MVP Business Design

1. Overview & Objectives

The application is a **multi-tenant secure file-sharing and project management platform**. Its purpose is to allow organizations to create and manage projects, securely share files and related information, and enforce access based on user security clearance.

The MVP goal is to **prove out clearance-based access logic** across organizations, teams, projects, and files while enabling secure user and file management by admins.

---

2. Core Business Concepts

2.1 Users & Accounts

- **Created only by admins** (no self-registration).
- **Attributes**:
    - Name
    - Email/Login
    - Organization ID
    - Department/Team ID (optional)
    - Role (Admin / Manager / User)
    - Security Clearance (Unclassified → Classified → Secret → Top Secret → Peer-to-Peer)

2.2 Clearance Levels

1. **Unclassified** – accessible by all users in the organization.
2. **Classified** – requires “Classified” or higher.
3. **Secret** – requires “Secret” or higher.
4. **Top Secret** – requires “Top Secret.”
5. **Peer-to-Peer (P2P)** – private, one-time transfer between users; message/file auto-deletes after view.

Inheritance Rule: Users with higher clearance inherit access to lower levels.

---

3. Organizational Structure

- **Organization** → highest-level tenant.
- **Departments/Teams** → subdivisions of an organization.
- **Projects** → belong to a team; hold files and metadata.
- **Files/Records** → belong to projects, individually clearance-tagged.
- **Project Metadata** (not clearance-bound unless explicitly tagged):
    - Budgets
    - Employees assigned
    - Deadlines

---

4. Access Control Rules

4.1 General Rules

- A user can only access content at or below their clearance level.
- Higher clearance grants implicit access to lower levels.
- **Files are individually tagged** (not inherited from project).
- A project can have files spanning multiple clearance levels.

4.2 File Creation & Assignment

- **Creators** can only assign clearance at or below their own clearance.
- **Admins** may reassign clearance:
    - To any level at or below their clearance.
    - If reassigned to a higher clearance than the creator's, the creator loses access.

4.3 Peer-to-Peer Rule

- User sends directly to another user.
- Receiver must acknowledge receipt (view/download).
- File/message auto-deletes after delivery.
- No audit log contents visible except "transfer occurred."

---

5. Roles & Permissions

Admin

- Create/manage user accounts.
- Set/adjust clearance levels of files at or below their own clearance.
- Reassign ownership/clearance of projects/files.
- View audit logs for all projects/files at or below their clearance.

Manager

- Same access as User, but can:
    - Assign team members to projects.
    - View activity reports at or below their clearance.

User

- Upload files (tagged up to their clearance level).
- Access files/projects at or below their clearance.
- Cannot modify other users' files.

---

6. MVP Features

6.1 Authentication & User Management

- Admin-created accounts with clearance level assignment.
- Login with username + password (MFA recommended).
- Role-based and clearance-based access enforced at session level.

6.2 Organization & Project Management

- Organization creation (admin only).
- Department/Team management within an org.
- Project creation (by authorized users).
- Assign users to projects.
- Metadata association: budgets, employees, deadlines.

6.3 File & Data Handling

- Upload/download any file type.
- Tag file with clearance level at upload.
- Version 1: secure storage, no in-app editing.

6.4 Peer-to-Peer (P2P) Secure Messaging

- Send file/message from one user to another.
- Auto-delete after view.
- Limited audit trail.

6.5 Audit Logging

- Record:
    - File uploads/downloads.
    - Reassignments of clearance or ownership.
    - P2P transfers (event-only, no content).
- Admins see logs at or below their clearance.

---

7. Non-Functional MVP Requirements

- **Security:**
    - Encryption at rest and in transit.
    - MFA (configurable per org).
    - Time-bound access and revocation supported.
- **Compliance (future scope):**
    - FedRAMP, ITAR, NIST-style controls.
- **Scalability:**
    - Multi-tenant (supports multiple organizations).
    - Clear separation of organizational data.
- **Auditability:**
    - Logs immutable and exportable.
    - Project/file clearance changes tracked.

---

8. Future Enhancements (Beyond MVP)

- File versioning & rollback.
- Commenting & collaboration tools.
- Rich in-app file previews.
- Automated reporting dashboards.
- More granular “need-to-know” restrictions (per-user rules).
- External sharing with time-limited links.
- More secure file storage via splitting data to different storage locations.