SERVICE LEVEL AGREEMENT

For,
Project: **Asset and Faculty Management System**
Organization: **Central Academy for State Forest Service, Coimbatore**

[Dated on 09th March 2025]

The Service Level Agreement (SLA) for the Asset and Faculty Management System (AFMS) is a comprehensive document that outlines the agreed-upon performance, availability, and support standards for the system. This SLA ensures that all stakeholders—administrative staff, asset handlers, faculty, and management—are aware of the system's operational parameters, data management policies, and versioning requirements.

The SLA is designed to align with the technological stack used in AFMS, including the operating system (OS), database (DB), frontend and backend versions, browser compatibility, and service pack requirements. It also specifies the responsibilities of both the service provider and the users, ensuring transparency, accountability, and high availability of the system.

Table of Contents

System Overview

The Asset and Faculty Management System (AFMS) is a centralized, web-based platform designed to streamline the process of purchasing, issuing, returning, servicing, and disposing of assets, along with structured workflows for faculty verification. Built on the MERN stack (MongoDB, Express.js, React.js, Node.js), the system ensures a structured workflow with hierarchical approvals, automated notifications, real-time tracking, and data analytics for improved decision-making.

Features of the System

- A single portal for asset management and faculty processing.
- Supports permanent and consumable assets, each with unique workflows.
- Hierarchical approval workflow for both asset and faculty processes.
- Unique ID generation for permanent assets with detailed metadata.
- Condition tracking, AMC, warranty, and disposal documentation.
- Real-time email alerts at key stages (e.g., purchase, approval, service).
- Faculty entry with role-based verification: Entry Staff → Superintendent → Head → Principal.
- Principal can rate faculty conduct with remarks.
- Role-Based Access Control (RBAC) with JWT authentication.
- Encrypted communications via HTTPS; AES-256 encryption for data at rest.
- Automated backups: weekly for active data, quarterly for archived records.
- Responsive design compatible with desktop, tablet, and mobile devices.
- Reports available in PDF and CSV formats with filters by ID, status, and date.

Technical Specifications

Category	Specification	Details / Notes
Operating System (OS)	Server OS	Windows Server 2022 Standard Edition
	Client OS	Windows 10 Pro (21H2), macOS Ventura (13.0)
Database (DB)	Database Engine	MongoDB 6.0.5
	Data Encryption	AES-256 encryption for data at rest
	Backup Strategy	Weekly for active; Quarterly for archived faculty/asset data
Frontend Versions	Framework	React.js (v18.2.0)
	State Management	Redux Toolkit (v1.9.5)
Backend Versions	Framework	Node.js (v18.17.1)
	Web Framework	Express.js (v4.18.2)
	Middleware	PM2 (v5.3.0) for process management and restarts
Browser Compatibility	Supported Browsers	Chrome, Firefox, Edge, Safari (latest versions)
	Responsive Design	Fully supports desktop, tablet, and mobile
Service Packs & Updates	Update Frequency	Quarterly security patches; Monthly feature/bug fix releases
	Rollback Procedures	Git-based rollback & backup-based restoration
	Deployment Automation	GitHub Actions (CI/CD) with zero-downtime deployment
Security & Compliance	Authentication	JWT-based authentication with Role-Based Access Control (RBAC)
	Encryption	TLS 1.3 for data in transit, AES-256 for data at rest
Hardware Requirements	Server Configuration	i5 12th Gen+, 16GB RAM (32GB recommended), 512GB SSD
	Network Requirements	≥10 Mbps; Firewall restricted to essential ports (HTTPS, API)

Category	Specification	Details / Notes
	Reverse Proxy	NGINX (v1.24.0) for HTTPS enforcement and request routing

Performance Metrics

Functional metrics focus on the system's ability to perform key tasks efficiently, like asset purchasing, issuing, return logging, faculty approval flows, and reporting. These metrics ensure the system meets user expectations and institutional SLAs.

Functional Metrics

Metric	Description	Target Value
Asset Purchase Entry Time	Time taken to submit asset purchase details after all fields are filled	≤ 5 seconds
Asset Issue Time	Time taken to issue an asset to a location	≤ 10 seconds
Faculty Entry Submission Time	Time to submit new faculty details	≤ 5 seconds
Asset Return Logging Time	Time to log return of an asset (good or to-be-serviced)	≤ 7 seconds
Approval Propagation Time	Time from submission to final approval (asset/faculty)	≤ 30 minutes (real-time ops)
Report Generation Time	Time taken to generate downloadable reports (PDF/CSV)	≤ 10 seconds
Asset/Faculty Filter Efficiency	Time to fetch filtered search results	≤ 3 seconds
Faculty Conduct Rating Update	Time to update and reflect faculty conduct score	≤ 1 minute

---

Non-Functional Metrics

Metric	Description	Target Value
System Uptime	Percentage of time the system remains available throughout the year	≥ 99% annually

Metric	Description	Target Value
Response Time for Key Operations	Time for system to respond to user actions (clicks, submissions, etc.)	≤ 3 seconds
Maximum Concurrent Users	Number of users supported simultaneously without degradation	≥ 100 users
Data Transmission Security	Ensures HTTPS + JWT-based data transmission is secure	100% encrypted
Storage Utilization Threshold	Alert system when approaching storage cap	≤ 90%
Backup Frequency and Retention	Weekly (active), Quarterly (resolved/archive); backup retention policy	4 weeks / 2 years
RBAC Compliance	Percentage of unauthorized access attempts blocked	100%

SLAs for Key Stakeholders

Stakeholder	Responsibility
Asset Entry Staff	Enter asset purchase details, issue assets, log returns, update servicing/disposal.
Asset Manager	Review and approve asset operations (purchase, issue, return, service, disposal).
Faculty Entry Staff	Enter internal/external/contract faculty details for verification.
Superintendent	Verify submitted faculty data and either approve or reject with remarks.
Head of the Office	Approve verified faculty entries; update faculty details if required.
Principal	Rate faculty conduct (0–5) with remarks, flag suspicious entries, update details.
Viewer	Has read-only access to all approved asset and faculty records.

Backup and Storage Management Metrics

Metric	Description	Target Value
Weekly Backup Execution Time	Time to complete backup for current assets and pending faculty records	≤ 30 minutes
Quarterly Backup Execution Time	Time to archive resolved/approved records and move media to external store	≤ 1 hour
Media File Cleanup After Backup	Time to delete local media after transfer to external storage	≤ 5 minutes

Metric	Description	Target Value
Backup Restoration Time	Time to recover the system using the most recent backup	≤ 30 minutes

---

Overall System Performance Summary

Aspect	Target Value
System Availability	99% uptime annually (≤ 8 hours downtime)
Response Time	≤ 3 seconds for key operations
Scalability	≥ 100 concurrent users without system degradation
Security	100% encrypted data transmission using HTTPS (TLS 1.3) and JWT
Backup and Recovery	Weekly for active records, quarterly for archived; recovery ≤ 30 min
User Satisfaction	≥ 90% based on stakeholder feedback and post-deployment surveys

---

Data Management

The Asset and Faculty Management System (AFMS) ensures high standards of data integrity, secure storage, and operational efficiency. All client-server communication is encrypted using TLS 1.3, and sensitive data at rest is secured using AES-256 encryption.

- **Role-Based Access Control (RBAC)** is enforced at all API endpoints to restrict unauthorized actions based on roles (e.g., Asset Manager, Faculty Entry Staff).
- **Audit Logs** track all actions with timestamps and user metadata, stored in MongoDB for future reference and compliance.
- **Storage Monitoring**: Alerts are triggered when usage exceeds 80%, with new entries temporarily restricted after 90%.
- **Quarterly Offloading**: Media from approved/archived records is offloaded to external storage, using `.tar.gz` compression to optimize space.
- **Backup Schedule**: Weekly backups occur every Friday at 12:00 AM, retained for 4 weeks. Quarterly backups occur on April 1, August 1, and December 1 and are preserved for 2 years.
- **Data Retrieval**: Filtering by asset ID, faculty name/email/year/domain with export options (PDF/CSV) available in ≤ 10 seconds.
- **Real-Time Dashboards**: Asset lifecycle and faculty approval metrics visualized using graphs and filters.

Compliance and Security

AFMS follows all applicable legal and regulatory standards for secure data handling, including GDPR and ISO 27001.

Role-Based Access Control (RBAC)

Role	Access Level	Permissions
Asset Entry Staff	Create, update	Manage asset purchase, issue, return, and disposal entries
Asset Manager	Approve, update	Review, approve, or reject asset actions with full visibility
Faculty Entry Staff	Create, update	Submit faculty entries and handle rejections
Superintendent	Verify	Approve or reject faculty details with remarks
Head of the Office	Approve, update	Final faculty approval and update access
Principal	Full access to faculty	View, rate, flag, and update faculty records
Viewer	Read-only	Access final reports and status of assets/faculty

Encryption Standards

Encryption Type	Description	Implementation
HTTPS / TLS 1.3	Encrypts data in transit between client and server	Enforced across all frontend and backend endpoints
AES-256	Encrypts sensitive data at rest in the database	Applied to asset and faculty collections in MongoDB
JWT Authentication	Secure access token-based authentication	Tokens validated on every protected route/action

Compliance

Regulation	Requirement	Implementation in AFMS
GDPR	User consent, data deletion, processing transparency	Consent on entry forms, deletion via admin panel
ISO 27001	Secure ISMS implementation, periodic audits	Audit logs, encryption, role validations in backend
Local Data Protection	Compliance with regional data laws	Data hosted in controlled servers with restricted access

Requirements Traceability Matrix (RTM)

Requirement ID	Description	Source	Implementation	Test Case ID	Testing Method	Status
FR-01	Role-based authentication and access control	Functional Req.	JWT + Middleware with role validation	TC-01	Automated API Testing	Passed
FR-02	Asset purchase form with metadata and attachments	Functional Req.	React form + MongoDB storage + upload service	TC-02	Manual & Automated	Passed
FR-03	Asset lifecycle tracking (store → issue → return → service)	Functional Req.	State transitions in DB, approvals in UI	TC-03	Manual Testing	Passed
FR-04	Faculty entry and approval workflow	Functional Req.	UI screens, state updates, email notifications	TC-04	Manual Testing	Passed
FR-05	Conduct rating for faculty	Functional Req.	Rating input + remarks + status tracking	TC-05	Manual Testing	Passed
NFR-01	System uptime ≥ 99%	Non-Functional Req.	Monitored via PM2, CI/CD recovery	TC-06	Monitoring Tools	Passed
NFR-02	Response time ≤ 3 seconds	Non-Functional Req.	Optimized endpoints, indexed DB queries	TC-07	ThunderClient	Passed
NFR-03	Cross-browser/device compatibility	Non-Functional Req.	Tailwind + responsive layouts	TC-08	Cross-Browser Testing	Passed

Incident Response and Recovery

Incident Type	Response Action	Recovery Time
Data Breach	Notify affected users, block access, launch forensic audit	≤ 24 hours

Incident Type	Response Action	Recovery Time
System Outage	Activate backup server, restore latest snapshot	≤ 4 hours

---

User Consent and Privacy Policy

Policy Aspect	Description	Implementation
Consent Management	Users must agree to terms before submitting entries	Consent checkbox in faculty/asset entry forms
Privacy Policy	Transparent handling of personal data	Linked in footer & notification emails
Data Deletion Requests	Faculty data can be deleted by admin upon request	Admin dashboard includes secure delete function