Software Requirements Specification (SRS)

Project: SaaS Management Platform

---

1. Introduction

1.1 Purpose

The purpose of this document is to provide a comprehensive description of the SaaS Management Platform, designed to help medium to large companies manage their third-party software subscriptions, user access, billing, and security compliance. The platform enables companies to streamline SaaS usage and optimize costs across departments.

1.2 Scope

The platform will offer:

- Centralized user and subscription management.
- Payment and billing management for different departments.
- Compliance and security features.
- Detailed insights and reporting on software usage.

1.3 Definitions, Acronyms, and Abbreviations

- **SaaS**: Software as a Service.
- **SSO**: Single Sign-On.
- **RBAC**: Role-Based Access Control.
- **API**: Application Programming Interface.

1.4 References

- User Role Management Standards.
- SaaS Management best practices.
- Industry standards for compliance (GDPR, HIPAA, etc.).

---

2. Overall Description

2.1 Product Perspective

The SaaS Management Platform will serve as a web-based application accessible by company admins, IT personnel, finance teams, and security officers. It will provide a centralized interface

for managing subscriptions, users, costs, and compliance for multiple SaaS applications in use across the organization.

2.2 Product Functions

- User management and role assignments.
- Subscription tracking and license allocation.
- Billing and payment processing.
- Security and compliance monitoring.
- Integrations with popular SaaS applications.

2.3 User Classes and Characteristics

- **Admin**: Manages the organization's account, subscriptions, and user roles.
- **IT Personnel**: Manages user access to SaaS tools and ensures compliance.
- **Finance Team**: Monitors billing, budget allocation, and cost-saving opportunities.
- **Security Officer**: Oversees security policies, access controls, and audit trails.

2.4 Operating Environment

The platform will be a cloud-hosted application accessible via modern web browsers on both desktop and mobile devices.

2.5 Assumptions and Dependencies

- Users will have internet access.
- The platform will integrate with SaaS providers' APIs where available.
- Payment processing will be managed via third-party services like Stripe or PayPal.

---

3. Functional Requirements

3.1 User Management

- **3.1.1 User Registration and Login**
  - Users can register or log in to the platform.
  - SSO integration with providers (e.g., Okta, Google Workspace).
- **3.1.2 Role-Based Access Control (RBAC)**
  - Roles: Admin, IT Personnel, Finance Team, Security Officer, Team Member.
  - Each role has specific permissions (e.g., only admins can add new SaaS subscriptions).
- **3.1.3 Team Management**
  - Admins can invite or remove team members.
  - Assign roles and manage permissions.

3.2 Subscription Management

- **3.2.1 SaaS Catalog and Subscription Tracking**
  - Ability to add SaaS tools from a predefined catalog.
  - Track subscription details like renewal dates, costs, and assigned users.
- **3.2.2 License Allocation**
  - Track the number of licenses for each SaaS tool.
  - Allocate licenses to users and reassign unused licenses.
- **3.2.3 Usage Monitoring**
  - Monitor user activity to detect unused or underutilized subscriptions.

3.3 Billing and Payment Management

- **3.3.1 Payment Processing**
  - Integrate with payment services (Stripe, PayPal) for subscription payments.
  - Generate invoices and receipts for each transaction.
- **3.3.2 Cost Allocation and Budgeting**
  - Track software costs by department or team.
  - Generate cost reports for better budgeting and financial planning.

3.4 Security and Compliance

- **3.4.1 Security Policy Enforcement**
  - Enforce password policies and 2FA for user accounts.
  - Require regular password updates for security.
- **3.4.2 Compliance Audits and Reporting**
  - Automated audit reports for SaaS usage, access, and security policies.
  - Maintain an audit trail for user activities and access history.
- **3.4.3 User Access Monitoring**
  - Track access permissions and alert admins of any unauthorized access attempts.

3.5 Insights and Reporting

- **3.5.1 Usage and Cost Analysis**
  - Detailed reports on software usage and spending.
  - Usage trends and recommendations for cost optimization.
- **3.5.2 User Activity Logs**
  - Logs of user actions for compliance and tracking purposes.
  - Filters for different time ranges, departments, or users.

3.6 Integrations

- **3.6.1 API Integrations**
  - Pre-built integrations with popular SaaS providers (e.g., Slack, Zoom, Salesforce).
  - API-based sync for user data and usage metrics.

- **3.6.2 Workflow Automations**
  - Automated workflows (e.g., assigning SaaS tools when a new employee is onboarded).

---

4. Non-Functional Requirements

4.1 Performance

- The platform should support real-time data updates for active users.
- Load times should remain under 2 seconds for typical actions on a standard internet connection.

4.2 Security

- Data encryption at rest and in transit.
- Support for 2FA and role-based access control.
- Compliance with GDPR for handling user data.

4.3 Availability

- The platform should have 99.9% uptime, with scheduled maintenance notifications.
- Cloud hosting with redundancy to prevent single points of failure.

4.4 Scalability

- Capable of scaling to support thousands of users and SaaS subscriptions.
- Modular architecture to add more features as required.

4.5 Usability

- Intuitive UI for non-technical users to manage subscriptions and view reports.
- Mobile-friendly interface for on-the-go access.

---

5. External Interface Requirements

5.1 User Interfaces

- **Dashboard**: Summarizes key metrics for admins.
- **User Management Screen**: Manage user roles, permissions, and team memberships.
- **Subscription Tracker**: Visualize SaaS tools, usage, and license allocation.
- **Reports and Insights**: Interactive reports on costs, usage, and user activity.

5.2 Hardware Interfaces

● No specific hardware requirements; operates on standard desktop and mobile devices.

5.3 Software Interfaces

● Integration with third-party SaaS providers' APIs for data sync.
● Integration with payment providers like Stripe for payment processing.

---

6. Other Requirements

6.1 Data Backup and Recovery

● Daily backups of the database and critical data.
● Disaster recovery protocols to restore services within 2 hours after an outage.

6.2 Regulatory Compliance

● The platform must adhere to GDPR for data protection.
● Support for HIPAA compliance for clients in regulated industries.