Sri Aurobindo Institute of Medical Sciences
Sri Aurobindo College of Dentistry, Indore
Recognized by Dental Council of India•   NAAC Accredited

ELECTRONIC DATA PROCESSING
DEPARTMENT MANUAL

Service Name :	**DEPARTMENTAL MANUAL** **Electronic Data Processing Department** **SAIMS / NABH / DM / EDP / 01**
Date Created :	
Approved By :	Name : Dr. Mahak Bhandari Designation: Managing Director Signature :
Reviewed By :	Name : Sameer Poorkar Designation: Manager (IT) Signature :
Issued By :	Name : Sameer Poorkar Designation: Manager (IT) Signature :
Responsibility of Updating :	Name : EDP Department Designation: Signature :

Principal,
Sri Aurobindo College of Dentistry
INDORE (M. P.)

CONTENTS

AMENDMENT SHEET

S.no	Section no & page no	Details of the amendment	Reasons	Signature of the preparatory authority	Signature of the approval authority

CONTROL OF THE MANUAL

The holder of the copy of this manual is responsible for maintaining it in good and safe condition and in a readily identifiable and retrievable.

The holder of the copy of this Manual shall maintain it in current status by inserting latest amendments as and when the amended versions are received.

Quality Accreditation Coordinator is responsible for issuing the amended copies to the copyholders, the copyholder should `acknowledge the same and he /she should return the obsolete copies to the HOD.

The amendment sheet, to be updated (as and when amendments received) and referred for details of amendments issued.

The manual is reviewed once a year and is updated as relevant to the hospital policies and procedures. Review and amendment can happen also as corrective actions to the non conformities raised during the self assessment or assessment audits by NABH. The authority over control of this manual is as follows:

Preparation	Approval	Issue
HOD, EDP Department	Managing Director, SAIMS, Indore	Quality Accreditation Coordinator

The procedure manual with original signatures of the above on the title page is considered as 'Master Copy', and the photocopies of the master copy for the distribution are considered as 'Controlled Copy'.

Distribution List of the Manual:

Sr. No.	Designation
1	Quality Accreditation Coordinator
2	HOD, EDP Department

1.0 INTRODUCTION:

1.1   SAIMS IT department has its major organizational units as infrastructure management and support and training division. These units serve and act with classified role of the department.

1.2   The main functional areas of the department are as follows:

     1.2.1   Develop and maintain the software application, database and Windows server.

     1.2.2   Provide data to management for decision making.

     1.2.3   Maintain internal network & lease port Connection.

     1.2.4   Development of software for user departments as per requirement.

     1.2.5   Maintain the hardware, software (in-house & third party) and network installation.

     1.2.6   Audio visual equipment support for seminars, conferences & meetings.

     1.2.7   Support for operation systems and applications.

     1.2.8   IT user support (Service desk).

     1.2.9   Computer Security for SAIMS.

     1.2.10   IT hardware/software procurements.

     1.2.11   AMC

2.0 PURPOSE:

2.1   The IT department mission is to provide the Information Technology required for the fulfillment of the SAIMS in an efficient and effective manner through building **Excellent Competencies** in the technical analysis, design, procurement, implementation, operation and support of computing infrastructure and services.

3.0 SCOPE:

3.1   The information technology department has in-house HIS (Hospital Information Systems), Inventory & Pharmacy Management System. Also patient portal (**Android App - YUVVAN**) is available to view diagnostics result.

3.2   Third party applications are

    3.1.1   Tally   -   Financial accounting

    3.1.2   Saral Paypack   -   Payroll

    3.1.3   Savior   -   Time office software

    3.1.4   PACS   -   Imaging

3.3   The department is responsible for development, maintenance, support and training of all software either in-house or third party.

3.4   The HIS/IMS/PMS modules meet most of the requirements for all the departments of SAIMS.

3.5   The IT Department is responsible for implementing the SMS (Short Message Service) applications.

3.6   The Information Technology department is responsible for providing technology support for SAIMS.

3.7   This supports includes maintenance and upgradation to the network infrastructure, business applications such as email, Internet, information security, desktop computer support, and reporting.

3.8   The IT department supports SAIMS hardware and software installation, troubleshooting and upgrades for staff.

3.9   In addition, the IT department is responsible for various academic computing aspects, including computer Domain policy and management oversight, academic software licensing, and overall IT governance.

3.10   The Technology Help desk is also an integral part of the IT support to SAIMS, and provides end user support as well as telephone directory.

4.0 ABBREVIATIONS:

4.1   NABH   : National Accreditation Board for Hospital & Healthcare Provider

4.2   IT   : Information Technology

4.3   HIS   : Hospital Information System

4.4   SAIMS   : Sri Aurobindo Institute of Medical Sciences

4.5   IMS   : Inventory Management System

4.6   PMS   : Pharmacy Management System

4.7   PACS   : Picture Archival & Communication System

4.8   PO   : Purchase Order

4.9   WO   : Work Order

4.10 UTM   : Universal Threat Management

4.11 MSSQL   : Microsoft Structured Query Language

4.12 SSRS   : SQL Server Reporting Services

4.13 MS   : Microsoft

4.14 SDLC   : Software Development Life Cycle

4.15 AMC   : Annual Maintenance Contract

4.16 OPD   : Out-Patient Department

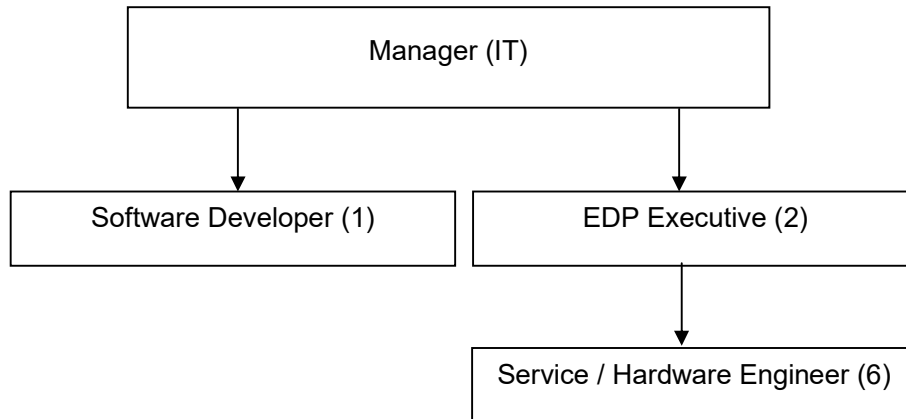4.17 LAN   : Local Area Network

5.0   DEFINITIONS:

5.1

6.0   RESPONSIBILITY:

6.1   Manager (IT)

6.2   Hardware Engineers (Centralized team)

6.3   Software Engineers (Centralized team)

7.0 DEPARTMENTAL HIERARCHY:

```
                    ┌──────────────────────┐
                    │     Manager (IT)     │
                    └──────────┬───────────┘
              ┌────────────────┴────────────────┐
              ▼                                  ▼
  ┌────────────────────────┐      ┌────────────────────────┐
  │ Software Developer (1) │      │   EDP Executive (2)    │
  └────────────────────────┘      └───────────┬────────────┘
                                              ▼
                               ┌──────────────────────────────────┐
                               │ Service / Hardware Engineer (6)  │
                               └──────────────────────────────────┘
```

8.0 COMPETENCY MATRIX:

Sr. No.	Name of the staff	Designation	Educational Qualification	Experience (Years)		
				SAIMS	Previous	Total
1	Sameer Poorkar	Manager (IT)	B.Sc. (Elec)	5	21	26
2	Vaibhav Limaye	Manager (IT)				
3	Ghanshyam Mishra	EDP Executive				
4	Sherbahadur Singh					
5	Manoj Choudhary					
6	Wasim Sheikh					
7	Pawan Godle					
8	Sunny Godle					
9	Rajesh Sharma					
10	Sameer Ranade					

9.0 ROLES AND RESPONSIBILITIES:

9.1 Manager IT :

9.1.1 Functional & administrative Head of IT department.

9.1.2 Responsible for day to day activities and smooth functioning.

9.1.3 Act swiftly to take apt action in line with policy of the management under emergency situation.

9.1.4 Responsible to provide and maintain Hospital Information System (**HIS**), Inventory & Pharmacy Management System & other third party applications.

9.1.5 Responsible to Recommend / Finalize the Capital and Consumables and to release Purchase / Work Orders (**PO / WO**).

9.1.6 Provide the required training for the users to use the respective module of HIS/IMS/PMS & other third party applications**.**

9.1.7 Maintain and Upgrade the hardware, software, networks, UTM, database and required infrastructure.

9.1.8 Responsible to assign / participate IT conference / seminars conducted by premier IT vendors like IBM , HP. Dell, Oracle , Microsoft, CITRIX, Cisco, etc.

9.1.9 Create master entries and make changes in existing master entries for respective application.

9.1.10 Assign user ID to the new user as per request from the user's HOD.

9.1.11 Troubleshoot problems arriving on Windows Server and MSSQL Database.

9.1.12 Maintenance and support of third party applications (PACS, Time office, console applications of CT/Sono/Xray etc.)

9.2 Service / Hardware Engineer # 1:

9.2.1 Operating System, Software and Drivers Installation on user machines.

9.2.2 Maintenance & Service.

9.2.3 Networking support.

9.2.4 Operating System, Software and Drivers Installation.

9.2.5   Desktop, laptop & printers maintenance.

9.2.6   Support for Email & Internet.

9.2.7   Anti-virus Security.

9.2.8   Audio-visual support.

10.0 DEPARTMENT WORKING HOURS:

10.1   There are multiple shifts as mentioned below.

Sl. No	Designation	Working Hours	Shift Timings
1	Manager (IT)	8 Hrs	10.00 – 18:00
2	Service / Hardware Engineer	8 Hrs	10.00 – 18:00
3	Service / Hardware Engineer	8 Hrs	08.00 – 04.00
4	Service / Hardware Engineer	8 Hrs	09.00 – 05.00

11.0 REFERENCE TO NABH STANDARDS:

S.No	Chapter	Relevant NABH Standard / Objective Element
1.	Continuous Quality Improvement	The organization identifies key indicators to monitor the managerial structures, processes and outcomes which are used as tool for continual improvement. **CQI.3.**
2.	Responsibility of Management	The services provided by each department are documented. **ROM.2.**
3.	Information management system	Policies and procedures exist to meet the information needs of the care providers, management of the organization as well as other agencies that require date and information from the organization. **IMS.1.**
4.	Information management system	The organization has processes in place for effective management data **IMS.2.**

12.0 POLICIES:

12.1 **Policy on network and data security:**

12.1.1 The IT department has limited access to authorized person only to safeguard the data. To enhance security UTM is placed on the top of network.

12.1.2 Direct access from website to database or file server is not available and hence there is strict control on the database.

12.1.3 The requirement and laying of new network is first analyzed by the Manager (IT).

12.1.4 The server needs to be restarted on every Friday for smooth functioning of Applications.

12.2 **Policy on storing and retrieving data:**

12.2.1 To access in-house applications, Employee ID and Password is must while to access third party software, user id & password is must.

12.2.2 The password rule ensures each employee need to reset their password periodically.

12.2.3 The authorized user can access the storage system and access the file server.

12.3 **Policy on data back-up:**

12.3.1 There is a pre-defined schedule of doing daily and yearly maintenance.

12.3.2 There is also a pre-defined time frame for data back-up storage.

12.4 **Policy on contribution to external database:**

12.4.1 External database contribution is not available.

12.5 **Policy on Hardware Procurement & Maintenance:**

12.5.1 The purchase process is through appropriate vendor selection process.

12.5.2   There is a schedule for planned preventive maintenance and attending to breakdown calls.

12.5.3   The downtime of the machines and the response times are monitored.

12.6   Policy on Validation and authentication details of applications:

12.6.1   All modules of HIS/IMS/PMS application, validation and authentication are done as per User Wise / Department Wise.

12.6.2   The authentication is user defined password, and users recommended changing the password at least once in sixty days.

12.6.3   Daily verification of database backup schedule is done and ensured that the backups are copied to external media.

12.7   Policy on Internet and Email:

12.7.1   Role based internet access have been assigned to limited user.

12.7.2   Internet access policy is defined using UTM device.

13.0 PROCEDURES:

13.1 Procedure for network and data security:

13.1.1 Security of the physical environment:

13.1.1.1 Limited access to location where Windows/database servers & storage server are placed.

13.1.1.2 User access is defined as per requirement based on role and requirement using Windows Group Policy/Permissions.

13.1.2 Security of online data:

13.1.2.1 There is no external data exposure for internet oriented access.

13.1.2.2 Direct access from website to Database or file server is not available

13.1.3 Requirement of a New Network Point:

13.1.3.1 Whenever a new Network point is required in the Hospital, Manager (IT) analyses the existing network and suggests that from which network switch the new network point is to be provided.

13.1.3.2 Then the Maintenance department is informed about the new network point requirement and the details regarding the start point and the end point for laying the cable is provided.

13.1.4 Laying of New Network Cables:

13.1.4.1 The network cables are laid by the Maintenance Department. After this the cables are crimped by Hardware Engineer and they are connected to the free ports on the Network Switch.

13.1.5 Maintenance of Switches and Routers:

13.1.5.1 The Switches needs to be restarted on Monthly basis for smooth functioning of Network.

13.1.6 Procedures for AMC renewals:

13.1.6.1 The devices, for which AMC is required, negotiated every year and it should be less 10% of purchase price.

13.1.6.2   In case of some network problem the vendor should provide support immediately either onsite or using remote access.

13.1.7 LAN Details:

13.1.7.1   The LAN of the SAIMS is an Ethernet LAN.

13.1.7.2   IT team has used a combination of star topologies.

13.1.7.3   The LAN consists of approximately 250 nodes comprises of server/desktop/laptop/thin client.

13.1.7.4   All the departments and different sections of the SAIMS constitute the users of this LAN.

13.1.7.5   Most of the nodes have been categorized under the DOMAIN 'BGHI' and few are in 'WORKGROUP'. Few nodes are out of LAN as per the requirement.

13.1.7.6   SAIMS Back bone switches are connected using OFC cables Single Mode.

13.1.7.7   Tail End Switches are connected using CAT5E and CAT6 Cables.

13.1.7.8   The following peripherals have been used in the LAN:

        13.1.7.8.1   Router.

        13.1.7.8.2   Switch.

13.1.7.9   MAIN Router is installed in IT Department, basement.

13.1.7.10 The MAIN switch in basement is the distribution point for all the nodes of the SAIMS. Multiple switches are installed in campus as per the distribution requirements.

13.1.7.11 Pictorial representations of the LAN layout have been provided in the later pages.

13.2   Storing and Retrieving of Data:

13.2.1   From the Database Storing and retrieving of data is performed through applications.

13.2.2 All in-house applications required Employee ID and Password to access the database. While third party applications access are based on user id and password.

13.2.3 The password rule ensures each employee need to reset their password periodically.

13.2.4 Another kind of storage is performed File Server (Central storage).

13.2.5 The privileged user can access the storage system and access the file server.

13.3 Data Back up:

13.3.1 Daily Backup:

13.3.1.1 All application databases are scheduled for backup every day. Backup process is automated and process start in the midnight. This backup set is stored on the same server. Backup set is checked by Hardware Engineer in the morning.

13.3.1.2 To create a copy, backup files are being copied on the storage device immediately after the backup process completed on the server. This process is also automated and immediately executes after the server database backup.

13.3.2 Data backup Retention period for back-ups:

13.3.2.1 The Database backup and retention period tape backup period as follows: daily backup – three days. Yearly / Financial Year Backup – minimum three years.

13.4 Contribution to external data base:

13.4.1 External database contribution is not available.

13.4.2 **Forms and formats:**

13.4.2.1 Presently database corrections through the applications only. However in very few cases the database needs to be updated by IT Personnel with request & recommended from the user department.

13.5 **Hardware Procurement & Maintenance:**

13.5.1   Procedure for New Hardware Procurement:

13.5.1.1   Desktops, Printers, scanners and Projectors:

13.5.1.1.1   A purchase indent is sent/mail by the respective user for the requirement of computer/printer etc. along with the approval of the department head.

13.5.1.1.2   The indent is evaluated by Manager (IT) along with the departmental head and the requirement is forwarded to Managing Director for Approval.

13.5.1.1.3   Quotations from three or more vendors are invited and a comparative statement is prepared.

13.5.1.1.4   The vendors are called for negotiation and the order is finalized by the Manager (IT) based on the following criteria:

13.5.1.1.4.1   His company should be more than 10 years old in this business.

13.5.1.1.4.2   His service experience should be more than 5 years.

13.5.1.1.4.3   He is ready to keep an inventory of spares / Standby computers / printers in our premises.

13.5.1.1.4.4   His quoted price is lowest.

13.5.1.2   Servers and Storage Solutions:

13.5.1.2.1   Central Purchasing from SAIMS.

13.5.1.3   Procedure of Hardware Installation:

13.5.1.3.1   The Vendor who has been awarded the Purchase order delivers the Hardware to Stores Department.

13.5.1.3.2   The goods received note (GRN) is prepared by the stores department after verification of Hardware components by Hardware Engineer.

13.5.1.3.3 The hardware is brought to computer department after giving the store indent to the stores department and the required software's are installed and the domain polices are applied.

13.5.1.3.4 The PC's are numbered as per the running number. The PC is then installed in the user department.

13.5.1.4 <u>Procedure for Call Management:</u>

13.5.1.4.1 Calls are received by the Hardware Engineer from various departments and wards. Call logs are maintained in software **BUGNET**.

13.5.1.4.2 The call may be categorised as non-functioning or partially functioning of the hardware.

13.5.1.4.3 The call details are given to the hardware engineer in the department.

13.5.1.4.4 The engineer tries to solve the problem through remote management, if possible, if not he attends the call personally.

13.5.1.4.5 After attending the complaint the details are entered in the call management software.

13.5.1.4.6 If the call is completed then it is closed, otherwise the problems is escalated to the higher level.

13.5.1.4.7 If the problem is regarding hardware related spares then the spares are replaced from existing stock in the EDP maintained.

13.5.1.4.8 If the required spares are not available in that case a standby PC is given on a temporary basis.

13.5.1.4.9 The computer received from the department is repaired by the engineer after availability of spares and is given back to the department and the temporary PC is brought back to the EDP Department.

13.5.1.5   <u>Procedures for AMC renewals:</u>

13.5.1.5.1   For all vendors it is mandatory to give a 5 Year warranty on Server, 3 year warranty on PC & 1 year warranty on the Printers.

13.5.1.5.2   After the warranty period or AMC period is over, an invoice is received from the hardware vendor. Based on usage requirement in future, AMC is renewed else hardware is maintained on call basis.

13.5.1.6   <u>Procedure for Hardware condemnation:</u>

13.5.1.6.1   When any hardware of department is not working and is beyond repair or repair cost is more than 25 % cost of new hardware then the hardware is condemned.

13.5.1.6.2   In case of not repairable condition of any hardware, certify it by hardware engineer and sent to SAIMS.

13.5.1.6.3   Materials department call vendors to sale the condemned material, and the highest quotation-giving vendor selected to purchase it.

13.5.1.6.4   Materials department mark the condemned hardware, then prepare Gate Pass (non-returnable) through material office and vendor takeout the material from EDP.

13.6 **Preventive Maintenance chart:**

Preventive Maintenance Activity	Frequency	Auto/Manual
Restart Server (Windows/Database/Application)	Weekly (Friday at 18:00 Hrs)	Manual
Restart Switches/Access Points/Routers	Monthly	Manual
Scan for viruses	Continuous	Auto
Back up data	As scheduled	Auto

Clean CRT screen	Daily by Users	Manual
Scan for hard disk read errors	On demand	Manual
Clean mouse	Daily by Users	Manual
Check for full hard disk volumes and remove unnecessary files	Continuous by users	Manual
Update virus definition files	Daily	Auto
Clean disk drive internals and read/write heads	On-demand	Manual
Check processor & SMPS fan to ensure they are working	During Preventive Maintenance – half yearly / On-demand	Manual
Check hard disk for any noise	During Preventive Maintenance – half yearly / On-demand	Manual
Clean exterior of case	During Preventive Maintenance – half yearly / On-demand	Manual
Clean exterior of monitor	Daily by users	Manual
Check and clean interior, motherboard and expansion cards if necessary	During Preventive Maintenance – half yearly / On-demand	Manual
Check internal connections and cables	On-demand	Manual
Clean keyboard	Daily by users	Manual
CCTV	Daily	Manual
PA System	Quarterly / On demand	Manual

13.7   **Validation and authentication details of applications:**

13.7.1   All modules of applications, validation and authentication are as per user wise / department wise.

13.7.2   The authentication is user defined password, and users recommended changing the password at least once in sixty days.

13.7.3   Daily verification of database backup schedule and ensure that the backups are copied to external media. The daily backup is scheduled at 1:00 AM.

13.7.4   Verify the execution of various day end scheduled process that are executed during the previous night.

13.7.5   The Day End Schedule processes are:

13.7.5.1   The Systems Personnel reporting in regular timing are expected to check the above noted process is executed.

13.7.5.2   Daily Review of pending complaints and take necessary actions.

13.7.5.3   Review the daily statistical reports and forward the same to the Chairman office.

13.7.5.4   Verify the attendance of the department staffs and take necessary actions in case of any deviations in shifts.

13.7.5.5   Periodic rounds to the user departments.

13.7.5.6   Periodic meeting to review for smooth functioning of the departments.

13.7.5.7   Provide application training to the new staff in each department.

13.7.5.8   There is no specific schedule for training; however every new recruit is trained in his or her respective fields.

13.7.5.9   Coordinate with the Head of Department for any new Hardware and Software requirements.

13.7.5.10   Periodic Review of Applications, Database, Network, Servers, UTM, Security, Backup, Communication, and Video Network.

13.8   **Application & Software Details:**

13.8.1   RDBMS   :   MSSQL Server 2008 R2

13.8.2   Development Tools / IDEs   :   Visual Basic 6/C#/Crystal Report/AngularJS/SSRS

13.8.3   Vendor   :   Microsoft

13.8.4   Operating Systems Of Production Database:

13.8.4.1   Environment   :   MS Windows Server 2012

13.8.5   Operating Systems of Domain Server:

13.8.5.1   Environment   :   MS Windows Server 2012 Virtual Machine

13.8.6   Operating Systems of Storage Server:

13.8.6.1   Environment   :   MS Windows Storage Server

13.8.7   Operating Systems used in Deployment (Client Side):

13.8.7.1   Environment   :   MS – Windows XP/Windows 7

13.9   **Hospital Management System – HIS/IMS/PMS:**

13.9.1   **Modules:** Hospital information system that includes all the principal and important modules for a super-multi specialty hospital. The various important modules as follows:

13.9.1.1   ADMISSION SYSTEM.

13.9.1.2   NURSING STATION.

13.9.1.3   OPD BILLING.

13.9.1.4   LABORATORY.

13.9.1.5   INFORMATION SYSTEM.

13.9.1.6   PHARMACY

13.9.1.7   BILLING.

13.9.1.8   USER MANAGEMENT.

13.9.1.9   BILLING/DEBTORS MANAGEMENT.

13.9.1.10   ACCOUNT MANAGEMENT (Transfer to Tally).

13.9.1.11   INVENTORY AND PURCHASE MAINTENANCE.

13.9.1.12   PAYROLL SYSTEMS.

13.9.1.13   MIS/DECISION SUPPORT SYSTEM (DSS).

13.9.2   **New Software Requirement:**

13.9.2.1   Whenever there is a New Software requirement for any department, Manager (IT) is informed for the same. The software/module is developed in-house as per the instruction from Manager (IT).

13.9.2.2   Below are the steps involved in Developing a New software:

13.9.2.2.1 SDLC: The System Development Life Cycle is the process of developing a new software from system study to the implementation and troubleshooting of the

new software. The steps involved in SDLC are as under:

13.9.2.2.1.1 Feasibility: The feasibility study is used to determine if the project should get the go-ahead. If the project is to proceed, the feasibility study will produce a project plan and budget estimates for the future stages of development.

13.9.2.2.1.2 Requirement Analysis and Design: Analysis gathers the requirements for the system. This stage includes a detailed study of the business needs of the organization. Options for changing the business process may be considered. Design focuses on high level design like, what programs are needed and how are they going to interact, low-level design (how the individual programs are going to work), interface design (what are the interfaces going to look like) and data design (what data will be required). During these phases, the software's overall structure is defined. Analysis and Design are very crucial in the whole development cycle. Any glitch in the design phase could be very expensive to solve in the later stage of the software development. Much care is taken during this phase. The logical system of the product is developed in this phase.

13.9.2.2.1.3 Implementation: In this phase the designs are translated into code. Computer programs are written using a conventional programming language or an application generator. Programming tools like Compilers, Interpreters, Debuggers are used to generate the code. Different high level programming languages are

used for coding. With respect to the type of application, the right programming language is chosen.

13.9.2.2.1.4 Testing: In this phase the system is tested. Normally programs are written as a series of individual modules, these subject to separate and detailed test. The system is then tested as a whole. The separate modules are brought together and tested as a complete system. The system is tested to ensure that interfaces between modules work (integration testing), the system works on the intended platform and with the expected volume of data (volume testing) and that the system does what the user requires (acceptance/beta testing).

13.9.2.2.1.5 Maintenance: Inevitably the system will need maintenance. Software will definitely undergo change once it is delivered to the customer. There are many reasons for the change. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that could happen during the post implementation period.

13.9.3 Procedures for software changes:

13.9.3.1 Any changes that are needed by the user department are brought to the notice of the Manager (IT).

13.9.3.2 The request is studied to quantify the changes.

13.9.3.3 If the changes requires a change in logic of the system or requires more than a day work [i.e. a major change] then it is

brought in the knowledge of Managing Director for approval or disapproval.

13.9.3.4 Any minor changes required are done in consultation with the software consultant and software programmers.

13.9.3.5 The changes are made in a test environment and tested in a test servers.

13.9.3.6 After the approval of the Manager (IT) and respective user department head the same is installed in the live environment.

13.9.4 Procedures for AMC renewals:

13.9.4.1 For In-house developed, no AMC is required.

13.9.4.2 Every year prior to renewal of AMC of third party applications, quotation is called and after comparing with purchase cost and after best negotiation, AMC get renewed.

13.10 **Internet & Email:**

13.10.1 The LAN environment consists mostly of PC's working on Win 7 (Prof) and Win XP (Prof) operating systems. Most of the printers are Inkjet, Dot Matrix and LaserJet (mono). While the LAN is used for file sharing, shared printer sharing etc

13.10.2 All client PC's in the SAIMS LAN have been installed with Quick Heal Antivirus solution to protect from virus threats.

13.10.3 The website of the SAIMS is hosted at the address www.saimsonline.com.

13.10.4 SAIMS has websites of its own. They are listed below:

13.10.4.1 www.saimsonline.com

14.0 QUALITY OBJECTIVES:

14.1   The following Quality objectives are followed by SAIMS IT team on all its development and Implementation activities:

14.1.1 To minimize the down time of server & network.

14.1.2 To ensure Safety and security of all the data.

14.1.3 To provide 24/7 Hardware, Application and Network support to the users.

14.1.4 To ensure the Compliance and Licensing.

15.0 QUALITY INDICATORS:

S.no	Performance indicator	Numerator	Denominator	Standardization factor
1	Response time for completion of breakdown calls	Total Time taken between registering to completion of breakdown call	Total number of breakdown calls	Average

16.0 DATA INFORMATION:

16.1   All the quality indicators are monitored at appropriate interval as defined in the policy.

16.2   The report shall be submitted to the Quality department or NABH coordinator.

16.3   Improvements on the quality care indicator shall be discussed in the Quality Assurance Committee.

16.4   Appropriate corrective and preventive actions shall be taken and the documentation done of the same.

17.0 RECORDS:

17.1   All the below mentioned records shall be maintained in the EDP department and destruction shall be done by the Administrative Department after getting approval from the management.

SR. NO.	TITLE	RESPONSIBILITY	REFERENCE	RETENTION PERIOD
1.	Software License	Manager (IT)	www.microsoft.com	
2.	Vendor Details	Manager (IT)	Soft Copy	
3.	Mail User Details	Manager (IT)	www.admin.google.com	
4.	Internet Policy &User Details	Manager (IT)	UTM Software - Policy & Objects	
5.	Asset Details	Manager (IT)	Soft Copy	
6.	Network Diagram Details	Manager (IT)	Soft Copy	
7.	Database back up Details	Manager (IT)	Soft Copy	
8.	Domain and policy Details	Manager (IT)	Online at Windows Server	
9.	Service Calls	Hardware Engineer	BugNet Software	
10.	Preventive Maintenance Details (Server / Desktop)	Hardware Engineer	Soft Copy	
11.	CCTV Preventive Maintenance Details	Hardware Engineer	Soft Copy	
12.	PA Preventive Maintenance Details	Hardware Engineer	Soft Copy	
13.	Purchase Order	Manager (IT)	Soft Copy	

18.0 TRAINING:

18.1   All Engineers and Technicians shall be trained regularly regarding the emergency management of patients, their treatment and how to handle different emergencies.

18.2   All new joining staff shall be oriented to the department by the Head of the department.

18.3   Training needs of the staff is assessed by the head of the department based on the performance of staff.

19.0 LIST OF EQUIPMENTS:

20.0 ANNEXURE

Principal,
Sri Aurobindo College of Dentistry
INDORE (M. P.)