# 4.4.2 – Documents relating to updation of IT and WiFi facilities

## 2015 to 2020

| Date | Updation Particulars. |
|---|---|
| 05-05-2011 To 05-05-2021 | 1 GBPS Leased Line Internet (BSNL) installed in the Institute- LAN through NKN ( National Knowledge Network ) For 10 years |
| 11-03-2015 | Lifeline Suite Server (HMS) software1.0 version installed in 2014 and updated to 2.0 version. 2.0 Version still in use |
| 17-03-2015 | Dell PowerEdge T420 16 GB RAM and 1 TB Hard disk installed. |
| 06.08.2015 | Techno Linux Proxy Software Wi-Fi with Ruckus Ap's installed. |
| 05-03-2018 | JioWi-Fi installedin Campus having 1 GB per day per user |
| 29-06-2018 | SONICWALL NSA 4600 firewall installed for Internet security |
| 28-01-2019 | Medsynapse PACS Software for (Imaging)Radiology installed |
| 03-05-2019 | Dell PowerEdge updated to- R540 2U Rack Server 24 GB RAM and 2 TB Hard disk for HMS Server. |
| 17-09-2019 | Additional internet Lease Line of 20 Mbps from Airtel installed. |
| 07-09-2019 | Restructuring of Fiber and LAN network to University and All Constituent faculty buildings for Fiber Backbone updation of network |

In-charge, ICT,
KIMSDU, Karad

REGISTRAR
Krishna Institute of Medical Sciences
"Deemed To Be University", Karad

## Purchase Details for Computer, Laptop, Projector

| Year | Desktop Computers | Laptop | Printer | Projector |
|---|---|---|---|---|
| 2015-16 | 6 | 1 | 4 | 5 |
| 2016-17 | 14 | 2 | 23 | 5 |
| 2017-18 | 26 | 7 | 45 | 4 |
| 2018-19 | 33 | 9 | 26 | 5 |
| 2019-20 | 23 | 16 | 35 | 5 |
| 2020-21 July onward | 5 | 3 | 8 | |
| | 107 | 38 | 141 | 24 |

## Purchase Details for Computer, Laptop, Projector, Computer:

| Date | Particulars | Qty. |
|---|---|---|
| 23/05/2016 | Lenovo Make | 1 |
| 29/06/2016 | Lenovo Make | 1 |
| 30/06/2016 | Lenovo Make | 4 |
| 20/07/2016 | Lenovo Make | 1 |
| 15/12/2016 | Dell Make | 1 |
| 15/12/2016 | Dell Make | 1 |
| 30/01/2017 | Dell Make | 1 |
| 31/01/2017 | Dell Make | 2 |
| 07/04/2017 | Dell Make | 4 |
| 12/04/2017 | Dell Make | 1 |
| 12/04/2017 | Dell Make | 1 |
| 12/04/2017 | Dell Make | 1 |
| 12/04/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 1 |
| 13/09/2017 | Dell Make | 4 |
| 28/10/2017 | Dell Make | 3 |
| 23/11/2017 | Dell Vostro 3268 | 1 |
| 29/01/2018 | Dell Optiplex 3050MT | 6 |
| 27/02/2018 | Dell Optiplex 3050MT | 1 |

In-charge, ICT,
KIMSDU, Karad

REGISTRAR
Krishna Institute of Medical Sciences
"Deemed To Be University", Karad

| | | |
|---|---|---|
| 27/04/2018 | Lenovo 520 (AIO & Touch Screen)- | 1 |
| 07/07/2018 | Dell Optiplex 3050MT | 2 |
| 24/07/2018 | Dell Optiplex 3050MT | 2 |
| 25/08/2018 | Desktop- Assemble | 1 |
| 19/10/2018 | Desktop- Assemble | 1 |
| 23/01/2019 | Dell Optiplex 3060MT (With License) | 21 |
| 23/01/2019 | Dell Optiplex 3060MT (With License) | 1 |
| 23/01/2019 | Dell Optiplex 3060MT (With License) | 1 |
| 23/01/2019 | Dell Optiplex 3060MT (With License) | 4 |
| 14/03/2019 | Dell Optiplex 3060MT(With License) | 1 |
| 03/05/209 | Server Dell R540 | 1 |
| 05/08/2019 | Dell Optiplex 3060M | 2 |
| 27/07/2019 | HP AIO C3231L AMD | 5 |
| 30/10/2019 | Dell Optiplex 3060 | 1 |
| 28/10/2019 | Dell Optiplex 3060 | 1 |
| 02/10/2019 | Dell Optiplex 3060 | 2 |
| 16/12/2019 | Acer Vertion | 1 |
| 24/12/2019 | Dell Optiplex 3060 | 2 |
| 31/01/2020 | Acer Veriton | 1 |
| 31/01/2020 | Acer Veriton | 1 |
| 07/02/2020 | Acer Veriton | 1 |
| 11/02/2020 | Acer Veriton | 3 |
| 05/03/2020 | Dell Optiplex 5060- | 1 |
| 06/03/2020 | Acer Veriton | 2 |
| 07/09/2020 | Dell Vostro 3470 | 2 |
| 24/09/2020 | Dell Vostro 3471 | 1 |
| 16/10/2020 | Dell Vostro 3471 | 1 |
| 16/10/2020 | Dell Vostro 3471 | 1 |

**LAPTOP:**

| Date | Particulars | Qty. |
|---|---|---|
| 30/06/2016 | Dell Make | 1 |
| 08/10/2016 | Dell Make | 1 |
| 22/09/2017 | Dell Make | 1 |
| 23/11/2017 | Dell Inspiron 3567 | 1 |
| 04/12/2017 | Lenovo AIO-i5-7400 | 2 |
| 18/12/2017 | HP 15-br011TX | 1 |
| 20/12/2017 | Lenovo ThinkPad E470 | 1 |
| 28/12/2017 | HP 15-br011TX | 1 |
| 27/04/2018 | HP 348 Laptop | 1 |
| 22/10/2018 | Laptop- Dell Vostro 3568 (With License) | 3 |
| 29/12/2018 | Dell Latitude | 2 |
| 29/12/2018 | Dell Vostro | 1 |
| 15/05/2019 | Dell 3568 | 1 |
| 19/05/2019 | Dell Latitude 3490 | 1 |

In-charge, ICT,
KIMSDU, Karad

REGISTRAR
Krishna Institute of Medical Sciences
"Deemed To Be University", Karad

| | | |
|---|---|---|
| 29/04/2019 | Dell Inspiron 3576 | 1 |
| 08/08/2019 | Lenovo lp330 7din | 1 |
| 16/09/2019 | Dell Latitude 3490 | 7 |
| 05/10/2019 | Dell Latitude 3490 | 2 |
| 28/10/2019 | Dell Latitude 3490 | 1 |
| 16/12/2019 | Latitude 3400 | 2 |
| 07/02/2020 | Dell Latitude 3490 | 1 |
| 16/03/2020 | Dell Latitude 3400 | 1 |
| 26/06/2020 | Dell Latitude 3590 | 1 |
| 10/07/2020 | Dell 3593  Laptop- | |
| 12/10/2020 | Dell 15- Inspiron 3583 | 1 |
| 12/10/2020 | Asus Ultra K413FA | 1 |
| | | |

## Projector:

| Date | Particulars | Qty. |
|---|---|---|
| 24/08/2016 | Panasonic Make | 1 |
| 03/10/2016 | Panasonic Make | 1 |
| 03/10/2016 | Panasonic Make | 1 |
| 03/10/2016 | Panasonic Make | 1 |
| 14/04/2017 | Sony Make | 1 |
| 26/09/2017 | Panasonic Make | 1 |
| 26/09/2017 | Panasonic Make | 1 |
| 30/11/2017 | Sony- VPL DX220 (LCD) | 1 |
| 16/02/2018 | Epson EBX05 | 1 |
| 23/10/2018 | Sony- VPL DX221 (LCD) | 1 |
| 23/10/2018 | Sony- VPL DX221 (LCD) | 1 |
| 22/11/2018 | Sony- VPL DX221 (LCD) | 1 |
| 30/01/2019 | Epson-X-05 | 1 |
| 26/02/2019 | Epson EB-W-05 | 1 |
| 01/07/2019 | Optima Make | 3 |
| 15/02/2020 | Epson EB 980W | 1 |
| 16/09/2019 | Optima Make | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

# KRISHNA INSTITUTE OF MEDICAL SCIENCES
# "DEEMED TO BE UNIVERSITY", KARAD

ICT Policy Manual.

DATE: 20/12/2019

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

REGISTRAR
Krishna Institute of Medical Sciences
"Deemed To Be University", Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## Vision and Mission

### VISION

Implement technology education – not as an end in itself – but as a means to promoting creativity, empowerment and equality, producing efficient learners, problem solvers, potential researchers and potential entrepreneurs.

### Mission

To create a knowledge-base on good use of internet and technology and to bring in to education the safety issues pertaining to Internet an integral part of parenting as well as teaching and learning activities in education.

| | | |
|---|---|---|
| *Surve* | | *M* |
| **PREPARED BY** | **ISSUED** | **APPROVED BY:** |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## Index

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 1. Introduction:

The most important use for IT may be to help reduce medical errors. This technology-based strategy has proven effective in reducing the effects of human error in industries such as banking and aviation. Clinical IT systems may make a substantial impact on medical quality and safety by integrating relevant automated decision making and knowledge acquisition tools into the practices of medical providers, thereby reducing errors of omission that result from gaps in provider knowledge or the failure to synthesize and apply that knowledge in clinical practice. These systems, when integrated within larger HIS systems, may improve medical decision making and appropriate use of diagnostic tests and therapeutic agents. Provide support to staff on all company supported applications. Ensure LAN performance meets company and user requirements.

In the ambulatory healthcare environment, the use of HIS offers a variety of benefits. First, it can improve the efficiency and financial health of the practice. For years, many offices have used computerized scheduling and financial systems to streamline office processes by tracking practice productivity and automating reimbursement processes. Second, the use of ambulatory electronic health records also offers an opportunity to monitor and improve clinical quality by improving information access and reducing duplicative documentation. And technology-based tools may improve the efficiency and safety of prescribing practices in the outpatient setting just as they have done in the hospital setting. Finally, the widespread adoption of HIS will allow the achievement of system connectivity and information exchange among providers of the same organization, among organizations, and ultimately regionally and nationwide.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 2. Scope:

To design the scope of IT department we need to first classify the basic categories of its functionality. Hence the basic functionalities are as given below.

- Technical Support.
- Systems Management and Administration.
- Project Management.
- Strategic Planning.

Let us draft each one indetail.

### 2.1 Technical Support.

Under Technical support there would be various sub categories

#### 2.1.1 Hardware Technical Support.

Under this category IT department would take support call for the following.

a) Any computer peripheral issue.

b) Any printer issue.

c) Any Networkingperipheral issue and Internet Facility.

Note: Any repairing job is outsourced.

#### 2.1.2 Software Technical Support.

Under this category IT department would take support call for the following

1. Support to all software's as mentioned in Electronic Information policy.

IT department maintains the following listed databases.

a) HMS System (Lifeline HIS database)

b) Tally Database.

c) TDS Database.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

    d)   Time and Attendance

    e)   HRPayroll (Payroll System)

2.   Support to databases maintained by IT department, as mentioned in the databasemaintained Policy.

The lists of database maintained as of 01st April 2011 are.

    a)   HMS System (Lifeline HIS database)

    b)   Tally Database.

    c)   TDS Database.

    d)   HR Payroll Database

    e)   Time And Attendance

    f)   System Backup of Doman controller.

3.   Support for any Operating System related issues.

4.   Support for any antivirus issues.

## 2.2 Systems Management and Administration.

Under this category we have following sub categories.

2.2.1   System management and administration of all Servers.

2.2.2   System management and administration of Network.

2.2.3   System management and administration of Databases maintained.

2.2.4   System management and administration of Antivirus server.

2.2.5   System management and administration of HMS server.

2.2.6   System management and administration of TDS, Tally server.

2.2.7   System management and administration of HR Payroll Server

2.2.8   System management and administration of Firewall.

2.2.9   System Management and administration of Preventive Maintenance of Computers.

## 2.3 Project Management.

We divide the point in two sectors.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

2.3.1 Ton key projects.^

In Ton key projects IT uses its own resources to work out the project feasibility to the plan.

2.3.2 Team projects.

2.3.3 In team projects IT would participate in the some project plan.

### 2.4 Strategic Planning.

Under this section IT innovates and finds better solutions to current issues.

We become proactive and anticipate and technical issues and inform them to respectiveauthorities.We make yearly budgets and work according on the sanctioned one.

## 3. Objectives:

3.1 To provide round the clock facilities of hardware, software and networking.

3.2 Zero loss of data store on server.

3.3 Minimize downtime for HMS software.

3.4 Provide secured access for information managed by IT (e.g. HMS user security, File server security, Mail access, Internet and virus security).

3.5 To provide various reports as demanded by management.

3.6 Continuous service improvement.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| **KIMSDU** | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | **ICT POLICY** | | | |
| | Name of the Process/Areas | ICT | | | |

## 4. Functions

4.1 Attending the issues for hardware (e.g. Computers, Printers, etc.).

4.2 Attending the issues regarding the software.

4.3 Conducting the rounds for the inspection of network switches.

4.4 Inspecting the servers for the issues and fixing them if found any.

4.5 Inspecting the UPS for servers for the issues and taking the action as required.

4.6 Adding and updating of HMS masters as per the request given by authorized personals.

4.7 Managing and assigning the rights of users for HMS, file servers and internet as per the request by the authorized personals.

4.8 Inspecting the safety of all computers from viruses and malwares with the help of central administration of the anti-virus.

4.9 Complete the various IT documentation as per decided by the policies,
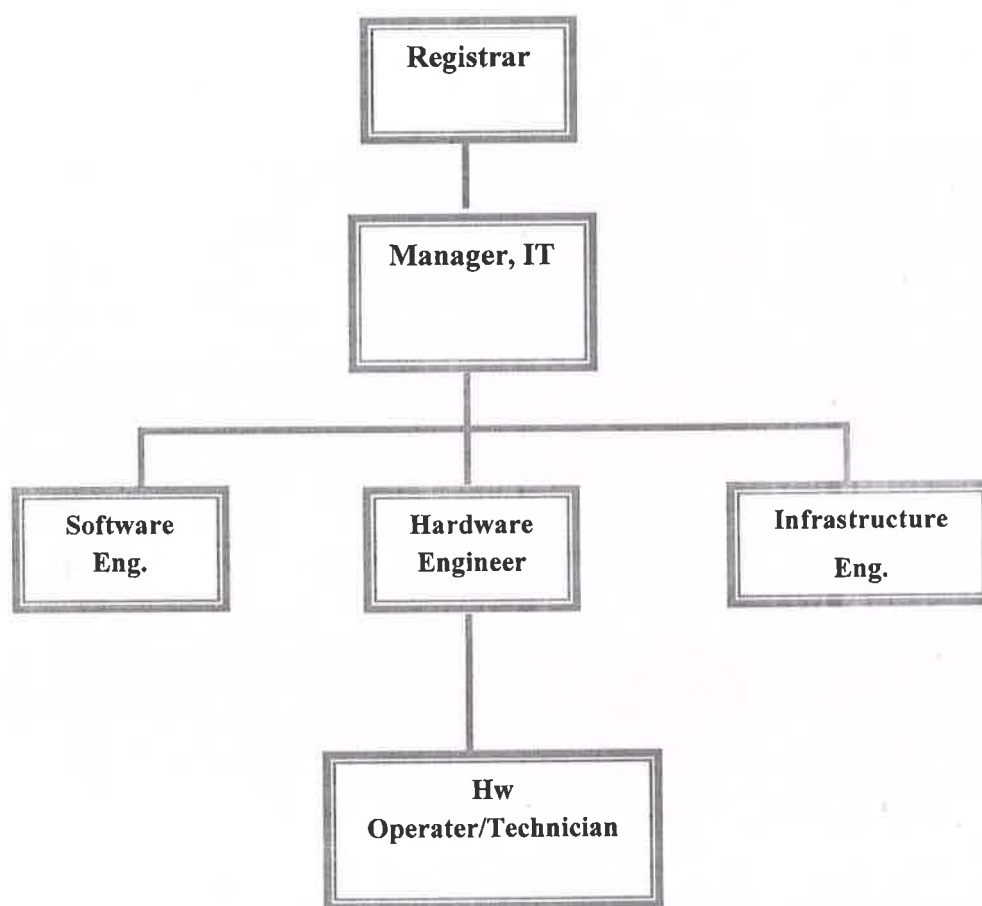
4.10 Backup data from all servers,

## 5. Services Provided

5.1 Provide computers to users as per the instructions of management.

5.2 Provide the user login credentials as per the authorized request.

5.3 Provide HMS access to users as per the authorized requests

5.4 Provide reports as requested by management.

5.5 Printing services as per the need of users.

5.6 Provide networking services to connect all the users to central server.

5.7 Provide central file storage with authorized access to users to store and maintain the official data,

PREPARED BY          ISSUED          APPROVED BY:

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 6. Organogram

```
                    ┌─────────────┐
                    │  Registrar  │
                    └─────────────┘
                           │
                    ┌─────────────┐
                    │ Manager, IT │
                    └─────────────┘
                           │
         ┌─────────────────┼─────────────────┐
   ┌───────────┐     ┌───────────┐     ┌────────────────┐
   │ Software  │     │ Hardware  │     │ Infrastructure │
   │   Eng.    │     │ Engineer  │     │      Eng.      │
   └───────────┘     └───────────┘     └────────────────┘
                           │
                  ┌──────────────────┐
                  │        Hw        │
                  │Operater/Technician│
                  └──────────────────┘
```

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 7. Job Descriptions

7.1 **Designation:** IT Assistant (Helpdesk Hardware)

**Reporting to:** IT Manager

**Responsible For:** Provide support to staff on all company supported applications. Ensure LAN performance meets company and user requirements

**Qualification:** Graduation from any steam with Hardware and networking Course.

**Skills Set Required:** Leadership, good communication.

**Responsibilities and Accountabilities:**

1) Answer staff questions in person and via phone on all company supported applications.
2) Troubleshoot computer problems.
3) Determine source of computer problems (hardware, software, user access, etc.).
4) Advise staff on appropriate action.
5) Serve as liaison between staff and the technology department to resolve issues.
6) Work one-on-one with staff on application projects.
7) Provide recommendations on company application purchases.
8) Investigate user problems, identify their source, determine possible solutions, test and implementsolutions.
9) Install, configure, and maintain workstations, file servers, Ethernet networks, network cabling, and otherrelated equipment, devices, and systems; adds or upgrades and configures modems, disk drives, data acquisition boards, CD ROM units, printers, and related equipment.
10) Maintain confidentiality with regard to the information being processed, stored or accessed by thenetwork.
11) Document resolutions for future reference. Administer network workstations, utilizing one or moreTCP/IP or non-TCP/IP networking protocols.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

12) Evaluate and/or recommend purchases of computers, network hardware, peripheral equipment, andsoftware.

13) Investigate user problems, identify their source, determine possible solutions, test and implementsolutions.

14) Install, configure, and maintain workstations, file servers, Ethernet networks, network cabling, and other related equipment, devices, and systems; adds or upgrades and configures modems, disk drives, data acquisition boards, CD ROM units, printers, and related equipment.

15) Perform and/or oversee software and application development, installation, and upgrades.

16) Plan and implement network security, including building firewalls, applying cryptography to network applications, managing host security, file permissions, backup and disaster recovery plans, file system integrity, and adding and deleting users.

17) Troubleshoot networks, systems, and applications to identify and correct malfunctions and other operational difficulties.

18) Develop and conduct various training and instruction for system users on operating systems, relational databases, and other applications; assist users in maximizing use of networks and computing systems.

19) Identify utilization patterns and their effect on operation/system availability and performance expectations.

20) Anticipate communication and networking problems and implement preventive measures.

21) Establish and perform maintenance programs following company and vendor standards.

22) Ensure timely user notification of maintenance requirements and effects on system availability.

23) Investigate, recommend and install enhancements and operating procedures that optimize network availability.

24) Maintain confidentiality with regard to the information being processed, stored or accessed by the network.

25) Document network problems and resolutions for future reference.

26) Other duties as assigned.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| Suove | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

**Additional Responsibilities**

1) Perform hardware and software installations.
2) Provide on-the-job training to new department staff members.

7.2 Assist personnel of other departments as a computer resource.**Designation:** Jr. Executive (Hardware Engineer)

**Reporting To:** Sr. Executive

**Responsible For:** To act as support for System administration, network engineer, as trainer, etc.

**Qualification:** Any Graduation Stream with m with computer hardware and networking course completion, with 1 Yr. Exp.

**Skills Set Required:** Should be all-rounder as to handle and carry out work as and when required, good communication.

**Responsibilities and Accountabilities:**

1) Answer staff questions in person and via phone on all company supported applications.
2) Troubleshoot computer problems.
3) Determine source of computer problems (hardware, software, user access, etc.).
4) Advise staff on appropriate action.
5) Serve as liaison between staff and the technology department to resolve issues.
6) Work one-on-one with staff on application projects.
7) Provide recommendations on company application purchases.
8) Investigate user problems, identify their source, determine possible solutions, test and implement solutions.
9) Install, configure, and maintain workstations, file servers, Ethernet networks, network cabling, and other related equipment, devices, and systems; adds or upgrades and configures modems, disk drives, data acquisition boards, CD ROM units, printers, and related equipment.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

10) Maintain confidentiality with regard to the information being processed, stored or accessed by the network.

11) Document resolutions for future reference. Administer network workstations,utilizing one or more TCP/IP or non-TCP/IP networking protocols.

12) Evaluate and/or recommend purchases of computers, network hardware, peripheral equipment, and software.

13) Investigate user problems, identify their source, determine possible solutions, test and implement solutions.

14) Install, configure, and maintain workstations, file servers, Ethernet networks, network cabling, and other related equipment, devices, and systems; adds or upgrades and configures modems, disk drives, data acquisition boards, CD ROM units, printers, and related equipment.

15) Perform and/or oversee software and application development, installation, and upgrades.

16) Plan and implement network security, including building firewalls, applying cryptography to network applications, managing host security, file permissions, backup and disaster recovery plans, file system integrity, and adding and deleting users.

17) Troubleshoot networks, systems, and applications to identify and correct malfunctions and other operational difficulties.

18) Develop and conduct various training and instruction for system users on operating systems, relational databases, and other applications; assist users in maximizing use of networks and computing systems.

19) Identify utilization patterns and their effect on operation/system availability and performance expectations.

20) Anticipate communication and networking problems and implement preventive measures.

21) Establish and perform maintenance programs following company and vendor standards.

22) Ensure timely user notification of maintenance requirements and effects on system availability.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

23) Investigate, recommend and install enhancements and operating procedures that optimize network availability.

24) Maintain confidentiality with regard to the information being processed, stored or accessed by the network.

25) Document network problems and resolutions for future reference.

26) Other duties as assigned.

**Additional Responsibilities**

1) Perform hardware and software installations.

2) Provide on-the-job training to new department staff members.

3) Assist personnel of other departments as a computer resource.

7.3 **Designation:** Jr. Executive (Software) '

**Reporting To:** IT Manager

**Responsible For:** Develop, install, maintain, and modify application programs, business application programs, or integrated programs. Identify and analyze user requirements and recommend appropriate applications or modifications. Perform a variety of programming assignments requiring knowledge of established programming procedures and data processing requirements. Maintain and modify programs.

**Qualification:** BCS with at least 1 year experience.

**Skills Set Required:** Leadership, good communication.

**Responsibilities and Accountabilities:**

1) Investigate user problems and needs, identify their source, and determine possible solutions.

   a) Analyze user project proposals to include identifying potential problem areas and recommend optimum approaches for project path.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT, KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

b) Participate in the development, implementation, installation, and testing of applications software.

c) Contribute through code/algorithm development and other means, for the development of tools and interfaces between application programs and for the development of debugging programs.

d) Provide system level support for computer software and classroom computer equipment used to conduct workshops.

e) Participate in the development of training materials and assist in conducting training and workshops in parallel processing and use of large computer systems.

f) Investigate, recommend and install new applications.

g) Maintain confidentiality with regard to the information being processed, stored or accessed by the network.

h) Document programming problems and resolutions for future reference.

i) Assist personnel of other departments as a computer resource.

j) Code, test and troubleshoot programs utilizing the appropriate hardware, database, and programming technology,

k) Refine data and format final product.

l) Maintain and modify programs; make approved changes by amending flow charts, develop detailed programming logic, and coding changes.

m) Test and develop programming modifications,

n) Write new program code using prescribed specifications.

2) Evaluate simple interrelationships between programs such as whether a contemplated change in one part of a program would cause unwanted results in a related part.

3) Analyze performance of programs and take action to correct deficiencies based on consultation with users and approval of supervisor.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

4) Confer with users to gain understanding of needed changes or modifications of existing programs. Resolve questions of program intent, data input, output requirements, and inclusion of internal checks and controls.

5) Analyze NT client/server and micro-computer based software solutions compatibility with company requirements.

6) Maintain confidentiality with regard to the information being processed, stored or accessed.

7) Document programming problems and resolutions for future reference.

8) Assist personnel of other departments as a computer resource.

9) Other duties as assigned.

**Additional Responsibilities**

1) Provide technical support and representation at trade shows, conferences, and similar events.

2) Provide on-the-job training to new department staff members.

3) Data entry as needed.

7.4 **Designation:** IT Assistant Manager

**Reporting To:** IT Manager

**Responsible For:** Responsible for the installation, layout, and maintenance of all network components. Plan, design, analyze, and provide technical support for data communications network or group of networks. Conduct research and evaluation of network technology and recommend purchases of network equipment. Responsible for the installation, layout and maintenance of all Database components. Plan, design, analyze, and provide technical support for database. Conduct research and evaluation of Database technology and recommend purchases of software's. Direct and manage computing and information technology strategic plans, policies, programs and schedules for business and finance data processing, computer services, network communications, and management information services to accomplish corporate goals and objectives.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | **KIMSDU** | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | **ICT POLICY** | | | |
| | Name of the Process/Areas | **ICT** | | | |

**Qualification:** Graduate or Post Graduate with 1 years' experience.

**Skills Set Required:** Should be all-rounder as to handle and carry out work as and when required, good communication.

**Responsibilities and Accountabilities:**

1) Direct and manage computing and information technology strategic plans, policies, programs, and schedules for business and finance data processing, computer services, network communications, and management information services to accomplish corporate goals and objectives.

2) Direct the information and data integrity of the company and its business units.

3) Develop strategic plans and implement the objectives of the information technology needs of the company to ensure the computer capabilities are responsive to the needs of the company's growth and objectives.

4) Develop and establish operating policies and approaches for computing and information technology.

5) Evaluate overall operations of computing and information technology functions and recommend enhancements.

6) Advise senior management on strategic systems conversions and integrations in support of business goals and objectives.

7) Prepare enterprise objectives and budgets to facilitate the orderly and efficient capture, storage, processing, and dissemination of information.

8) Interact with company managers on internal and external operations that are impacted by the capture, storage, processing and dissemination of information.

9) Review and approve major contracts for computing and information technology services and equipment.

10) Ensure the security of the information systems, communication lines, and equipment.

11) Oversee the development, design, and implementation of new applications and changes to

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

existing computer systems and software packages.

12) Responsible for the development, review, and certification of all back-up and disaster recovery procedures and plans.

13) Identify emerging information technologies to be assimilated, integrated, and introduced within the company.

14) Assess new computing technologies to determine potential value for the company.

15) Oversee ongoing improvements and the feasibility of system enhancements.

16) Establish company infrastructure to support and guide individual divisions/departments/sites in computing and information technology efforts.

17) Establish and implement short- and long-range departmental goals, objectives, policies, and operating procedures.

18) Serve on planning and policy-making committees.

**Additional Responsibilities**

1) Recruit, train, supervise, and evaluate department staff.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | **KIMSDU** | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | **ICT POLICY** | | | |
| | Name of the Process/Areas | **ICT** | | | |

7.5 **Designation:** IT Manager

**Reporting To:** Vice President Finance and IT

**Responsible For** Direct and manage computing and information technology strategic plans, policies, programs and schedules for business and finance data processing, computer services, network communications, and management information services to accomplish corporate goals and objectives.

**Qualification:** M.C.M

**Skills Set Required:** Proper knowledge of handling computers.

**Responsibilities and Accountabilities:**

1) Direct and manage computing and information technology strategic plans, policies, programs, and schedules for business and finance data processing, computer services, network communications, and management information services to accomplish corporate goals and objectives.

2) Direct the information and data integrity of the company and its business units.

3) Develop strategic plans and implement the objectives of the information technology needs of the company to ensure the computer capabilities are responsive to the needs of the company's growth and objectives.

4) Develop and establish operating policies and approaches for computing and information technology.

5) Evaluate overall operations of computing and information technology functions and recommend enhancements.

6) Advise senior management on strategic systems conversions and integrations in support of business goals and objectives.

7) Prepare enterprise objectives and budgets to facilitate the orderly and efficient capture, storage, processing, and dissemination of information.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

8) Interact with company managers on internal and external operations that are impacted by the capture, storage, processing and dissemination of information.

9) Review and approve major contracts for computing and information technology services and equipment.

10) Ensure the security of the information systems, communication lines, and equipment.

11) Oversee the development, design, and implementation of new applications and changes to existing computer systems and software packages.

12) Responsible for the development, review, and certification of all back-up and disaster recovery procedures and plans.

13) Identify emerging information technologies to be assimilated, integrated, and introduced within the company.

14) Assess new computing technologies to determine potential value for the company.

15) Oversee ongoing improvements and the feasibility of system enhancements.

16) Establish company infrastructure to support and guide individual divisions/departments/sites in computing and information technology efforts.

17) Establish and implement short- and long-range departmental goals, objectives, policies, and operating procedures.

18) Serve on planning and policy-making committees.

**Additional Responsibilities**

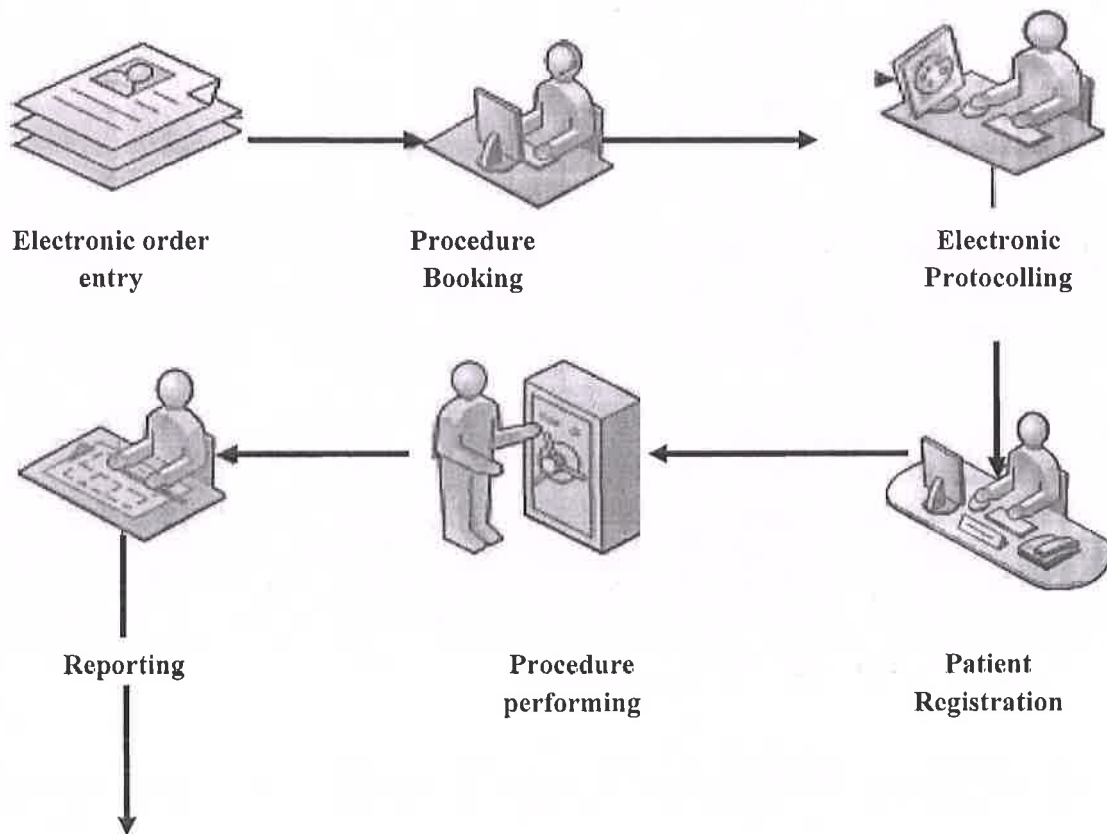1) Recruit, train, supervise, and evaluate department staff.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 8. Work Flow.



Electronic order entry → Procedure Booking → Electronic Protocolling

Reporting ← Procedure performing ← Patient Registration

| | ISSUED | APPROVED BY: |
|---|---|---|
| **Work Done** | | |

In-charge, ICT,
KIMSDU, Karad

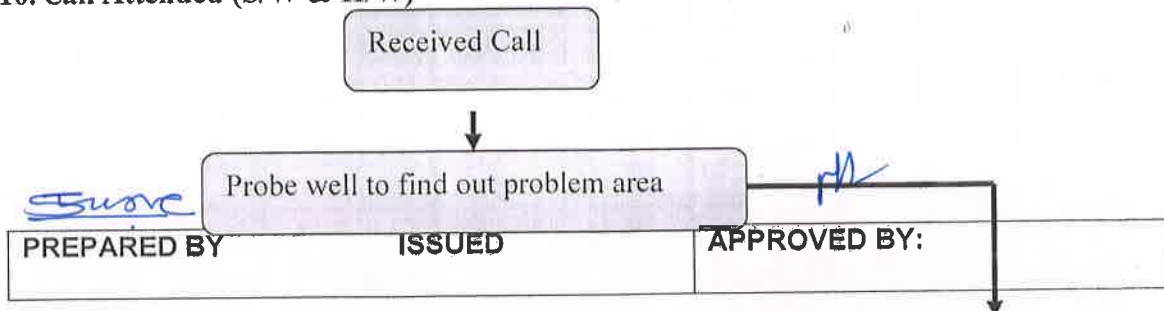| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 9. Process Maps

Process: Database Backup

1) IT Department take backup on every day, IT have 2 HDD one hard disk is at Cash Vault of cash store and other remain with IT we use to take backup on alternate HDD and submit that HDD to billing and bring other HDD back.

Take HDD-1 OR HDD-2

↓

Take Backup of Tally, TDS, KH-backup, HMS Server

↓

Create txt file as per date (e.g.ddmmyyyy.txt) & use data.txt file

↓

Record file to IT department Staff

## 10. Call Attended (S/W & H/W)

Received Call

↓

Probe well to find out problem area

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

```
                        │
                        ▼
              ◇ If user is unable ◇ ──────►  We send IT Eng. For probing
              ◇ to narrate?       ◇                        │
                        │ ◄───────────────────────────────┘
                        ▼
        Analyze the solution and start working ◄──────┐
                        │                              │
                        ▼                              │
            Enter the issue in call sheet              │
                        │                              │
                        ▼
  Yes  ◄──────  ◇ If issue is ◇  ──────► No
                ◇ resolved?   ◇              │
                        │                    ▼
                        │         Mark that call as Open/In progress
                        │                    │
                        ▼                    ▼
          Mark as Hold with reason ──►  ◇ If        ◇
                        │               ◇ resolved? ◇
                        │                    │ Yes
                        ▼                    ▼
  └──► Mark that call as Closed ◄──────────┘
                        │
                        ▼
          Informs to seniors or IT Manager ◄──────────┘
```

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 11. Standard Operating Procedures

    11.1  SOP for Server Backup

    11.2  SOP for Complaint Management

    11.3  SOP for Network Point Requisition

    11.4  SOP for Preventive Maintenance

    11.5  SOP for Data Theft and Security

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

1. **Aim**: To take the daily **backup of Server data.**

2. **Definition: Nil**

3. **Applicable areas:** All servers

4. **Authority & Responsibility:**

   4.1 IT. Manager

   4.2 All IT. Staff

5. **Procedure:**

   IT engineers are supposed to take daily backup of the server data for the disaster recovery. The data to be backed up can be found in the disaster recovery policy. The procedure to take the backup is as follows. The data is backed up in two different ways.

   - Automated backup using software.
   - Manual backup on the portable HDD

   **Automated Backup using software**

   a) We have Microsoft Data Protection Management software. This software is installed on the server connected to tape library.

   b) This is a Disk - Disk - Tape backup method used for the backup.

   c) IT administrator needs to deploy to DPM agent on the server or the desktops for which the backup needs to be taken. The list for the same is decided by the IT Manager.

   d) Administrator decides the strategy for the backup in terms of space needed for the backup, retention time and type of the backup (full, incremental, etc.).

   e) After the decision the protection groups are prepared on the server. These groups involve the space for the backup, retention time, destination for backup (disk, tape).

   f) Once done the backup interval is decided and the DPM starts to take backup automatically.

   **Manual Backup on the portable HDD**

   a) This step is to make sure that we do have backup in case of the failure of the automated backup.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

b) Manual backup is done only for the predefined databases, critically required for the business.

c) Administrator manually takes the backup of the decided database from the backup server to the local server.

d) The files are then copied from the local computer to the portable hard disk.

e) We do maintain two different hard disks for the backup. The disks are used alternately each day, just to make sure that the data is not lost completely in worst case of the disk failure.

f) After backup the hard disks are kept in the cashiers vault with proper written handover of the drive. This is to make sure that the disk is not damaged and handled by other personals.

6. **Monitoring & analysis/ indicators: Nil**

1. **Aim:** The purpose of the policy is to lay a procedure for **complaint management.**

2. **Definition:** Nil

3. **Applicable areas:** To lay a procedure for complaint management for Hardware and Software

4. **Authority & Responsibility:**

   4.1 IT. Manager
   4.2 All IT. Staff
   4.3 Users using the data

5. **Procedure:**

   After receiving a call from respective departments, we probe well to find out the problem area. If the user is unable to narrate the problem we send personnel from IT for the probing. Once we analyze the solution for the problem we start working on it and get the issue resolved. At the end of the day the respective engineers make an entry in the Daily Call sheet for hardware and Bug list for software. These sheets have 4 statuses.

   a) Closed

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | **KIMSDU** | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | **ICT POLICY** | | | |
| | Name of the Process/Areas | | ICT | | |

b) Open,
c) In process.
d) On hold.

If for any reason the call goes on hold we mention the On-hold reason.
At the end on the month we make the similar entries in the Quality indicators worksheet which automatically calculates the indicator lapse or maintained status.

**Escalation levels:**
If the issue remains unresolved within the quality indicator time slot it should be raised to the next senior functional head. If the issue remains undiagnosed after then it should be raised to the IT manager. The senior functional head and the IT manager are responsible for its closure. If the closure require any support from Management should be immediately conveyed.

**Vendor Escalation:**
If the issue is about any repairing, AMC or anything we IT does not maintain in house should be immediately raised to respective vendor. The senior functional head remains responsible for the follow up. If the vendor is not supportive enough it should be immediately escalated to the IT manager. The senior functional head and the IT manager are responsible for its closure. If the closure require any support from Management should be immediately conveyed.

6. **Monitoring & analysis/ indicators :** Nil

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

1. **Aim:** The purpose of the policy is Laying of Network point at location.

2. **Definition:** Nil

3. **Applicable areas:** Nil

4. **Authority & Responsibility:**

    4.1 IT. Manager

    4.2 All IT. Staff

5. **Procedure :**

    5.1 IT maintains the template for Network Point Requisition.

    5.2 Requested user need to collect the templates for network.

    5.3 Requested user should be filled up the template and by taking the HOD approval and approval authority and submit the requisition to IT.

    5.4 After submitting the requisition IT will take the appropriate action against it.

    5.5 After submitting the requisition to IT, We follow the procedure.

    5.5.1 We co-ordinate with requested user for the exact location, to lay down the CAT6 cable.

    5.5.2 We check the feasibility of Laying of cable to the location with the help of engineering department person.

    5.5.3 Due to lying of cable is in house activity hence we send email request to engineering department.

    5.5.4 Once the laying of LAN cable is completion from engineering department we checked the both end point.

    5.5.5 After lying of cable we do the crimping, and punching to the cable at both end (switch side end and requested user end.)

    5.5.6 We test the network by network tester. And informed to the requested user.

    5.5.7 We update the documentation for the same. Also mentioning the date of completion on the requisition template.

6. **Monitoring & analysis/ indicators :** Nil

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

1. **Aim**: To do the Preventive Maintenance of Computers with Schedule.
2. **Definition:** Nil
3. **Applicable areas:** Nil
4. **Authority & Responsibility:** All IT staff.
5. **Procedure:**

   IT department does the preventive maintenance for the computers belonging to IT network. The policy for the same is as follows.

   5.1 IT help desk engineer prepares the schedule for the preventive maintenance of the computers belonging to IT network. The schedule is prepared in such a way that each computer or laptop is taken care of quarterly.

   5.2 The schedule is mailed to the respective users a month prior to the schedule.

   5.3 IT engineer reminds the user one day before the schedule so the user can prepare himself herself for the decided downtime.

   5.4 The downtime for the maintenance should not exceed more that hour. This does not include the time for the transportation of the computer.

   5.5 The IT help desk engineer visits the respective location and after seeking final permission from the user, disassembles the computer. The ward boy on duty carries the computer to IT department for further actions.

   5.6 The IT team on receiving the computer makes entry of the receiving computer in the sheet.

   5.7 The team works out various activates for maintenance on the PC. The details of the same are as follows.

       5.7.1 The computer is first cleaned with the dry cloth and then dust is blown out of the PC with the help of blower.

       5.7.2 The unwanted, temporary files are deleted with the help of windows clean up software

6. **Monitoring & analysis/ indicators:** Nil

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

1. **Aim: To take care of Data Theft and Security in University and all offices.**
2. **Definition: Nil**
3. **Authority & Responsibility:** All IT staff.
4. **Procedure:**

With each new piece of technology comes new potential for data security breach. The dangers inherent in using a smartphone or tablet are quite different from those associated with a laptop. Even the convenience of wireless internet has more opportunities for attack than traditional hard-wired systems. While most security measures focus on external threats from hackers and malicious downloads, internal threats account for twice as much monetary loss as external threats. An internal threat could be the deletion or dissemination of computer files related to a client's case. One employee could also share their password with another, granting someone access beyond the scope of their position. To prevent the intentional or unintentional problems created by employee use of software and equipment, developing a thorough data securities policy is more important than ever. This policy should provide employees with information regarding the acceptable use of mobile technology as well as password security and wireless access policies to protect confidential data.

### Office Computers and Server

There are some truths that should be self-evident but need to be spelled out in a written policy, because inevitably an employee will otherwise do the unthinkable. Some may ignore the Not Safe for Work (NSFW) tag and view pornography if they are 'off the clock' during a break or lunch hour, while others may decide to run a personal business or game server using the firm's servers. Both of these activities expose the office to security risks. Some less obvious but equally risky behavior is the desire to download software from the internet onto company computers and/or servers. An employee could simply be looking for a tool to make them more efficient in their job. However, looking in the wrong place and downloading the wrong file could install malicious software onto your system. Perhaps the scariest danger is the easiest one to complete: deleting files. Deleting a file can sometimes be as simple as hitting the wrong key combination, resulting in a mad dash to the IT specialist with the order to "retrieve!" said file from the trash bin. On those occasions that the deletion wasn't noticed right away, IT can spend a significant amount of time with the backup locating the document to hopefully restore

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

it. To prevent these and other related computer and server nightmares, create an acceptable use policy as part of your data security package. Restrict who has the right to download executable files (programs) and who can modify items in certain folders. Firewalls, virus scan and anti-spam software should be installed, updated and the system regularly scanned.

**User Leval Access Control :**

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data. At a high level, access control is a selective restriction of access to data. ... Without authentication and authorization, there is no data security. Many Institutes have documents or data that should not be accessible to everyone in the company. An access control system allows a business to limit the access to certain areas that hold hardware or software that this information is saved on.

**Secure Backups**: Data is losing a day's worth of work acceptable, let alone a week? Backing up the office servers every night and storing that data off-site can save a law firm. Disasters don't wait for you to be prepared before they strike. Servers, like other computers, can die without warning. Having a full backup available allows you to upload your data onto a new server (after a new server is acquired and built) and continue working without having to reinvent lost work. It's even better when you have a redundant system, and you can simply switch to your backup server and continue on as if nothing has happened. There are different varieties of backup systems available. Nash backups remove the need for equipment but require extra vigilance regarding security when selecting a company. USB backups give the convenience of a portable backup, but proper security must be maintained since they are small and easily lost.

**Data Security Tool Kit:** When planning your backup system, budget may be a factor in deciding which route you take. However, you have to pick a system you will use. Saving money isn't a value if it's tedious work that never actually gets done and you don't have a current backup when you need it. Your backup policy should include determination for how long backup copies will be kept. Additional USB drives can be purchased to maintain offsite backups. If using the tape system, have a series of tapes that you rotate. Because tapes

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

deteriorate, replace them on a regular basis to prevent problems. Keeping end of month or end of year backup's offsite may be helpful as well.

**Password Security:** Recent headlines highlight the continued problem of creating simple passwords that are quickly hacked because they are easier to remember. If a site requires a complicated password, some people will write it down and attach the post-it note to their computer so they have easy access to it when they need it. Others save a document in the system with their list of passwords to various sites. Any of these methods are hazards that can provide unauthorized access to your system.

**Internet Use :** Preventing employees from ever surfing to a network-related website can be cost prohibitive for small and medium sized firms. However, having a clear internet use policy can help limit the types of sites they visit. Streaming music and video use a lot of bandwidth, and downloaded files from file sharing sites can contain malware or expose the firm to liability if material was copyrighted. Some employees may be tempted to spend too much time on activities such as online shopping, social media or travel planning.

**E-mail Misuse of company email is one of the most common problems :**

Faced, and covers a large variety of actions. Sending a free "Happy Birthday!" card from a free website can introduce massive spamming into your system and bog down your server. Employees may use company e-mail for running a personal business with less thought than storing hard files on the computers or servers. A Good Samaritan employee may send out emails to everyone in the firm regarding a fundraising event for a local charity, and follow up with four or five reminders. Personal use of the firm email system should be addressed to reduce the amount of server space such items consume. E-mail policies should also include limits on the size of attachments as appropriate. Consider this: an e-mail with a 20MB attachment is received and then forwarded to ten other employees.

**Remote Access :** Employees may need to access the firm's system when they are out of the office occasionally. Prohibiting employees from using public computers or using wireless access in public places removes the exposure of client data from hackers because security settings in these circumstances are often lower than those created for the office.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

**Smartphones, Tablets and Remote Storage Devices** :The trickiest part of data security is protecting the mobile data that leaves the building. Smartphones and tablets all contain internet connections but often do not have all of their security measures activated as a firm laptop would provide. A USB drive often contains pure, unencrypted files available for anyone who plugs the drive into their computer; worse yet, it is small enough to easily lose.

**When an Employee Leaves** :Often the biggest threat to your data is within your own company. A disgruntled or exiting employee can easily delete files from your system or take files out of the office without notice. Locking down data from employees can be the hardest part of data security. When an employee leaves, immediately lock their computer, e-mail, remote access and any other access privilege to prevent them from accessing information. Create protocols within the firm for who may need to access an employee's files. If the employee has any equipment, such as a laptop or USB drive, at home, verify that it is returned before they exit the premises on their final day.

**Visitors and Contractors From time to time**: Office visitors may need to use office computers or email. Any temporary account established should have a notice regarding expectation of privacy. Passcodes for these accounts should also expire immediately after use. This ensures someone temporarily allowed into your system won't be able to access your confidential data later, when you're not looking.

**Security Audit** :To ensure all facets of your system are properly secure, consider a third party secuity audit. A trained professional will see any holes in your protection that could leak confidential information. The auditor will be able to provide you with suggestions to improve your security to prevent data security breaches in the future. This may include the purchase of additional security software, or simply changing internet usage habits. The end result will be a safer practice.

**Monitoring & analysis/ indicators:**

Safety devices like smoke detectors, Fire extensions, fire alarms and CCTV surveillance

Implementation of Email Server on Cloud.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 12. Work Instructions

12.1 Work Instructions for Software call management

    12.1.1 Receive the call politely.

    12.1.2 Take down the username, department, extension number

    12.1.3 Probe well to find out the problem and log the call in call sheet

    12.1.4 Analyzed the problem and start solving it

    12.1.5 If it is bug log in bug list and forward it to Akhil Eng.

12.2 Work instructions for Hardware call management

    12.2.1 Receive the call politely

    12.2.2 Take down the username, department, extension number

    12.2.3 Probe well to find out the problem and log the call in call sheet

    12.2.4 Analyzed the problem and start solving it onsite

    12.2.5 If can't solve bring PC or printer to IT and solve it

    12.2.6 Mark the call in call sheet as onsite or offsite call

    12.2.7

12.3 Work instruction for backup

    12.3.1 The data is backed up in two different ways.

        a) Automated backup using software(DPM).

        b) Manual backup on the portable HDD.

    12.3.2 The files are then copied from the local computer to the portable hard disk.

    12.3.3 We do maintain two different hard disks for the backup. The disks are usedalternately each day, just to make sure that the data is not lost completely in worstcase of the disk failure.

    12.3.4 After backup the hard disk is submitted to authorize person.

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

12.4 Work instruction for adding master data in HMS

    12.4.1 We give the template to the user

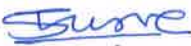    12.4.2 User has to fill that template and get authorized person signature on that

    12.4.3 Once we receive the template from user we take the action

12.5 Work instruction for file server

    12.5.1 We give the folder sharing template to the user

    12.5.2 User has to fill that template and get authorized person signature on that

    12.5.3 Once we receive the template from user we take the action

12.6 Work instruction for internet

    12.6.1 We give the internet facility template to the user

    12.6.2 User has to fill that template and get authorized person signature on that

    12.6.3 Once we receive the template from user we take the action

12.7 Work instruction for mail

    12.7.1 We give the new mail facility template to the user

    12.7.2 User has to fill that template and get authorized person signature on that

    12.7.3 Once we receive the template from user we take the action

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|
| | | |

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 13. List of Forms & Performa's

13.1   Bed Addition or Edition

13.2   Change Request

13.3   Company Addition or Edition

13.4   Computer Requisition (Replacement)

13.5   Computer Requisition (New)

13.6   Department Addition or Edition

13.7   Doctor Addition

13.8   Doctor Appointment Scheduling

13.9   Doctor Signature

13.10  Document Sharing

13.11  Firewall Services

13.12  HMS User Login

13.13  Incident Report

13.14  Internet Facility

13.15  Mail Facility

13.16  Network Point Requisition

13.17  Package Addition

13.18  Printer or Scanner Requisition

13.19  Printer or Scanner Requisition (Replacement)

13.20  Service Addition or Edition

13.21  SMS Requisition

13.22  Surgery Addition

13.23  Video Conferencing Request

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 14. Types of Records Maintained

14.1  Help-desk call details (S/W & H/W)

14.2  HMS bug list

14.3  New HMS user login details

14.4  New Doctor Addition

14.5  New Nurse Addition

14.6  MRD

14.7  New Service Addition

14.8  Change Request

14.9  Company Addition

14.10 Bed Addition

14.11 Package Addition

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | **ICT POLICY** | | | |
| | Name of the Process/Areas | ICT | | | |

## 15. Performance Indicators

15.1  HMS Uptime

15.2  HMS Bug Resolution

15.3  On-site Hardware Issue Resolution

15.4  Off-site Hardware Issue Resolution

15.5  Technical Feasibility

15.6  Installation of New Computers

15.7  Training Details

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

| | KIMSDU | Doc Number | KIMSDU/ICT/FOR/K | Issue date | 20/12/2019 |
|---|---|---|---|---|---|
| | | Rev No | 0.0 | Issue No | 01 |
| | Name of the Document | ICT POLICY | | | |
| | Name of the Process/Areas | ICT | | | |

## 16. Training & Development of Staff

16.1  Training for all HMS modules.

16.2  Training for new technologies

16.3  Installation of new software and OS

16.4  Management level trainings

16.5  Call handling training

16.6  Material management

16.7  Networking Training

| PREPARED BY | ISSUED | APPROVED BY: |
|---|---|---|

In-charge, ICT,
KIMSDU, Karad

REGISTRAR
Krishna Institute of Medical Sciences
"Deemed To Be University", Karad