Product Requirements Document: User Management Module

1. Executive Summary

The User Management module serves as the foundational authentication and authorization system for the Photography Studio Management platform. It handles user accounts, roles, permissions, and access control across all system modules.

2. Objectives

- Provide secure user authentication and authorization
- Enable role-based access control (RBAC)
- Support user profile management
- Maintain audit trails for security compliance
- Enable scalable user onboarding and offboarding

3. User Personas

System Administrator

- Manages all user accounts
- Assigns roles and permissions
- Monitors system access and security

Studio Manager

- Creates employee accounts
- Manages team member access
- Reviews user activity logs

Employee/User

- Manages own profile
- Updates personal information
- Changes password and security settings

4. Functional Requirements

4.1 User Authentication

FR-UM-001: User Registration

- System shall allow administrators to create new user accounts
- Required fields: email, password, first name, last name, phone number
- Email must be unique across the system
- Password must meet security requirements (min 8 chars, uppercase, lowercase, number, special character)

FR-UM-002: User Login

- Users shall authenticate using email and password
- System shall implement session management with configurable timeout
- Failed login attempts shall be tracked (max 5 attempts before temporary lockout)
- Lockout duration: 15 minutes

FR-UM-003: Password Management

- Users shall be able to reset forgotten passwords via email
- Password reset links shall expire after 1 hour
- Users shall be able to change passwords from profile settings
- Old password must be verified before setting new password
- Password history: prevent reuse of last 5 passwords

FR-UM-004: Multi-Factor Authentication (MFA)

- System shall support optional MFA via email or authenticator app
- Administrators can enforce MFA for specific roles
- Users can enable/disable MFA from security settings

4.2 Role-Based Access Control

FR-UM-005: User Roles

- System shall support the following default roles:
    - Super Admin: Full system access
    - Admin: All features except system configuration
    - Manager: Team management, projects, clients
    - Photographer: Shoots, tasks, attendance
    - Editor: Task management, file access
    - Viewer: Read-only access
- Custom roles can be created by administrators

FR-UM-006: Permission Management

- Each role shall have granular permissions for modules:
    - User Management (create, read, update, delete, assign roles)
    - Attendance Management (view own, view all, approve, edit)
    - Employee Management (create, read, update, delete)
    - Client Management (create, read, update, delete)
    - Shoot Management (create, read, update, delete, assign)
    - Task Management (create, read, update, delete, assign)
- Permissions shall be configurable per role

FR-UM-007: Role Assignment

- Administrators can assign/remove roles to users
- Users can have multiple roles
- Effective permissions are union of all assigned roles
- Role changes take effect immediately

4.3 User Profile Management

FR-UM-008: Profile Information

- Users can view and edit their profile:
    - Profile photo
    - First name, last name
    - Email (requires verification if changed)
    - Phone number
    - Department
    - Job title
    - Bio/Description
    - Emergency contact information

FR-UM-009: Account Settings

- Users can configure:
    - Notification preferences (email, in-app)
    - Language preference
    - Timezone
    - Date/time format
    - Theme (light/dark mode)

FR-UM-010: Profile Privacy

- Users can control visibility of profile information
- Options: Public, Team Only, Private
- Admin can always view all profiles

4.4 User Management Operations

FR-UM-011: User Listing

- Administrators can view list of all users
- List shall display: name, email, role, status, last login
- Support filtering by: role, status, department
- Support searching by: name, email
- Support sorting by: name, email, role, created date, last login

FR-UM-012: User Creation

- Administrators can create new user accounts
- System shall send welcome email with temporary password
- User must change password on first login
- Account status defaults to "Active"

FR-UM-013: User Editing

- Administrators can edit user information
- Administrators can change user roles
- Administrators cannot edit their own role
- Changes are logged in audit trail

FR-UM-014: User Deactivation

- Administrators can deactivate user accounts
- Deactivated users cannot login
- Deactivated users retain data associations
- Deactivation can be reversed (reactivation)

FR-UM-015: User Deletion

- Super Admin can permanently delete users
- Deletion requires confirmation
- Option to reassign user's data before deletion
- Deleted users are logged in audit trail

4.5 Security Features

FR-UM-016: Session Management

- Active sessions shall timeout after configurable period (default: 8 hours)
- Users can view active sessions
- Users can remotely logout from other devices
- System tracks: device, browser, IP, login time, last activity

FR-UM-017: Audit Trail

- System shall log all user management activities:
    - User creation/modification/deletion
    - Role assignments/changes
    - Login/logout events
    - Failed login attempts
    - Password changes
    - Permission changes
- Logs include: timestamp, actor, action, target, IP address

FR-UM-018: Security Notifications

- Users receive email notifications for:
    - New login from unrecognized device
    - Password change
    - Email address change
    - Role/permission changes
    - Account deactivation

5. Non-Functional Requirements

5.1 Performance

- Login response time: < 2 seconds
- User list loading: < 3 seconds for 1000 users
- Profile updates: < 1 second
- Password reset email: delivered within 5 minutes

5.2 Security

- Passwords stored using bcrypt hashing (min 12 rounds)
- All authentication endpoints protected against brute force
- HTTPS required for all connections
- Session tokens encrypted and stored securely
- GDPR compliant data handling

5.3 Scalability

- Support up to 10,000 concurrent users
- Support up to 100,000 total user accounts
- Horizontal scaling capability

5.4 Availability

- 99.9% uptime SLA
- Graceful degradation if authentication service unavailable
- Database replication for high availability

6. User Interface Requirements

6.1 Login Page

- Clean, professional design
- Email and password fields
- "Remember me" checkbox
- "Forgot password" link
- MFA code input (if enabled)
- Error messages clearly displayed

6.2 User Management Dashboard

- User list with pagination (25/50/100 per page)
- Search and filter controls
- Bulk action capabilities
- Quick actions: edit, deactivate, view profile
- User statistics: total users, active users, by role

6.3 User Profile Page

- Tab-based interface:
    - Profile Information
    - Account Settings
    - Security Settings
    - Activity Log
- Inline editing with save/cancel
- Profile photo upload with preview
- Clear save confirmation

6.4 Role Management Interface

- List of roles with permission matrix
- Create/edit role modal
- Permission checkboxes grouped by module
- Visual indication of inherited permissions

7. API Requirements

7.1 Authentication Endpoints

POST /api/auth/login
POST /api/auth/logout
POST /api/auth/refresh-token
POST /api/auth/forgot-password
POST /api/auth/reset-password
POST /api/auth/change-password
POST /api/auth/verify-mfa

7.2 User Management Endpoints

GET /api/users
GET /api/users/:id
POST /api/users
PUT /api/users/:id
DELETE /api/users/:id
PATCH /api/users/:id/deactivate
PATCH /api/users/:id/activate
GET /api/users/:id/sessions
DELETE /api/users/:id/sessions/:sessionId

7.3 Role Management Endpoints

GET /api/roles
GET /api/roles/:id
POST /api/roles
PUT /api/roles/:id
DELETE /api/roles/:id
POST /api/users/:id/roles
DELETE /api/users/:id/roles/:roleId

8. Database Schema

Users Table

id: UUID (primary key)
email: VARCHAR(255) UNIQUE NOT NULL
password_hash: VARCHAR(255) NOT NULL
first_name: VARCHAR(100) NOT NULL
last_name: VARCHAR(100) NOT NULL
phone: VARCHAR(20)
profile_photo_url: VARCHAR(500)

department: VARCHAR(100)
job_title: VARCHAR(100)
bio: TEXT
emergency_contact: JSON
status: ENUM('active', 'inactive', 'suspended')
email_verified: BOOLEAN DEFAULT FALSE
mfa_enabled: BOOLEAN DEFAULT FALSE
mfa_secret: VARCHAR(255)
last_login: TIMESTAMP
created_at: TIMESTAMP
updated_at: TIMESTAMP
created_by: UUID (foreign key)

Roles Table

id: UUID (primary key)
name: VARCHAR(100) UNIQUE NOT NULL
description: TEXT
permissions: JSON
is_system_role: BOOLEAN DEFAULT FALSE
created_at: TIMESTAMP
updated_at: TIMESTAMP

User_Roles Table

id: UUID (primary key)
user_id: UUID (foreign key)
role_id: UUID (foreign key)
assigned_by: UUID (foreign key)
assigned_at: TIMESTAMP

Sessions Table

id: UUID (primary key)
user_id: UUID (foreign key)
token_hash: VARCHAR(255) NOT NULL
device_info: JSON
ip_address: VARCHAR(45)
last_activity: TIMESTAMP
expires_at: TIMESTAMP
created_at: TIMESTAMP

Audit_Logs Table

id: UUID (primary key)
user_id: UUID (foreign key)
action: VARCHAR(100) NOT NULL
resource_type: VARCHAR(50)
resource_id: UUID
details: JSON
ip_address: VARCHAR(45)
user_agent: TEXT
created_at: TIMESTAMP

9. Integration Points

- Email service for password resets and notifications
- SMS service for MFA (optional)
- File storage service for profile photos
- Analytics service for user activity tracking
- All other modules for permission enforcement

10. Testing Requirements

10.1 Unit Tests

- Password hashing and verification
- JWT token generation and validation
- Permission checking logic
- Input validation functions

10.2 Integration Tests

- Complete authentication flow
- Role assignment and permission verification
- Session management
- Password reset flow
- MFA enablement and verification

10.3 Security Tests

- SQL injection attempts
- XSS vulnerability testing
- CSRF protection verification

- Brute force attack resistance
- Session hijacking prevention

10.4 Load Tests

- 1000 concurrent login attempts
- 5000 simultaneous active sessions
- Permission checking under load

11. Deployment Requirements

- Environment variables for configuration
- Database migration scripts
- Seed data for default roles and admin user
- SSL certificate configuration
- Backup and recovery procedures

12. Success Metrics

- User login success rate > 99.5%
- Average login time < 2 seconds
- Zero unauthorized access incidents
- User satisfaction score > 4.5/5
- Password reset completion rate > 90%
- MFA adoption rate > 30% within 6 months

13. Future Enhancements

- Social login (Google, Microsoft)
- Biometric authentication
- Advanced password policies
- IP whitelist/blacklist
- Temporary user accounts
- User impersonation for support
- Advanced audit reporting
- API key management for integrations