of SDUAHER (Deemed to be University).	
Policy status	☑ Original ☐ Revised	
Date of approval of Version 1	**12 October 2020**	
Revision No.	0	
Brief description of last revision	Not Applicable	
Date of approval of current revision	Not Applicable	
Effective date		
Approval Authority	Board of Management	
Responsible officer	Registrar	
Name of the Policy/ Guidelines		
Details of division	Date of Revision	Approved by

1.0. Introduction:

Effective management of information is crucial for higher service effectiveness and efficiency levels. Effective systems and procedures will helps in achieving and fulfilling the quality objectives. This document describes the policies and procedures pertaining to information systems which provide relevant information to the staff, management, external agencies and the patients.

The purpose of the ICT Department is to plan, design, develop and maintain the information technology infrastructure, in alignment with the strategic objectives. Functions include, but are not limited to, information technology planning and evaluation, purchasing, hardware and software installation, providing ongoing user support and training, implementing management standards and policies and procedures related to information technology processes, and providing for network and information security.

2.0. ICT Department Staffing:

The composition of the ICT department and the primary responsibilities and functions of its staff are:

2.1 ICT-HEAD:

2.1.1 Smooth functioning of the department
2.1.2 Organizing the training program's for new applications or new software
   a. Implementing the new applications/ software/ versions
2.1.3 Overall supervision of the ICT department
2.1.4 Approval for providing the statistical and patient data for clinical research or other purposes
2.1.5 To provide for a liaison between the ICT department, users and the Hospital Management.
2.1.6 Collecting the feedback from all the user departments.
2.1.7 Managing the Mail server, creating mail ids and assigning quota to the Mail ID
2.1.8 HIS & LIS installation/ support/ training
2.1.9 Approving authority for providing privileged communication.
2.1.10 Website update and Servers management.
2.1.11 Router(Wi-Fi) configurations.

2.2 System Administrator:

2.2.1 HIS & LIS and other softwares installation/ support/ training
2.2.2 Administration & Maintenance of HIS & LIS and other software applications

2.2.3 Users policy, Roles creation
2.2.4 Attending to all the complaints related to HIS and other software in use
2.2.5 Maintenance of all applications
2.2.6 Monitoring systems and server side software to ensure systems are working.
2.2.7 Escalating problems pro-actively & Collecting and reporting errors and improvements to appropriate teams.
2.2.8 Creating and maintaining a knowledge base, support scripts, documentation and
    a. Procedures.
2.2.9 Implementation of all software
2.2.10 Coordinating between the developers and End users.
2.2.11 Preparing of Training plans and training to the user

2.3 Jr. System /Hardware Executive:

2.3.1 Checking the backup status
2.3.2 Administration & Maintenance of LAN, Setting up desktop PCs.
2.3.3 Attending to all the hardware related complaints
2.3.4 Handling the network related complaints.
2.3.5 Setting up the connectivity for telemedicine and video conferencing and also troubleshooting
2.3.6 Monitoring and updating Anti-Virus updates in Server & Clients.
2.3.7 Attending to problems pertaining to existing desktops.
2.3.8 Ongoing fault diagnosis and support.
2.3.9 Configuring/reconfiguring desktops as per profiles of the user
2.3.10 Preventive measure
2.3.11 Software installation (MS Office.adobe reader, chrome,firefox etc.)
2.3.12 Configuration of outlook express
2.3.13 Alternate day checking all the systems
2.3.14 On call support
2.3.15 Network health to be checked
2.3.16 Troubleshooting
2.3.17 Installation and configuration
2.3.18 User data back up
2.3.19 Maintenance of the Printers, scanner, 1kv ups, desktops etc.

3.0 Information Needs of the Hospital:

The various information needs that are identified for the effective and efficient functioning of the hospital are listed below:

3.3.1 Demography of the patients
3.3.2 Medical records of the patients
3.3.3 Service scope of the hospital
3.3.4 Investigation results
3.3.5 Billing
3.3.6 Pharmacy
3.3.7 Employee Records
3.3.8 Purchase
3.3.9 Store Data
3.3.10 Summarized information from various areas for management decision making.
3.3.11 External agencies, business associates etc. and their requirement

4.0 Strategies to meet the information needs of the hospital:

The hospital has employed both manual and computerized systems to meet the current information needs. The hospital is also in the process of implementing an integrated hospital information system to manage the information needs in an efficient and effective manner. The following table describes how the various information needs are met currently

Information Need	**System/Process**
Demography of the patients	Patient demography is captured in HIMS at the time of registration. This is the master copy of the patient demography that is used at various areas in the hospital.
Medical records of the patients	The medical records in the form of OP cards or IP case-sheets are hand written and are kept under the safe custody of the medical records department. The medical records index data and the file movement information are tracked in the HIMS. Now the medical records are stored in N/w storage.
Service scope of the hospital	The service scope, departments/medical specialties and facilities, doctors and their OP timing are displayed in the hospital, made available to the front office staff in HIS and provided in the hospital website.

Investigation results	The lab investigation requests and results are captured in the LIS module of HIMS. Other investigation results are prepared and a copy of the same are kept at the service centers.
Billing	Hospital billing is carried out in HIMS. The list of service items and their rates are maintained in HIMS. For credit billing, the list of TPA, companies, the agreed package or item rates, reference codes, coverage etc. are also maintained in the system
Pharmacy	The drug list, order, stock, billing are computerized.
Employee records	Employee records are maintained both physically and electronically. The physical employee record contains the personal particulars, copy of qualification and registration certificates, copy of offer letter and appointment letter, reference check, credentials, medical check-up etc. The electronic record contains attendance, leave and payroll related information
Purchase	The hospital follows manual and online procurement process and the records are kept in the purchase department.
Store data	The items on delivery are captured into the store system. The hospital currently follows manual and online intending and the approved requests are captured in the store system at the time of issuing the items.
Summarized information from various areas for management decision making.	Information for management decision making are captured and processed in HIMS, HR, Store, Pharmacy, Accounts system etc. The various information that are made available electronically include: Daily and periodic revenue collection Various statistics on OP, IP, OT, ICUs, bed occupancy, resource utilization, births, deaths etc. Material consumption, sales volume, sales pattern etc. Department wise headcount, attrition,

	leave etc. Periodic financial information
External agencies, business associates etc. and their requirements	Hospital Administration office maintains a database of vendors, referring doctors/institutions etc. for easy communication

5.0 ICT Procurement and Acquisition Policy:

The purpose of this policy is to provide a framework for the procurement of ICT hardware and software within the hospital. This policy outlines the procedures that must be in place to ensure that the purchase, delivery and installation of ICT equipment are coordinated successfully.

5.1.1 The end-user line managers make request for desktop hardware, software, peripheral devices etc.
5.1.2 Top management makes decision on procurement of major ICT systems
5.1.3 ICT related hardware and software will be specified by the Head of ICT

5.1.4 The Head of ICT will make a decision whether to approve, decline or amend the requirements for the purchase of the equipment from users.
5.1.5 If the equipment is approved then ICT will order the equipment directly with purchase.
5.1.6 Equipment suppliers are also recommended by the ICT Department but may be changed, in agreement with the Head of ICT, by the Purchase Department in favor of a better price or service.
5.1.7 The ICT Department requests that equipment be delivered to the ICT Department. Here it can be checked for damage and compliance with the ordered specification before being set up and transported to its final destination.
5.1.8 The ICT Department is responsible for arranging delivery of the equipment from the ICT Department to its intended destination
5.1.9 The ICT Department has a standard set-up procedure for new hardware, software and systems. This procedure ensures the equipment is configured correctly and that all ICT security measures are addressed. This includes the set-up of passwords, anti-virus software etc.
5.1.10 ICT department is responsible for the procurement/design of application software packages in line with top management policy decisions.
5.1.11 Implements these packages in conjunction with vendor personnel.
5.1.12 Trains hospital users and develops system interfaces to link various packages into a consistent whole

6.0 Computer Network:

The ICT network physical infrastructure is provided as a central platform for all users of the Hospital Information and other Computing Environment. The network infrastructure is managed by the ICT department both through its own resources and via support contracts and other external supplies.

The LAN employs a switched 10/100/1000 Ethernet architecture at data transfer rates of 1000 Mbps . Devices on the network, such as computers, servers, printers, copiers, are arranged in a Tree topology, where all devices are connected to a network switch or hub. Network devices are connected with category 5e/6 unshielded twisted pair cables and fiber optic cables. Category 5e/6 unshielded twisted pair cabling is the most widely used media to connect the network devices. Fiber optic cabling is used Main switch

Network Hardware:

Core and Distribution Switches: CISCO
End point Switches: D-LINK
Firewalls: SOPHOS XG 450
Servers: DELL Power Edge R530 -2 Num, DELL power Edge R420 -3 Num, IBM x3650 M2 -2 Num, Think serverST50(Lenovo)

Network Security Policy:

All connections to the hospital network infrastructure will be made and coordinated through the ICT department.

7.0 Computer Hardware and Software:

The ICT Department selects specific computer hardware for business need, stability, proven effectiveness in the workplace, cost-effectiveness, ease of use and ease of support. Following is the list of Major ICT equipment's that are currently in use:

a) Servers – DELL Power Edge R530 -2 Num, DELL power Edge R420 -3 Num, IBM x3650 M2 -2 Num, Think serverST50(Lenovo)

b) Desktop Computers – Acer, HCL, Dell

c) Laptop Computers – Lenovo, HP

All Servers & Storage utilize RAID 5 storage, creating a stable and redundant hardware solution allowing one hard drive to fail without data loss. Servers include redundant fans and power supplies ensuring maximum system up time.

7.1 Server Room:

ICT department keeps all the major ICT equipment in the Server Room and the door to the server locked. Only authorized ICT staff have access to the server room. Each server is password locked when not in use, requiring a domain user name and password to access the servers.

7.2 Standard Desktop Software Configuration:

- Windows 7 Professional, or Windows 8.1 operating system and windows 10
- Google Chrome, Mozilla Firefox
- Adobe Acrobat Reader (.pdf document reader)
- MS office 2010,2013 and 2019
- Microsoft Essentials
- Kaspersky Anti-virus

The ICT department is responsible for configuring computers with standard software applications and any additional specific software. Employees may not install or delete software without ICT department approval or assistance. The ICT Office reserves the right to place controls on hospital computers to restrict or prevent unauthorized software installations, or modifications to the Windows operating system or to other installed software.

The ICT Department is responsible for installing or implementing virus protection software on all servers and computers. The virus protection software must automatically update on a daily basis to protect against the most current viruses, and be configured for real-time protection and to "clean and notify" if it detects a virus. Virus protection measures are also installed on the firewall In addition, the ICT Department applies security patches and updates to servers and computers as necessary to prevent security holes and possible virus intrusions.

8.0 Electronic File Storage:

Employees are to store only work-related files onto storage devices, in a manner that maximizes and does not jeopardize the use of available disk space, especially on network servers. Files to be shared with other network users should be saved to "group" folders established by the ICT department. Files saved to a network file server are backed up regularly and can be accessed from any network-connected computer, but only with the appropriate access rights. Employees may also save to their computer's hard drive, but the ICT department

does not back up the hard drives of employee computers. The files may be lost if the hard drive crashes

The IT department may periodically request employees to delete their unneeded files, and may delete without notice inappropriate files that are jeopardizing network or server functionality.

9.0 Storage and Retrieval of Electronic data:

Data will be stored in database of the server and network storage. Database will be backed up automatically every day in both the server and network storage.

10. 0 Maintenance of IT Hardware:

- Hardware inventory is maintained by the ICT Department.
- The hardware will be maintained by the ICT Department.
- In case of any problem to the hardware, it will first be verified by the Computer Technician and minor part will be replaced ,for major issues sent to services.
- On rectification of the problem, the system will be checked by the computer Technician Defective HDDs with data were low level formatted/destroyed before handed over to vendor/stores

11.0 Service and Support Requests:

Employees are encouraged to contact the ICT Department to request service and support for computer or network issues. All employees can request service and support for the following:

- Assistance with computer applications
- Network or email login problems
- Printing/printer problems
- Hardware troubleshooting

Certain requests for ICT Department support must come from The department head or above. Examples include the following:

- Any requests relating to file access permissions
- Replacing or moving equipment, office reconfigurations
- Creation of new accounts
- Installation of new software

The following procedures are followed when processing a service and support request:

A. The request is input into the helpdesk as a new work order, prioritized, and assigned to the appropriate ICT staff. The ICT Department may not be able to respond to the request immediately, depending upon the priority of the issue or the number of existing open requests that are pending.

B. The ICT department will troubleshoot the issue with the employee. Troubleshooting steps may include working with the employee over the phone, and requesting the employee to perform certain troubleshooting steps under the ICT department's instructions.

C. The ICT department may utilize remote desktop support whenever possible to troubleshoot the issue, in order to save time and expense. The ICT department can remotely access and take control of an employee's computer using remote access software. As a courtesy, the ICT department will notify the employee when remote access will be used.

D. All troubleshooting steps and results are logged into the work order. When the issue is resolved, the completion date and time is noted in the work order.

E. The ICT Department makes every effort to resolve all issues in a timely manner; however, due to such variables as equipment, licensing, and budget constraints, some requests cannot be immediately granted or solved.

12. 0 Computer Hardware Disposal:

It is the policy of the ICT not to keep computer equipment longer than its useful life, and to dispose of it properly through recycling procedures. Computer or other electronic equipment must not be thrown in the trash or dumpster. When computer equipment is identified as obsolete, ICT department will inform the Store to dispose the ICT equipment as per the e-waste disposal policy.

13.0 Formats for data collection:

The ICT has standardized the formats for data collection which is in line with data requirements of HIMS and other software systems

14.0 Resources for data collection, processing and analysis:

Hospital has employed staff in front office, MRD, laboratory, Pharmacy etc. to collect, process and analyze data and information.And also we are using online leave applications and online indent in I-web software and justHRMS for biometrics

Users/Department	Data/Information	System
Front office	Patient registration Admission Room/Bed allotment OP and IP billing	HIMS
Credit billing	List of companies & Schemes Tariff Credit bills	HIMS
Laboratory	Lab investigation order/results	LIS
MRD	Medical records index Medical records movement tracking Patient statistics	Manual MRD,Data is scanned and stored in Hard disks
Pharmacy	Item ordering/reordering Goods receive Sales Inventory monitoring Various analysis on inventory	HIMS
All Users/Employees	Online leave application, Online indent,	I-WEB (ERP)
Admission Department	Fee collection	I-WEB (ERP)
Students and Principal office	Online attendance and timetable	I-WEB (ERP)
All Users/Employees	biometric	JustHRMS

15.0 Information Security:

The ICT department maintains data and information, computers, computer systems and networks with various hardware and software components. ICT department is committed to help protect this computing environment, particularly to ensure the confidentiality, integrity, and availability of information. Towards that goal the ICT security policies have been established, to comply with national laws, regulations, and mandates regarding the management and prudent use of the Information and Computing Environment.

15.1. Users must adhere to the ICT Security Policy.

15.2. Users are responsible for managing their use of ICT department Information and Computing Environment and are accountable for their actions relating to security.

15.3. Users are responsible for reporting any suspected or confirmed violations of this policy to the appropriate authority.

15.4. User shall protect passwords, Personal Identification Numbers (PIN), and other computer system security procedures and devices from use by, or disclosure to, any other individual or organization.

15.5. Users shall not bypass or disable security controls.

15.6. Information access authority for each user must be reviewed on regular basis, changes in job status change such as: a transfer, promotion, demotion, or termination for service will require timely action and review.

16.0 User ID Management:

16.1. ICT department is responsible for the creation, control and removal of user accounts in the systems, applications, etc.

16.2. The User ID is created only after the request and approval process by the respected head of the departments.

16.3. The User ID must be based on employee code/reg, no/ID card which should be uniquely identifiable across the hospital.

16.4. All passwords for User IDs must be constructed in accordance with IT department Password Policy.

16.5. The access/permissions/roles given to the User IDs are as per the request of head of the departments.

16.6. If any employee is resigned or terminated then the corresponding User ID is disabled/removed from further accessing the systems, applications, etc.

17. 0 Password Protection Policy:

These are ICT policies implemented for Password Protection

17.1. The ICT department will create default password for the employees for using the systems and applications. Employees should then change this password immediately to avoid any unauthorized access.

17.2. Employees must set the password which should not contain their names, family member names, pet names, sequential numbers, etc. which can be easily guessed.

17.3. Employees should change passwords every 90 to 120 days or at any time they feel

17.4. password has been compromised.

17.5. Employees must not share their passwords with other persons.

18.0 Portable Computing Devices:

The access to USB storage devices is restricted to most of the computers in the Hospital,university and college. Shared folders which are accessible through LAN have been provided to copy/view/edit the documents.

19.0 E-Mail:

Each department in the Hospital has been provided with official email ID's for the purpose of communication and circulars for the office use only.

These are ICT policies implemented for using the E-mail

19.1. You must not use the email to create or distribute junk mail, spam mail or send anonymous email.
19.2. You must not use the email harass another person or send unwanted offensive material.
19.3. You are responsible for all email originating from your email account.
19.4. Make sure that unauthorized people do not have access to your computer accounts so that others cannot send email under your user account.
19.5. Sending or forwarding of email to the wrong person is very easily done and not very easily undone. Check carefully before sending.
19.6. Documents received by email are a frequent source of computer viruses. Such files should be scanned with antivirus software before use.
19.7. Your email may be ceased when you are resigned/terminated as per the guidelines of the management.

20.0 Internet Use:

The entire campus is connected to 1 Gbps leased line internet connectivity from JIO and BSNL through NMEICT project. This is the main backbone for the purpose of using the internet. Alternatively BSNL provides 1000Mbps redundancy internet line when the main JIO connection is down thereby eliminating the downtime of internet. All the systems in the Hospital are connected to this internet through LAN (Local Area Network).

These are ICT policies implemented for using the internet

20.1. As and when required websites which is found illegal/unnecessary will be blocked by the ICT department in the firewall.

20.2. Visiting illegal websites (pornographic, torrents, etc.) is strictly prohibited.
20.3. Downloading movies, music, games, software, etc. is strictly prohibited.
20.4. Laptop users must use Wi-Fi to access internet and should not use network cable as it conflicts the entire campus network.
20.5. Sharing of copyright material through processes such as peer to peer file sharing like torrent is strictly prohibited. It is illegal and may lead to criminal proceedings and it may even implicate the University.
20.6. If any unauthorized Wi-Fi router is found will be removed immediately and action will be taken against them.
20.7. In cases where a computer is "hacked into", it is recommended that the system be either shut down or be removed from the campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. The ICT Dept. reserves the right to disable the network connection to isolate the compromised computer.

21.0 ICT E-Waste Policy:

ICT E-Waste is regulated by Condemnation Committee which will when required identifies the items to be disposed. IT E-Waste covers the following ICT equipment's

Category	**Items**
Systems & accessories	Desktops(CPU, Monitor, Keyboard, Mouse), Servers, Laptops, Hard Disk, RAM, SMPS, DVD, Cables, etc.
Printers & accessories	Printers, Scanners, Cartridges, etc.
Network equipment's	Switches, Wi-Fi routers, LAN cables, etc.
Cameras & accessories	DVR, NVR, Cameras, etc.
Electrical items	UPS, Batteries, Power cables, etc.
Others	TV, Projectors, etc.

22.0 List of Licensed Software & Applications

Name of the Licensed Software	Total no of Licenses
Windows 7 Professional	150
Windows 8.1 Professional	119
Windows 10 Professional	175
Microsoft Office 2010 Standard	150
Microsoft Office 2013 Standard	119
Microsoft Office 2019 Professional	50
Windows Server 2008 R2 Enterprise	3
Windows Server 2012 R2 Standard	2
Windows Server 2019 Datacenter	3

Application	**Vendor**
PACS	Moksha Digital Software Limited
HIMS (Existing)	Biosoft Health Tech Pvt Ltd
HIMS (New One under implementation)	NTT Data services
ERP	I-web
HRMS	Fortuna
Easylib & dspace(library)	Easy lib