




List of e-governance software/websites

1. Adroit HMS Medisteer
2. CAL pharm
3. CAMU
4. Delnet
5. ESSL e time track
6. Examination
7. KOHA
8. Moodle
9. ProQuest
10. Tally

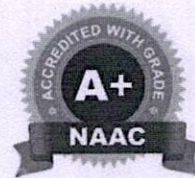

DIRECTOR
Sri Venkateshwaraa Medical College
Hospital & Research Centre
Ariyur, Puducherry - 605 102



sri venkateshwarraa
Medical College Hospital and Research Centre

CREATING HEALTHIER SOCIETY

Ariyur, Puducherry 605 102.

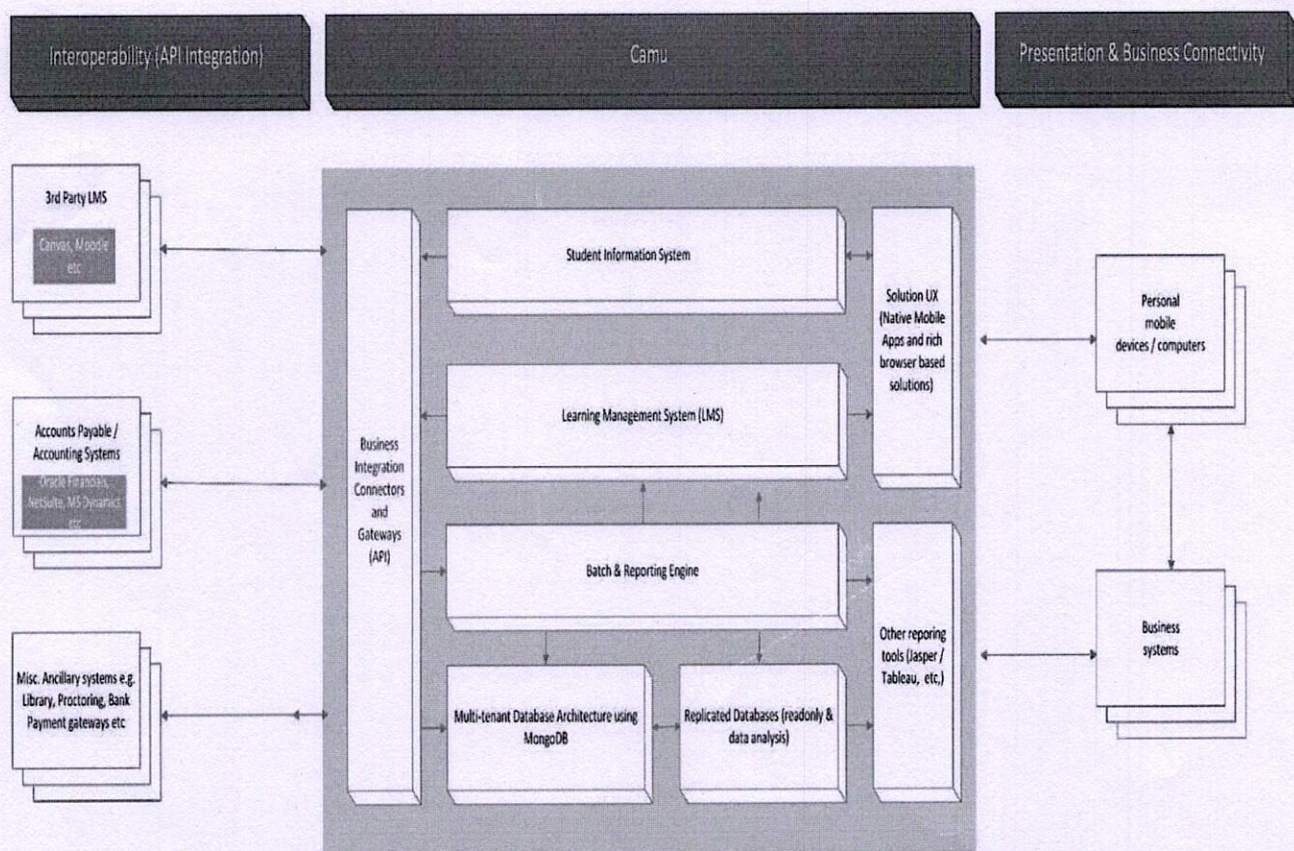


Department of Information Technology | E-Mail: infotech@srivenkateshwarraa.edu.in

SRI VENKATESHWARAA MEDICAL COLLEGE HOSPITAL AND RESEARCH CENTRE

CAMU ARCHITECTURE

Camu Application Architecture



E-GOVERNANCE INITIATIVE:

1. Adopted and implemented e-governance in maximum areas of operation entered into an agreement with a CAMU ERP vendor and provided efficient system of governance within the institution.
2. Implemented e-governance in Administration, Student Admission, Support Services, Accounts and Examinations.
3. Demonstrated the policy through CAMU ERP trainings given All Staffs.

AREAS OF E GOVERNANCE:

1. **Website:** The website of the college acts as the face of the college activities and provides information about all programmers, important notices. Faculty are given an additional responsibility of managing the website of the college.
2. **Student Admission:** The College processes admissions for all programmers through online mode.
3. **Attendance:** Online portal is launched for students to view attendance, internal marks and OD availed.
4. **Accounts:** For effective maintaining of accounts, the society uses Tally ERP9 software. And Tally ERP9 Integrated to HMS Software
5. **Library:** Library is fully automated. Koha Technology, Smart card and Biometrics are used for efficient e-governance.
6. **Administration:** Facilities for online leave management of employees, e copy of salary certificates, booking of venues, internal communication are processed through e-governance.

7. **Examination:** As per the directions of the Affiliating University, the institution follows the CAMU ERP module for examination purpose.
8. **Alumni:** In order to strengthen alumni interaction, a separate alumni portal is provided with registration, information of the college activities, list of prominent alumni, achievements of the alumni and feedback.



srivenkateshwaraa

Medical College Hospital and Research Centre

CREATING HEALTHIER SOCIETY

Ariyur, Puducherry 605 102.



Department of Information Technology | E-Mail:infotech@srivenkateshwaraa.edu.in

SRI VENKATESHWARAA DENTAL COLLEGE

Standard Operating Procedures

1. Purpose

The purpose of the SOP is to provide the Sri Venkateshwaraa Group of Institutions staffs, faculties and system users, high quality technical services provided by the Department of Information Technology and to assist management computer users in finding the appropriate resource to answer their questions, resolve any computer or network related problems, Software Issues, applications update, security update, Hardware update and assist with Organization Technical needs.

2. Mission

The Vision of the Information Technology is to most practices claim convenience, we live by it. We strive to make IT services as convenient as a light switch. We do that by improving our availability, increasing user's choice, and lowering wait time. We're committed to investing in the latest technology to identify the problem and resolve the problem instantly.

3. Vision

The mission of the Department of Information Technology is to provide opportunities for enhancement in the Sri Venkateshwaraa Group of Institutions operations by implementation and incorporation of technological advancements in secure level hardware, software Automation and Digitalize Campus.

4. Scope of Work

The IT Department provides technical assistance and maintenance and oversight of the Sri Venkateshwaraa Group of Institutions computer networks, software's, hardware's, Centralized Security Surveillance network, and any technology initiatives within the Group of Institutions. The IT Department encourages department staffs in planning for future Digitalized environments for the Group of Institutions. We also hope that by understanding the role the IT Department plays in maintaining the reliability and integrity of Technology resources.

5. Contact Information

The Department of Information Technology is located in the Dental College Fifth Floor.

IT-INCHARGE – Balamurugan.B	Email: infotech@srivenkateshwaraa.edu.in Telephone: 0413-2260601 Extn: 444
System Engineer	Pandiyan.R
System Engineer	Elamparuthi.B
System Engineer	Rameshkumar.M
IT Technicians	Veeraminikandan.K, Santhakumar.K, Canniyaprabu.S.

6. Responsibility and Roles:

The IT Department determines and conceptually plans the best ways for technology to meet the goals of the Management. The IT Department will be responsible for developing new ways to accomplish tasks in a Technology timely manner. All Virtual devices and applications added to the Centralized servers have an impact on the overall network. The IT Department ability to properly support new devices and applications often require additional

resources that may take time to acquire and install. The IT Department will balance the load of services across resources as necessary. The Department of Information Technology is responsible for the following functions:

- Internet Access & E-mail.
- Servers, Computers, Laptop and other Hardware Accessories.
- Firewall, Routers, Network Switches and other Accessories.
- Management Softwares and Application Softwares.
- Copiers/Fax/Scanners – All peripherals
- Video & Audio equipment.
- Maintains network security and performance; establishes workable directory structure, network security, and Centralized disk space allocation, etc.,
- Setup user accounts according to set established policies, procedures, and limitations.
- Tracks all Category of issues and requirements through Phone call, Ticketing and approval letters.
- Plans Network Data ports when needed.
- Performs network maintenance, changes and upgrades.
- Enhances network by assessing new software and hardware products that would increase network performance and expand network services.
- Directs the performance of regularly scheduled systems management and maintenance procedures designed to ensure the integrity of all programs by running backup procedures and diagnostic software routines.
- Implements disaster recovery plans; runs system backups and disaster recovery operations.
- All Institutions surveillance under CCTV implementation and maintain.
- All Institutions Biometric device like face reader, finger print Implementation and maintain.

- Develops procedural documentation or policies as needed.
- Provides technical advice and training to staff in the faculties, Non-Teaching, Administration and Maintenance.
- Prepares reports and makes recommendation to ensure the optimum efficiency of equipment and systems in accordance with departmental needs.
- Maintains stock of expendable and non-expendable computer equipment, materials, system, application, and supplies sufficient to ensure continuous and uninterrupted operation of systems; communicates with vendors regarding purchases.
- Maintains professional and technical knowledge by conduction research; attending seminars, education workshops, online classes and conferences; reviewing professional publications and related organizations.

7. Software

The IT Department will maintain all software which is located on the Group of Institutions. As it pertains to software, the following procedures will be followed:

- a. The IT Department will maintain a current list of standard and recommended software's.
- b. To ensure software is compatible and not destructive to the computer systems, the IT Department will approve software programs.
- c. If a user is interested in software that is not on the maintained list, the user will need to give request letter to the IT Department and then it will be analyze by the IT engineer assistance in determining if that software is sustainable on systems and network.
- d. The IT Department will determine if software is qualified and need as being compatible with system Configuration in Group of Institutions.
- e. If software is not qualified as being not compatible with the System Configuration or the software is purchase wrongly, the software will be returned to supplier and cannot be installed on the system.

- f. If a software program exceeds the specifications of the user's computer system the user will be notified to look for alternative software or to upgrade the system as per IT policy.
- g. All Software user Login credentials will be provide by as per IT policy.
- h. The user will be responsibility after provide the Login details for software's.
- i. All software installed on Group of Institutions by IT department as per management policy.
- j. All software installed on Group of Institutions on the servers must have a valid license.
- k. The Software should installed in the servers make a server unstable, the IT Department will be responsible for restoring any data that was stored on a server that is backed up by the IT Department backup server.
- l. The IT Department is obligated by certain software vendors to monitor all software licenses in order to ensure compliance with the vendor's license agreements.
- m. Users may contact the IT Department through phone call or ticket raise by software to obtain additional guidance, queries and issues on any software.

8. Hardware

The IT Department will maintain all hardware which is located on the Group of Institutions. As it pertains to hardware, the following procedures

Will be followed:

- a. The IT Department will maintain a current list of System Asset.
- b. If a user is required in computer hardware, the user will need to provide an approval letter through concern institutions Dean or Chairman and then IT Department assistance in determining if that computer is sustainable to user and give specification to Purchase department to procure the computer hardware.
- c. The IT Department will determine if hardware is qualified as being standard as per given requirement.
- d. If hardware is not qualified as being standard with the given requirement, it will not be installed.

- e. The IT Department and the concern users will be responsible for all hardware that is associated with the Group of Institutions.
- f. Fully supported hardware are those hardware devices which are maintained by the IT Department. The IT Department recommends install and tests the compatibility and specification of such hardware with all supported environments, and may upgrade hardware when new technology are released or become available.

9. Replacement Plan

The IT Department will follow an 8 year Computer Replacement Plan.

This plan will provide for the systematic replacement of older computers that are connected to the Group of Institutions but are:

- a. Not adequate to provide access to all services available on the computer or
- b. Not adequate to support advanced needs of the specific user.

If a system requires an upgrade before the scheduled computer replacement date, the IT department engineers will need to be sent to the purchase request through proper channel and providing a detailed justification for why the computer must be replaced.

10. Relocation of Computers or Printers

The IT Department will be responsible for relocating all computer systems and peripherals. An user must be inform to the IT department for the Support ticket or phone call at least one business days in advance of the relocation to avoid delays in the setup process. In the case of an extreme emergency, the user must contact the IT-INCHARGE.

11. Material to be Checked Out

The IT Department maintains material checking for users. This Materials (computer, laptops and Network accessories etc.) can be check out by IT Engineers.

All items may be checked out for concern user and management purposes only. When

using the computer and other IT devices, it is important for the user to follow all applicable rules and regulations associated with such devices.

12. Website

The Sri Venkateshwaraa Group of Institution websites are designed and Maintain by Digital Marketing department with the support of IT Department.

13. Condemnation of IT Materials

The IT Department condemned the defective and outdated IT Materials. In order to have the condemned IT materials, the user must complete an IT condemnation process and submit it to the IT Department. The IT Department will keep outdated Materials in storage for at least 90 days, after which, the IT devices will be disposed of an environmentally friendly electronics recycle location where the hard drives will be destroyed and a certificate of destruction will follow.

14. Data Backup/Disaster Recovery Plan

The IT Department provides complete automatic backup services on Group of Institution servers located at centralized location. Data is backed up to provide server failover and disaster recovery and also to provide for future retrieval. The IT Department plan minimizes disruptions of critical functions and ensures the capability to recover operations expediently and successfully.

15. Maintenance

The IT Department will schedule half yearly maintenance on the network to perform hardware & software updates and checking for errors. The IT staff will be schedule for the Maintenance work

16. Security

Maintaining data security is the responsibility of the IT-INCHARGE. The security

of the Group of Institution Server, computer system and Network is a major priority of the IT Department. The following are components to how the IT Department monitors the system's security:

- a) Each Department and Program will determine what data is considered public, confidential, or for official use only.
- b) The IT-INCHARGE will review all security alerts.
- c) The IT-INCHARGE will setup logs and review them to monitor possible security breaches.
- d) The IT-INCHARGE must maintain backups as needed to recover from deliberate security threats and damage.
- e) The IT Department will use Endpoint security software to protect the Group of Institution from email threats in the form of viruses and SPAM.
- f) The IT Department staff will log onto the email appliance to monitor mail activity with the intent of detecting email threats.
- g) The IT Department is able to log on to the server and client system remotely to ensure the network's security is effective.
- h) The Group of Institution is equipped with a firewall rules and policies to secure encrypted tunnel for remote users to gain a secure connection from outside the network.
- i) The Group of Institution network is equipped with firewall content filtering which allows for control of the users Internet access to the web. This service is used to monitor user's website visits and block inappropriate websites.
- j) If a user suspects security violation, they should submit a ticket or through phone call to the IT Support email address detailing the time and error that occurred on the user's system.

17. Remote Access

Remote access to the Group of Institution computer system and information is only permitted through secure, authenticated and centrally managed access methods. This access must be approved by the user and can only be used by IT

department. The IT-INCHARGE will establish a VPN connection and will ensure the connection is authenticated and encrypted

18. User Accounts, Email & Passwords

The IT Department assigns updates and monitors all institution email addresses and accounts. Additionally, the IT Department monitors and updates all systems passwords as appropriate for each individual user. Every new employee whose position requires them to use a computer will be assigned an email account with a password at the time of joining. Each department head must make an appropriate request for a new user setup to the IT Department through a request letter to set up a new user account. The same policy should follow up for the Software Login credentials. All computer users must change passwords every (6) six months. Each users computer system will prompt them to change passwords automatically. The IT Department reserves the right to have users change their passwords at any time if the system has been compromised.

19. Internet Access

The internet provides access to a variety of information, both good and questionable value and is not a secure means of communication. It is the responsibility of the user to ensure the Group of Institution Computer, Intranet, and Internet Use Policy is being followed. The IT Department will monitor user activity through monitoring and filtering software to prevent access to sites which are illegal or against IT policies.

20. Problem Resolution

The IT Department strives to provide the most effective and efficient services to the management employees and other users of the Group of Institution. If for some reason there is a complaint regarding the IT Department services or staff, this should be expressed to the IT-INCHARGE. If this does not lead to improvement, the complainant should be direct through the appropriate chain of Executives, the Administrative Officers, Chief Operation Officer and then the Chairman.

21. Reporting

The IT Department shall provide progress reports to the Chief Operation Officer on a quarterly basis or as requested. Timelines of the Annual Report and annual budget narratives are determined on an annual basis. The IT Department staff is responsible for ensuring all timelines are met according to directives.

22. Ticketing

If a user is experiencing a problem with their computer system or other electronic device, they must complete a ticket raised and send the document to the IT Support email address. In the event of an emergency or email is not working, the user can call the IT Department at intercom 444 or staff mobile to begin the troubleshooting process. The remedy will be addressed according to the severity of the problem. These types of problems will require the IT staff to do further research and often requires them to coordinate solutions with third parties



sri venkateshwarraa
Medical College Hospital and Research Centre
CREATING HEALTHIER SOCIETY
Ariyur, Puducherry 605 102.



Department of Information Technology | E-Mail: infotech@srivenkateshwarraa.edu.in

SRI VENKATESHWARAA MEDICAL COLLEGE HOSPITAL **AND RESEARCH CENTRE**

CAMU SOFTWARE POLICY DOCUMENT

Terms and conditions specific to License Fee Payments

- The License is activated upon order and the next year license fee will be invoiced as per the above schedule.
- Invoicing will be done based on the student count in Camu or as per any other terms agreed. The active students in Camu will have a direct impact on the license fee payable.
- The Invoice will be auto generated from Camu as per the payment schedule.
- The license fee is for the software demonstrated during the pre-sales engagement which may or may not have all the expected requirements.
- The Licensee is encouraged to adequately assess the software during the pre-sales engagement
- Camu will ensure that all the features demonstrated during the pre-sales engagement will be available in production

- Data to be loaded into the system should be provided in the specified templates within 14 Business Days from the start of the project. Any delay in Data provision and its implications will be the responsibility of the Licensee. There will not be any change to the payments schedule due to delay in data provision.
- Training Sign-off, Implementation Sign off or any other Sign off must be responded to within 5 business days or else it will be considered as signed off.
- Implementation Sign off will entitle the privileges for the licensee to get backup's, failovers, high performance servers. Once the first transaction is posted in the system by the users or by the Camu support team with authorization from the
- Licensee the system is considered live. It is the obligation of the Licensee to sign the Implementation Sign off document.

Scope and Specification

Following modules will be provided in this CAMU Campus Management Software

Student Information System (SIS)	
Admissions	<ul style="list-style-type: none"> ✓ Schedule and issue Applications ✓ Online applications and collection of application fees Workflow for Applications from Submission to Admission • Online Document Collection and Storage ✓ Allocation to Hostel and/or Bus Transportation

Student Record	<ul style="list-style-type: none"> ✓ 360 Student view ✓ Student Document Generation Bona fide Certificates • Transfers/Termination ✓ Automatically updated academic records
Staff Record	<ul style="list-style-type: none"> ✓ Staff record maintenance ✓ Publications, Research & Co-curricular activities ✓ Printing of statutory staff reports ✓ Resignations
Fee Management	<ul style="list-style-type: none"> ✓ Automatic generation of bills using billing policies Receipts, Credit Notes & Cancellations ✓ Outstanding bills and cash collection tracking ✓ Student Accounts View ✓ Online Payments with a Camu authorised payment gateway
Internal Examinations	<ul style="list-style-type: none"> ✓ Define and Conduct Internal Examinations ✓ Results entry ✓ Academic Performance Reports ✓ Download Master data for University Submission Upload University Results
Communication	<ul style="list-style-type: none"> • Mass communication to students and staff through a) Email ✓ SMS ✓ App Messages ✓ Announcements ✓ Chat facility for students and staff registered in a course

Learning Management (LMS)

Attendance	<ul style="list-style-type: none"> ✓ Attendance on Mobile Apps and by students scanning a QR code ✓ Attendance dashboard on Mobile Apps ✓ • Attendance reports
Academic Planning	<ul style="list-style-type: none"> ✓ Allocation of Staff to subjects ✓ Timetable creation ✓ Personal Lecture Schedule for Staff ✓ Students can view the Lecture Schedule ✓ Substitutions ✓ Day order method and regular weekday method ✓ Reallocation of staff
Teaching Plan	<ul style="list-style-type: none"> ✓ Creation and Maintenance of Teaching Plans ✓ Auto generation of teaching plans ✓ Print teaching plans ✓ Progress tracking of teaching plans
Assignments	<ul style="list-style-type: none"> ✓ Schedule assignments ✓ Student can submit assignments online ✓ Record and rate Assignment Submissions ✓ Transmit the Assignment rating to the student's Online submission of Assignments

Assessments	<ul style="list-style-type: none"> ✓ Online Assessments based on MCQ ✓ Automatic scoring of Assessments ✓ Scheduling of Assessments
Question Bank	<ul style="list-style-type: none"> ✓ Create and manage Question Banks ✓ Question banks with question linked to learning outcomes, bloom's taxonomy and rubrics. ✓ Generate Question Papers
Feedback	<ul style="list-style-type: none"> ✓ Record feedback on students ✓ Record feedback on staff ✓ Control on who can view the feedback
Video Conferencing	<ul style="list-style-type: none"> ✓ Video conferencing with MS Teams, Zoom ✓ Automatic Recording of Student Attendance ✓ Dashboards on Online classes
Outcome Based Education (OBE)	
Outcome Based Education	<ul style="list-style-type: none"> ✓ Define PEO, PO and CO for all Programs and Courses ✓ Blooms Taxonomy based Assessments ✓ Mapping of Question paper for all Examinations ✓ Question Bank with Mapping to Course Outcomes • Real time availability of Course and Program Outcome Attainment ✓ OBE Dashboards for Curriculum Design and Attainment

NAAC Reports (NAAC)	
NAAC Reports	<ul style="list-style-type: none"> ✓ De centralised Data Collection ✓ Role based Secure Access ✓ Supports Hierarchical Work flows for Accreditation Process ✓ Document and Content Management System(for NAAC related documents) ✓ Simulated Grades ✓ IQAC Dashboards for Workflow Management& Grade Review • Identifying Weak Metrics

Video Conferencing will be offered either with Zoom or MS Teams. The Licensee will purchase the Key and provide to the company for implementation.

The Online Gateway will be offered through Paytm.

IT Infrastructure Specifications

The Second Party will ensure following below mentioned IT infrastructure which is required to run CAMU software on the computer / (s).

S.N	Workstation	Name/ Description	Specification/ Recommendations	Remarks
1	Hardware	Intel Core 2 Duo processor with Minimum of 2 GB RAM, 10/100 MBPS Ethernet with about 200 GB of Hard Disk Space		To be Provided by the Second Party

2	Operating System	Operating System	MS Windows XP/7/8/10	To be Provided by the Second Party
3	Connectivity	Connectivity	LAN Connectivity Internet	To be Provided by the Second Party

4	Browser	Browser	Mozilla Firefox, Google Chrome	To be Provided by the Second Party
5	Mobile Devices	Tablet Devices or Mobile Phones running iOS or Android 4.3 or higher	Wi-Fi, 16 GB, 4GB RAM	To be Provided by the Second Party
6	Mobile Communication	Bulk SMS will be sent through the authorized service provider of the First Party.		
7	Wireless Connectivity	Wi-Fi connectivity in the campus to be installed by the Second Party.		To be Provided by the Second Party

8	Internet Connectivity	Internet Connectivity	Recommended to have a minimum of 4 MBPS Internet connectivity through the primary internet service provider for the use of CAMU. It is also recommended to have an alternate service provider and the necessary switch to automatically offer the backup in case of any downtime with the primary service provider	To be Provided by the Second Party
---	-----------------------	-----------------------	--	------------------------------------

Software Delivery and Implementation

- The Second Party is agree to provide Hardware and software mentioned in Table B to meet the infrastructure and hardware required by First Party.
- Site means, the location where the Institution is presently located and also its office/s present or future. If there is any additional site for which the software has to be implemented, the charges will be mutually agreed before proceeding with the implementation.
- The First Party agrees to integrate third party software's like MS Teams, Tally & KOHA (open source for Library management or any other software) If required by Second Party after mutually agreeing the configuration costs.

Upgrades and Customization of Software

Regular updated versions of the Camu Service that may be developed and released from time to time shall be offered at no additional cost. However, there is no obligation for the first party to provide any upgrades.

The product will be implemented as per the standard processes supported by Camu. Any customization to the software of any kind will be charged at Rs.10,000 per man day. The requirement and estimation must be agreed upfront and a written authorization must be provided by the Licensee to the company to execute the work and to Invoice the customer as per the agreed payment schedule.

Support and Response

In the event the Licensee requires the support of the Company with respect to any issues with the Software, the Licensee shall contact the Company via telephone, email or web portal (where available) during the Support Hours. The Licensee may contact the Company during After Hours only on the occurrence of the Severity 1 fault.

Response

Service request that is placed by the Licensee at the Service Desk in accordance with the terms of this SLA, the Service Desk shall perform an initial assessment of the service request as set forth in this agreement and provide support via (a) telephone or email; and/or (b) remote access to the Licensee's computer environment using appropriate support tools (where available).

Depending on the type of the service request, the Licensee and/or the Company shall be required to responsible in the following manner:

Level	Description	Ownership
Level 1	<ul style="list-style-type: none">✓ This is the first level of onsite support offered to the Licensee. The Licensee's IT team will respond to these issues.✓ In the event it is not within the Company's scope of responsibilities (e.g. relates to a network issue, configuration issue or training issue), it shall be handled by the Licensee	<ul style="list-style-type: none">● Licensee

	<ul style="list-style-type: none"> ✓ In the event it falls within the Company's scope of responsibilities as set forth in Appendix A of this SLA, it will be forwarded to Level 2. 	
Level 2	<ul style="list-style-type: none"> ✓ These are issues pertaining to the Software which requires resolution from the Service Desk. ✓ The Service Desk will handle these issues and respond in accordance with the agreed process and Service Levels. ✓ The Licensee shall provide the requisite corporation to the Service Desk to respond in accordance with the agreed process and service levels 	First Party Service Desk
Level 3	These are issues which require the involvement of the Company's development team. The Service Desk will continue to track the issues through to resolution or completion.	First Party's development Team in coordination with the Service Desk.

Response Time

The Company shall attempt to respond to faults with the Software in accordance with the following timeframes:

Severity	Description	Response
----------	-------------	----------

Level		Time
Severity 1	<p>Critical business impact: one or more key business functions cannot be completed.</p> <p><i>For example, Production server down, Application/DB down, a whole critical Module itself cannot be launched. No work around in any form exists. Without this resolved, business cannot continue. If needed, technical team should stop all other Development work and address this issue.</i></p>	Immediate
Severity 2	<p>High business impact: key business functions can still be completed but require process or performance compromise.</p> <p><i>For example, it is a showstopper but a work around exists or any important business process cannot be performed. Business can continue with the work around or tolerable until resolved.</i></p>	1 Day
Severity 3	<p>Medium business impact: significant defects impact key business functions but do not prevent function being completed, or a manual workaround exists.</p> <p>For example, the fix will be worked on with priority basis along with other high priority items.</p>	5 Days

Severity 4	<p>Low business impact: minor application error(s) or cosmetic issues. Key business functions can still be completed.</p> <p><i>For example, there are bugs/observations such as GUI issues, or issues arise in very rare scenarios. It follows the normal release cycle.</i></p>	5 Days
------------	---	--------

The Licensee acknowledges and agrees that the Response Time refers to the response provided by the Company to the issue with a diagnosis, further steps and delivery timescale where possible and does not guarantee a resolution.

The Company shall allocate a Severity Level to each fault logged by the Service Desk. The Company may need to downgrade the Severity Level if the Licensee does not provide the assistance required by the Company to enable the Company to resolve the fault.

Ownership of data or information shared:

All data or information including Confidential Information that is entered into the Camu software solution by the Second Party, its authorized persons or any of its students or faculty including such of this data or information that is stored on Camu's cloud ("Data") shall remain the property of Second Party and/or its students or faculty, as the case may be.

All Data collected through Camu shall be the property of the Second Party. It is the responsibility of the First Party to ensure the data is not lost at any point in time once saved in the CAMU system.

INTELLECTUAL PROPERTY

The Second Party acknowledges and agrees that all the rights, title and interest in the Software and Documentation as well as any customization, updates and upgrades to the Software and all the Intellectual Property rights therein are solely and absolutely owned by the First Party and shall continue to vest with the First Party during and after the Term of this Agreement.

TERM AND TERMINATION

a) This Agreement shall be effective for a period of 5 (Five) years (“Term”) which shall commence from the date of the purchase order. At the beginning of each Academic Session in June each year, the second party will apply for renewal of software license along with license fees as mentioned in payment schedule.

b) The Second Party may choose not to continue with the Agreement at the end of an Academic year due to non-performance of the First Party by providing at least 60(Sixty) days written notice to the Company. The notice of termination can be served only after settlement of all outstanding dues. The second party can terminate the contract by paying 20% of the value of the remaining period of the Agreement.

c) The first Party can only terminate if the agreed payment is not made by Second Party even after 30 days of the default.

LIMITATION OF LIABILITY

Under no circumstances shall either Party be liable to the other for any consequential, indirect, special, punitive or incidental damages, whether foreseeable or unforeseeable, based on claims of the other Party or suppliers (including, but not limited to, claims for loss of goodwill, loss of profits, loss of revenue, interruption in use or availability of data, stoppage of other work, computer failure or malfunction or impairment of other assets), arising out of breach or failure of express or implied warranty, breach of contract, misrepresentation, negligence, strict liability in tort or otherwise. Without prejudice to the above, in no event shall the liability of the Company whether to the Licensee or any third party exceed an amount representing the Annual License Fee paid by the Licensee to the Company under this Agreement.

GOVERNING LAW AND JURISDICTION

- a) This Agreement shall be governed by and construed in accordance with laws of India.
- b) In Case of any dispute, the Parties agree to resolve amicably, if need be, referred to the sole arbitrator mutually decided. The Venue of arbitrator will be Chennai & the language shall be English.

FORCE MAJEURE

- a) If the performance by either Party hereto, of any of its obligations hereunder is prevented, restricted or interfered with by reason of fire, or other causality or accident; strike or labor disputes; war or other violence; any law, or regulation of any government; or any act or condition whatsoever beyond the reasonable

control of such Party (each such occurrence being hereinafter referred to as a “Force Majeure”), then such Party shall be excused from such performance to the extent of such prevention, restriction or interference; provided, however, that such Party shall give prompt notice within a period of 24 hours from the date of Force Majeure occurrence and providing a description to the other Party of such Force Majeure in such notice, including a description, in reasonable specificity, of the cause of the Force Majeure; and provided further that such Party shall use reasonable efforts to avoid or remove such

MISCELLANEOUS

The parties hereto confirm that it is their wish that these Conditions as well as other documents relating here to have been and shall be drawn up in English only. This English version shall be valid and enforceable between the parties and both of them understand entirely any and all of its clauses.



SRI VENKATESHWARAA MEDICAL COLLEGE HOSPITAL AND RESEARCH CENTRE

Policy Documents:

Enterprise Software Solutions Lab Pvt Ltd (eSSL)

Software licensing policy

- In connection with your license activation, you agree to:
- Provide true, accurate, current and complete information about yourself as prompted by the registration form; and
- Maintain and promptly update such information to keep it true, accurate, current and complete. If you provide any information that is untrue, inaccurate, not current or incomplete, eSSL has the right to suspend or terminate your account and refuse any and all current and future use of the Services.
- "Software License Key" means a license key which activates and enables use of the eSSL eTimeTrackLite Software or any Paid-For Functionality within the eSSL eTimeTrackLite Software, for a defined period of time. The scope of the rights and permissions granted by any Software License Key and its duration will be as specified by eSSL at the time you order and purchase the same from eSSL or are otherwise supplied with the same;

- "you" or "your" means the person (including individuals, firms and companies and other organizations) to whom this Software License has been granted and who has purchased any Software License Key, or to whom this Software License may be transferred in accordance with Indian Software Privacy Act;
- For the avoidance of doubt, this Software License only covers the executable files we supply and does not extend to any source code
- You agree to permit us to audit your use of the eSSL eTimeTrackLite Software, including allowing us to visit and inspect any computers on which it is installed.
- The eSSL eTimeTrackLite Software is proprietary to eSSL and/or its licensors. All right, title and interest in and to the eTimeTrackLite Software and all copyright, trade secret rights, patents, trademarks and any other intellectual property or proprietary rights in and to the eSSL Software, and all copies of the eSSL eTimeTrackLite Software, regardless of the form or media on which it exists, shall at all times remain the exclusive property of eTimeTrackLite. All rights not expressly granted under this Software License are reserved by eSSL. You hereby acknowledge our ownership and rights stated above.

Return, Refund and cancellation policy

- Issued License key cannot be Surrendered / Non-Returnable
- There will be no refund of amount on Issued License key
- Issued license key cannot be canceled
- Issued License key is not transferable
- License key once issued cannot be re-issued. We do not guarantee licensed key in case of system crash/format or folders deleted.

Shipping/Delivery policy

This product is “Software” this can be downloaded from the url www.eTimetracklite.com Hence (Software-eTimetracklite) soft copy will not be shipped/delivery to the billing address

Legal Representative

eSSL's Privacy Representative is the Company Secretary. Any questions, concerns or complaints about the company's Privacy Policy or its practices related to privacy of personal information should be address to the Representative, as follows:



Adroit Soft India Pvt Ltd. Software Usage Policy

Policy Purpose

The purpose of Adroit Soft India Pvt Ltd. Software Usage Policy is to ensure that Adroit Soft India Pvt Ltd. employees are properly trained on appropriate procedures surrounding safe and legal use of company-owned software. Furthermore, this policy is intended to discourage inadvertent (or deliberate) violations of the terms of our organization's software license agreements and applicable laws when installing and/or using software on computers owned by Adroit Soft India Pvt Ltd. or private computers used to perform work related to Adroit Soft India Pvt Ltd...

Background

Adroit Soft India Pvt Ltd. purchases and licenses software from a variety of sources. Any duplication of software except as permitted by related license agreements is a violation of law and is therefore prohibited. Installing unauthorized software on a computer system, workstation, or network server within Adroit Soft India Pvt Ltd. can lead to potential system failures, system degradation or viruses. Unauthorized installations also place Adroit Soft India Pvt Ltd. and its employees at risk for civil and criminal action, which can result in punitive measures imposed on all involved parties.

Adroit Soft India Pvt Ltd. employees who use computer systems for work-related purposes must therefore agree to the following conditions for the use of software:

1. To purchase, install, and/or use only software that has been authorized for use on **Adroit Soft India Pvt Ltd.** computers.

2. To obtain proper documentation for all work-related software purchases.
3. To abide by the terms of all license agreements as they pertain to the use of software on **Adroit Soft India Pvt Ltd.** issued computers, as well as on “at home” or personal computer systems used for **Adroit Soft India Pvt Ltd.** related work.
4. Not to reproduce or duplicate software, in any way, except as provided by the license agreement between **Adroit Soft India Pvt Ltd.** and the software manufacturer.

SOFTWARE USAGE POLICY

Authorized Software

Only software authorized by **Adroit Soft India Pvt Ltd.** may be purchased, installed, or used on **Adroit Soft India Pvt Ltd.** issued computers. Personal software, or software that an employee has acquired for non-business purposes, may not be installed on **Adroit Soft India Pvt Ltd.**-issued computers. The only software permitted for installation on **Adroit Soft India Pvt Ltd.** computers is authorized software for which **Adroit Soft India Pvt Ltd.** has been granted a license.

Software Purchases

Only software authorized may be purchased by **Adroit Soft India Pvt Ltd.** employees. If employee wish to purchase an authorized application, the following procedures must be adhered to:

1. A copy of the software license must be provided to Admin Department for completion of registration and inventory requirements.
2. Licenses must be registered in the name of **Adroit Soft India Pvt Ltd.** and not in the name of an individual end-user.

* Note: If employee wish to purchase software that is not authorized, employee must fill out a software request form and submit it to Admin Dept. If approved by Admin Dept., the software will subsequently be authorized.

Duplication of Licenses

Software shall not be duplicated, reproduced, or installed on more than one machine without prior written authorization by Adroit Soft India Pvt Ltd.

If a software license states it is eligible and approved for home use**, the following conditions must be adhered to:

1. Use of the software is limited to Adroit Soft India Pvt Ltd.business.
2. The software must be removed from the computer if the individual is no longer employed by Adroit Soft India Pvt Ltd..

* Most software is licensed for use on one computer at a time with a provision for making a single backup copy of the software, but in order to protect individual employees and **Adroit Soft India Pvt Ltd.**, written consent to do so must be obtained by Admin Dept.

** Most software licensed to **Adroit Soft India Pvt Ltd.** cannot be run on home and work computers simultaneously. Some software vendors, however, permit employees, who are licensed to use the product at on work-issued computers and on a “home” computer under certain limited conditions. **Adroit Soft India Pvt Ltd.** has no specific policies prohibiting such use, assuming it is permitted under the terms of the license agreement.

Retirement or Transfer of Licenses

The following rules apply when a license or licenses are replaced by newer versions or are being transferred from one user to another:

1. Licenses may not be uninstalled from one user's machine and re-installed on another user's machine without written permission from Admin Dept.
2. All software and documentation for releases or versions that have been replaced by newer versions are to be returned promptly to Admin Dept.
3. All software and documentation for those products no longer required should be returned promptly to Admin Dept. and the software must be uninstalled promptly from the computer.

* In most cases, software licenses are *not* transferable without prior authorization from the vendor. This is especially important as it relates to the disposition of previous releases and the disposition of software licenses that have been upgraded. For example, it is almost always a violation of the license agreement to give anyone an older version of software after receiving an upgrade. Even if a new license (not an upgrade) has been obtained, it may be *still* be a violation of the license agreement to give the old copy to another person. Under some conditions, **Adroit Soft India Pvt Ltd.** may have rights to transfer software from one user to another. Admin Dept. will review license agreements and limitations for each software product, and if appropriate, authorize acceptable transfers of licenses.

Computer Reassignment

The following rules apply when a computer is being transferred from one user to another:

1. The computer reassignment must be authorized by the Admin Dept.

2. The intention to transfer the computer must be reported to Admin Dept. at least 72 hours in advance to allow for proper documentation.
3. If, after the transfer, both users are using the software, an additional license must be obtained according to the guidelines specified above.

MONITORING

To ensure adherence to the software usage policy and related laws and statutes, **Adroit Soft India Pvt Ltd.** reserves the right to monitor software installations and usage of all computers owned by **Adroit Soft India Pvt Ltd.**, as well as any privately-owned computers when used to conduct **Adroit Soft India Pvt Ltd.**-related business.

FAILURE TO COMPLY

There are no exceptions to this policy. Any employee found violating this Software Usage policy in any manner is subject to disciplinary action including possible termination of employment, and/or legal action.



R. Deepa
Chief Operating Officer,
Adroit Soft India Pvt Ltd.





srivenkateshwaraa
Medical College Hospital and Research Centre
CREATING HEALTHIER SOCIETY
Ariyur, Puducherry 605 102.



Department of Information Technology | E-Mail: infotech@srivenkateshwaraa.edu.in

SRI VENKATESHWARAA MEDICAL COLLEGE HOSPITAL AND RESEARCH CENTRE

Koha Policy

Koha Library Software

The world's first free and open source library system

Koha is a fully featured, scalable library management system. Development is sponsored by libraries of varying types and sizes, volunteers, and support companies worldwide.

Policy

We are pretty easy going around here, but we do have a few rules. All policies have been adopted by the community during IRC meetings or meetings of the Koha HLT Subcommittee.

Comments Policy

Comments on this site are moderated (damn spammers) but most comments will be approved once a moderator reviews them. Abusive (technically or expressively), off-topic, illegal, hate-inciting or swears comments may and probably will be deleted.

Comments are closed after 30 days on all news items. Information pages do not allow comments: please post general questions to our mailing lists or web forums. Moderators may expire old comments after a reasonable time.

If you disagree with a moderator's decision, please appeal during one of the chat (IRC) meetings. They are announced on the forums from time to time or you can ask in the chat session for the time of the next meeting.

TRADEMARK USAGE POLICY

On the 18th January 2012, following consultation with the Koha Subcommittee, Te Horowhenua Library Trust, trading as Horowhenua Library Trust, adopted the following Koha Trademark Usage Policy:

The Horowhenua Library Trust has been elected by the worldwide online Koha user community to be the custodian of Koha intellectual property including the KOHA name and associated logos in any form, font or stylization, and whether alone or in combination with other words or marks, including

We at the Horowhenua Library Trust love it when people talk about Koha, build businesses around Koha and produce products that make life better for Koha users and developers. We do, however, have a trademark, which we are obliged to protect. The trademark gives us the exclusive right to use the term to promote websites, services, businesses and products, but is also important to learn about trademarks laws and resources like a Trademark Lawyer Toronto is also really helpful with this. Although those rights are exclusively ours, we are happy to give people permission to use the term under most circumstances.

The following is a general policy that tells you when you can lawfully refer to the KOHA name and associated logos without need of any specific permission from the Horowhenua Library Trust:

First, you must make clear that you are not Horowhenua Library Trust and that you do not represent [Horowhenua Library Trust] or the Koha user community. A simple disclaimer on your home page is an excellent way of doing that.

Second, you may use the KOHA name and logo only in descriptions of your website, product, business or service to provide accurate information to the public about yourself or your website, product, business or service.

If you would like to use the KOHA name or logo for any other use, please contact us and we'll discuss a way to make that happen. We don't have strong objections to people using the name for their websites and businesses, but we do need the chance to review such use.

This trade mark usage policy is intended to be legally binding.

Generally, we will approve your use if you agree to a few things, mainly: (1) our rights to the KOHA trademark are valid and superior to yours and (2) you'll take appropriate steps to make sure people don't confuse you with us or your website, product, business or service with ours. In other words, a short conversation (usually done via email) should clear everything up in short order. If you currently have a website that is using the KOHA name and you have not gotten permission from us, don't panic. Let us know, and we'll work it out, as described above.

KOHA COMMUNITY CODE OF CONDUCT

All delegates, speakers, sponsors and volunteers at any Koha event are required to agree with the following code of conduct. Organizers will enforce this code throughout the event.

The Quick Version

Koha event organizers are dedicated to providing a harassment-free experience for everyone, regardless of gender, gender identity, sexual orientation, disability, physical appearance, body size, race, or religion. We do not tolerate harassment of event participants in any form. Sexual language and imagery is not appropriate for any event venue, including talks. Event participants violating these rules may be sanctioned or expelled from the event without a refund at the discretion of the event organizers.

Harassment includes, but is not limited to:

- Violent threats, intimidation or personal insults directed against another person
- Verbal, graphic or written comments related to gender, gender identity, sexual orientation, disability, physical appearance, body size, race or religion
- Posting sexually explicit or violent material
- Stalking or following, including harassing photography or recording
- Sustained disruption of talks or other presentations
- Inappropriate physical contact or sexual attention
- Posting (or threatening to post) other people's personally identifying information
- Advocating for, or encouraging, any of the above behavior
- Repeated harassment of others. In general, if someone asks you to stop, then stop

The Less Quick Version

Participants asked to stop any harassing behavior are expected to comply immediately. Sponsors are also subject to the anti-harassment policy. In particular, sponsors should not use sexualized images, activities, or other material. Booth staff (including volunteers) should not use sexualized clothing/uniforms/costumes, or otherwise create a sexualized environment.

If a participant engages in harassing behavior, event organizers retain the right to take any actions to keep the event a welcoming environment for all participants. Event organizers may take action to redress anything designed to, or with the clear impact of, disrupting the event or making the environment hostile for any participants.

If you are being harassed, notice that someone else is being harassed, or have any other concerns, please contact a member of event staff immediately. Event staff can be identified by a clearly marked “STAFF” badge, button or shirt.

Event staff will be happy to help participants contact hotel/venue security or local law enforcement, provide escorts, or otherwise assist those experiencing harassment to feel safe for the duration of the event. We value your attendance.

We expect participants to follow these rules at all event venues and event-related social activities. We think people should follow these rules outside event activities too!

This code of conduct is borrowed, slightly modified, from the folks at Evergreen who borrowed it from the folks at GopherCon, who borrowed it from JSConf, with permission. A section is adapted from the Open Stack Summit Code of Conduct.



sri venkateshwaraa
Medical College Hospital and Research Centre

CREATING HEALTHIER SOCIETY

Ariyur, Puducherry 605 102.



Department of Information Technology | E-Mail: infotech@srivenkateshwaraa.edu.in

SRI VENKATESHWARAA MEDICAL COLLEGE HOSPITAL AND RESEARCH CENTRE

Policy Documents for Moodle:

Moodle Policies:

The policies tool provides a new user sign-on process, with ability to define multiple policies (site, privacy, third party), track user consents, and manage updates and versioning of the policies.

The policies tool forms part of Moodle's privacy feature set assisting sites to become GDPR compliant.

Site policy handler:

The Site policy handler in Site administration / Users / Privacy and policy / Policy settings determines how policies and user consents are managed. The default (core) handler enables a site policy URL and a site policy URL for guests to be specified. The policies handler enables site, privacy and other policies to be set. It also enables user consents to be viewed and, if necessary, consent on behalf of minors to be given.

Default (core) handler:

When the site policy handler is set to 'Default (core)', a site policy may be set by entering the URL in 'Policy settings'. The URL can point to any type of file anywhere online that can be accessed without a log in to your Moodle site.

- The site policy will be displayed in a frame. You can view it via the URL *yourmoodlesite.org/user/policy.php*.
- If Email-based self-registration is enabled on the site, a link to the site policy is displayed on the signup page.
- When a site policy URL is set, all users will be required to agree to it when they next log in before accessing the rest of the site.
- A site policy for guests may also be enabled. Guest users will need to agree to it before accessing a course with Guest access enabled.
- It is not recommended that a page resource is used as a site policy, since the site header will be repeated in the frame (see MDL-30486).
- It is recommended that the site policy is on the same domain as Moodle to avoid the problem of Internet Explorer users seeing a blank screen when the site policy is on a different domain.
- Policies (tool policy) handler

When the site policy handler is set to 'Policies (tool policy)', two new pages appear in 'Privacy and policies' - 'Manage policies' and 'User agreements'. The remainder of this page describes the policies tool. Note that when 'Policies (tool policy)' is set as the site policy handler, the settings 'Site policy' and 'Site policy for guests' are ignored.

Adding and managing policies:

An admin or any user with the Manage policies capability (by default manager) can access the page 'Manage policies' in the Site administration and:

- Add a new site / privacy / third parties / other policy for all users, authenticated users or guests
- Change the active / inactive status of each policy
- View the number and percentage of users who have agreed to each policy
- Edit a policy and specify whether it is a minor change (not requiring users to reconfirm their consent) or not
- View the current version of each policy and also previous versions
- Change the order in which policies are shown to users

To add a new policy:

1. Go to 'Manage policies' in the Site administration.
2. Click the button 'New policy'
3. Complete the form and save changes.

Note that once created, a policy can be edited, or set to inactive, but if users have agreed to it, it can't be deleted.

The policy type (site / privacy / third parties) is only displayed at the 'Policies' page linked on the footer and the behavior is the same for all the policy types.

Giving consent to policies:

All users (with the exception of admins) will be required to give their consent to all policies defined either for “Authenticated users” or for “All users” before proceeding further on the site.

If a new policy is added, all users will be required to give their consent when they next log in. Similarly, if an existing policy is edited and is not marked as a minor change, all users will be required to give their consent when they next log in.

If Email-based self-registration is enabled on the site, new users will be required to give their consent to all policies before proceeding to the sign-up form. If digital age of consent verification is enabled in 'Privacy settings' in the Site administration, when a new user clicks the 'Create new account' button, they will be prompted to enter their age and country. If the user's age is lower than the age of consent for their country, they will see a message prompting them to ask their parent/guardian to contact the support contact (as specified in 'Support contact' in the Site administration).

Policies for guests:

If a user browses to the site or logs in as a guest, a modal window will be shown at the bottom of the user's browser window with links to all policies defined either for guests or for all users.

Minors:

Users who are younger than the age of digital consent, called 'minors', may be prevented from giving their consent by prohibiting the capability Agree to policies. They will then be prevented from proceeding further on the site until someone can give consent on their behalf.

Sites with minors as the majority of users:

To prohibit users from agreeing to policies because they are a minor:

1. Go to 'Define roles' in the Site administration.
2. Edit the role of authenticated user and set Agree to policies to prohibit.
3. Save changes.

To enable teachers and other users who are not minors to agree to policies:

1. Go to 'Define roles' in the Site administration.
2. Click the button 'Add a new role'.
3. Give the role a name such as 'Able to give consent', short name and description.
4. For context types where this role may be assigned, tick system.
5. Enter policy in the filter box, then allow the capability Agree to policies.
6. Click the button 'Create this role'.
7. Go to 'Assign system roles' in the Site administration.
8. Choose the 'Able to give consent' role to assign.
9. Select teachers and other users in the Potential users list, and use the left-facing arrow button to add them to the Existing users list.

Sites with only a few minors:

To prohibit users from agreeing to policies because they are a minor:

1. Go to 'Define roles' in the Site administration.
2. Click the button 'Add a new role'.
3. Give the role a name such as 'Digital minor', short name and description.
4. For context types where this role may be assigned, tick system.
5. Enter policy in the filter box, then prohibit the capability Agree to policies.
6. Click the button 'Create this role'.
7. Go to 'Assign system roles' in the Site administration.
8. Choose the 'Digital minor' role to assign.
9. Select minors in the Potential users list, and use the left-facing arrow button to add them to the Existing users list.

User agreements:

An admin or any user with the View user agreements reports capability (by default manager) can access the page 'User agreements' in the Site administration and:

- View user consents
- Filter by policy, permission, status or role
- Give consent on behalf of minors
- Download table data

User agreements for a particular policy may also be viewed via the 'Manage policies' page by clicking the link in the Agreements column.

Giving consent on behalf of other users:

An admin or any user with the capability Agree to the policies on someone else's behalf can give consent on behalf of minors or when a written consent was obtained offline.

Users with capability Agree to the policies on someone else's behalf in the system context, such as managers, can give consent on behalf of multiple users as follows:

1. Go to 'User agreements' in the Site administration.
2. If necessary, filter by 'Permission: Cannot agree'.
3. To give consent for multiple policies, tick the box next to selected users' names then click the consent button.
4. To give consent for a single policy, click the Red Cross next to the user's name.

When giving consent on behalf of other users, there is an opportunity to add some remarks. Clicking on the link in the Overall column gives an overview with details of who gave consent and when, together with any remarks.

It's not yet possible to give consent in bulk, however a workaround would be to install and use a browser extension for checking all checkboxes on the page.

Giving consent on behalf of a child:

A parent or guardian may be allowed to give consent on behalf of their child by giving them the capability Agree to the policies on someone else's behalf in the user context. See the Parent role for details of how to create the role and assign a parent to a student. The parent or guardian will then be able to give consent as follows:

- Go to the child's profile page.
- Click the link 'Policies and agreements'.
- Click the Red Cross next to the policy name.

Capabilities:

- Agree to policies - allowed for authenticated user role
- Manage policies - allowed for default role of manager only
- View user agreements reports - allowed for default role of manager only
- Agree to policies on someone else's behalf - allowed for default role of manager only

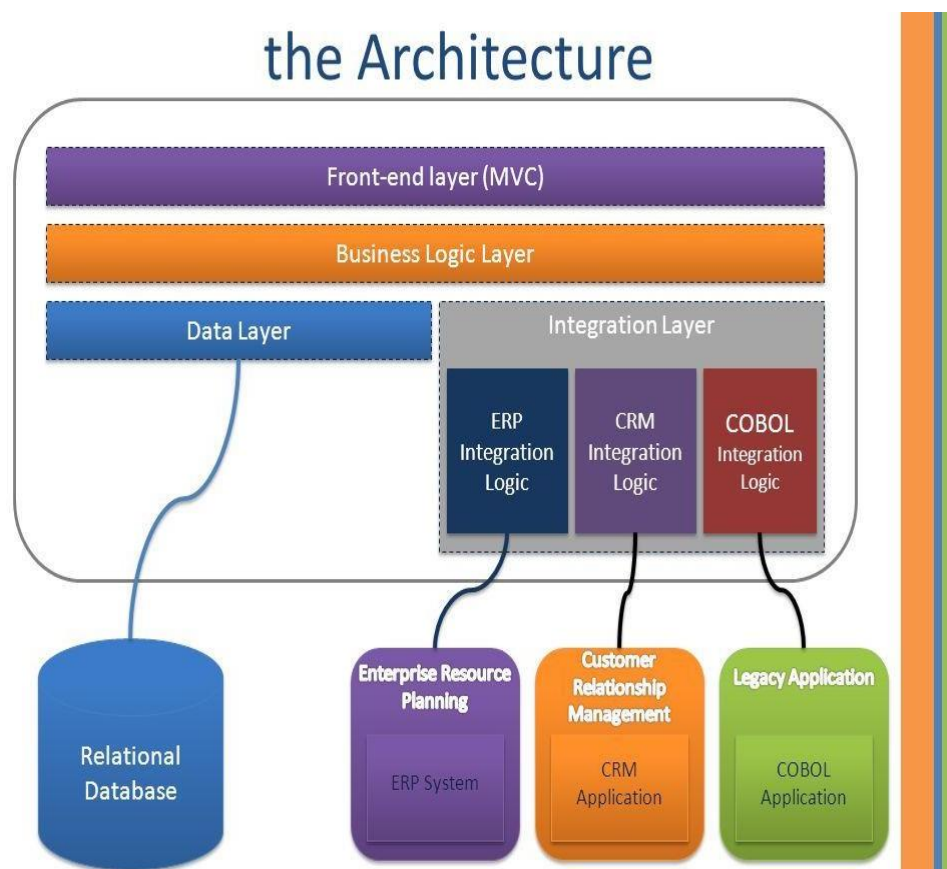


SRI VENKATESHWARAA MEDICAL COLLEGE HOSPITAL AND RESEARCH CENTRE

TALLY.ERP 9 ARCHITECTURE

3 LAYERS OF TALLY.ERP 9 ARCHITECTURE

- The Application/Tally.ERP 9 Layer
- The TDL Language and Interpreter Layer
- The Platform Layer/Engine



The Application Layer:

All the user interactions take place at the Application or the Tally layer. It is through this interface that the user gets access to all the product functionalities.

Tally Definition Language:

Tally Definition Language (TDL) provides capabilities for Rapid Development, Rendering, Data Management and Integration. The entire user interface is built using TDL.

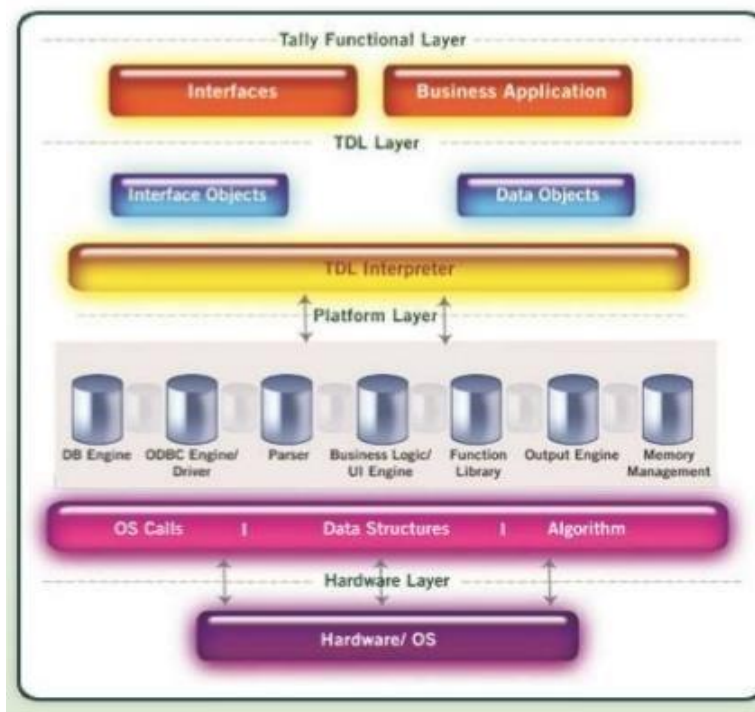
TDL is an Action driven language based on definitions. It comprises of the User Interface and Info/Data objects. User Interface Objects mainly determine the behavior of the product in terms of user experience. Info/Data objects are mainly used for data persistence in the Tally Database.

Platform Layer:

The capabilities which TDL offers are due to the capabilities provided by the platform layer. This is the lower most layers which interact with the OS and the file system. The various components of the platform layer are:

- Database Engine
- ODBC Engine/Driver
- Parser
- Business Logic
- Function Library
- User Interface and Output Engine
- Memory Management

All the retrieval and manipulation requests to the database by the application program are handled by the Database Engine. This is a true OODBMS. It is possible to store data as objects and retrieve data as objects. Stored as a block of data, this allows faster retrieval of data. Object Oriented Recursive Management System follows the concept of Flexi-Length Record, Flexi-Field, and Self-Indexed weighted file structure for an extremely compact and fast database. Fault tolerance is built in and along with transaction support (using roll forward capability); this provides an extremely robust system to withstand several system failures.



The File System consists of Data files (Master, Transaction, Link Masters), MessageFiles (for transaction management) and State Files (for concurrency and exclusivity control).

To

The Librarian
SVMCH
Pondicherry

ProQuest Policy Document

Sir,

ProQuest is committed to empowering researchers and librarians around the world. The company's portfolio of assets -- including content, technologies and deep expertise -- drives better research outcomes for users and greater efficiency for the libraries and organizations that serve them.

ProQuest is a key partner for content holders of all types, preserving and enabling access to their rich and varied information. Those partnerships have built a growing content collection that now encompasses 90,000 authoritative sources, 6 billion digital pages and spans six centuries. It includes the world's largest collection of dissertations and theses; 20 million pages and three centuries of global, national, regional and specialty newspapers; more than 450,000 ebooks; rich aggregated collections of the world's most important scholarly journals and periodicals; and unique vaults of digitized historical collections from great libraries and museums, as well as organizations as varied as the Royal Archives, the Associated Press and the National Association for the Advancement of Colored People.

Today's libraries have countless challenges to manage. Supporting too many platforms shouldn't be one of them. That's why ProQuest's comprehensive databases are some of the world's most-used in libraries across the globe. ProQuest works with thousands of publishers to acquire and curate content through a single point of access: the newly enhanced and user-friendly ProQuest platform.

ProQuest databases deliver a variety of content, serve a wide range of users, support all forms of teaching and learning, and help libraries meet their budget goals.

Achieve better research, teaching and learning outcomes

In one easy-to-use interface, get news, dissertations, ebooks, video and journals from renowned publishers – including Wiley, Springer Nature, the Lancet, The New York Times, PBS, CNN and many more.

More details: <https://about.proquest.com/globalassets/proquest/files/pdf-files/infographic-pqoneacademic.pdf>

Get sought-after content in a range of disciplines

From the humanities to STEM and everything in between, ProQuest's comprehensive databases cover a myriad of topics enabling deep subject-specific research and study.

More details: <https://about.proquest.com/globalassets/proquest/files/pdf-files/whitepaper-variedcontent.pdf>

Discoverable from a single entry point

Users can begin their database search from the open web by visiting www.proquest.com. Through their search results, they'll be delivered straight to the resources their library subscribes to.

More details: <https://about.proquest.com/en/news/2020/ProQuest-Streamlines-Discoverability-of-Subscription-and-Open-Access/>

Secure/Remote Access. All access and use of the Service must be made via a secure network and secure authentication methods. Use of the Service by remote access is allowed unless otherwise stated on the Order Form. Customer will strictly limit any remote access to its Authorized Users through the use of secure methods of user verification. Customer will promptly notify ProQuest if Customer believes security has been compromised. Posting or sharing of passwords, or otherwise enabling access for the benefit of non-subscribing institutions or users, is strictly prohibited.

Supplemental Terms. Some content included in the Service has terms of use applicable solely to such content. Content-specific terms are clearly displayed with the associated content or embedded in the systems and technologies incorporated into the Service. Where third-party databases or content are subject to supplemental terms, such terms shall be clearly referenced on the Order Form. Such supplemental terms shall not materially alter use of the Service.

Term. Customer's access to a particular Service shall continue for the period on the Order Form, plus any agreed renewal period(s). This Agreement shall continue in force for so long as Customer subscribes to at least one Service. Thereafter, the following survive: Sections 8-10 and 12-15, and any perpetual archive licenses ("PAL") (subject to all relevant use restrictions and security requirements).

Service Level. If the Service or content are hosted by ProQuest, ProQuest will use commercially reasonable efforts to provide access to the Service on a continuous 24/7 basis (except for regularly scheduled maintenance) and free from viruses or other harmful software. ProQuest shall not be liable for any failure or delay or interruption in the Service or failure of any equipment or telecommunications resulting from any cause beyond ProQuest's reasonable control. Customer is responsible for providing all required information for account set up and activation, and for its own telecommunications connections and related third-party charges.


DIRECTOR
Sri Venkateshwaraa Medical College
Hospital & Research Centre
Ariyur, Puducherry - 605 102

ii. **Scholarly Sharing.** Customer and its Authorized Users may provide to a third party colleague minimal, insubstantial amounts of materials retrieved from the Service for personal use or scholarly, educational research use in hard copy or electronically, provided that in no case is any such sharing done in a manner or magnitude as to act as a replacement for the recipient's or recipient educational institution's own subscription to either the Service or the purchase of the underlying work.

All Streaming Video and Audio Products. Audio and Video files are delivered to Customer and its Authorized Users via streaming service over the Internet. Customer and its Authorized Users shall not download or otherwise copy the streaming videos or audio contained in the Service. In the case of content that can potentially be publicly performed, Customer must secure permission from ProQuest's Licensor and/or the copyright holder for any public performance other than reasonable classroom and educational uses.

MARC Records. MARC records may be placed in Customer's online public access catalog (OPAC) or shared online catalog (e.g., WorldCat) unless otherwise specified on the Order Form with respect to a particular Service.

Scholar/Researcher Profiles. The data contained within scholar profiles are for use in facilitating research and collaboration amongst colleagues. Neither Customer nor its Authorized Users may export or otherwise exploit the scholar profiles for mass mailings or similar marketing purposes.

Analytics. Some Services contain library collection analysis capabilities related to library holdings, or functionality that allows Authorized Users to create reports, lists, or alerts. Customer and Authorized Users may create, download, store and retain any such analytics or lists delivered by the Service. ProQuest may use library holdings and other information in the Service for comparison and metrics purposes and in order to better understand the customers' needs.

Restrictions. Except as expressly permitted above, Customer and its Authorized Users shall not:

- a) Translate, reverse engineer, disassemble, decompile, discover, or modify ProQuest's software;
- b) Remove any copyright and other proprietary notices placed upon the Service or any materials retrieved from the Service by ProQuest or its licensors;
- c) Circumvent any use limitation or protection device contained in or placed upon the Service or any materials retrieved from the Service;
- d) Perform penetration tests or use the Service to execute denial of service attacks;
- e) Perform automated searches against ProQuest's systems (except for non-burdensome federated search services), including automated "bots," link checkers or other scripts;
- f) Provide access to or use of the Services by or for the benefit of any unauthorized school, library, organization, or user;
- g) Publish, broadcast, sell, use or provide access to the Service or any materials retrieved from the Service in any manner that will infringe the copyright or other proprietary rights of ProQuest or its licensors;
- h) Use the Service to create products or perform services which compete or interfere with those of ProQuest or its licensors;
- i) Text mine, data mine or harvest metadata from the Service;
- j) Communicate or redistribute materials retrieved from the Service; or
- k) Download all or parts of the Service in a systematic or regular manner or so as to create a collection of materials comprising all or a material subset of the Service, in any form.
- l) Store any information on the Service that violates applicable law or the rights of any third party.

1.16
DIRECTOR
Sri Venkateshwara Medical College
Hospital & Research Centre
Ariyur, Puducherry - 605 102