**Functional Requirement:**

1. Allow users to upload case-related documents (petitions, evidence, court orders).

2. Support multiple file types (PDF, DOCX, JPEG, etc.).

3. Ensure successful storage of documents with metadata (Case ID, upload date, upload-er role).

4. Automatically assign unique identifiers to each uploaded document.

5. Capture and manage metadata (e.g., file type, size, related case ID, upload er information).

6. Judges and Clerks: Full access to view and approve case documents.

7. Lawyers: Access only their case documents.

8. Public Users: Restricted access to view approved case-related public records.

9. Search by case ID, parties involved, document type, or upload date.

10. Use filters to narrow down search results (e.g., document status, upload er role).

11. Enable judges or authorized clerks to review and approve uploaded documents.

12. Notify users (lawyers) when their submitted documents are approved or rejected.

13. Allow lawyers and authorized users to submit documents electronically for review.

14. Provide a confirmation receipt for each successful submission.

15. Maintain a version history for updated documents.

16. Allow users to view or revert to previous versions if needed.

17. Allow users (especially clerks) to upload multiple documents at once.

18. Provide bulk download options for case bundles (e.g., all documents related to a specific case).

19. Maintain a log of all document activities (e.g., upload, review, approval, download).

20. Ensure logs include timestamp, user ID, and activity type.

21. Notify users of pending document approvals or new uploads relevant to their cases.

22. Alert users about nearing deadlines for document submission.

**Non-Functional Requirements:**

1. Handle uploads of large files (up to 100 MB) with minimal delay.

2. Enable document search to return results within 2 seconds, even with large data sets.

3. Accommodate increasing volumes of documents and concurrent users as the system grows.

4. Ensure smooth operation with tens of thousands of documents in the repository.

5. Encrypt documents during upload, storage, and retrieval to prevent unauthorized access.

6. Implement strict role-based access controls to ensure only authorized users can view or modify documents.

7. Ensure regular backups of the document repository to prevent data loss.

8. Provide quick recovery mechanisms in case of system failures.

9. Ensure the interface for uploading and retrieving documents is intuitive and user-friendly.

10. Offer tool-tips and error messages to guide users in case of upload or search issues.

11. Adhere to legal and regulatory standards for data protection ( GDPR, HIPAA, or country-specific regulations).

12. Ensure proper handling of sensitive and confidential documents.

13. Integrate with external systems (e.g., third-party storage solutions or court databases) for seamless data exchange.

14. Support API connections for document retrieval and updates from other systems.

15. Ensure 99.9% uptime for the document management system.

16. Provide consistent performance across all user roles and locations.

17. Support multiple languages for document metadata and user interface.

18. Provide detailed error messages for upload failures (e.g., file too large, unsupported format).

19. Implement retry mechanisms for failed uploads.

**Use Case Specification: Document Management – Upload Documen**t

**Actor:**Clerk,Lawyer,Admin

**Description/Scenario :**

1. The actor logs into the system with valid credentials.
2. The actor navigates to the "Document Management" module.
3. The actor selects the "Upload Document" option.
4. The system displays a form for uploading documents with mandatory metadata fields (Case ID, Document Type).
5. The actor fills in the required metadata and selects the file(s) to upload.
6. The system validates the file format, size, and completeness of metadata.
7. If validation passes, the document is stored in the system with a unique identifier.
8. The system updates the case record with the new document status.
9. The system sends a confirmation notification to the actor.
10. The system logs the upload activity in the audit trail.

**Exceptions:**

**Invalid File Format**: Error message for unsupported file formats.

**File Size Exceeded:** Error message for exceeding maximum file size.

**Missing Metadata:** Error message for incomplete metadata.

**Authentication Failure:** Redirect to the login page or error message for unauthorized access.

**Precondition:**

1. The actor must be logged into the system with valid credentials.
2. The actor must have appropriate upload permissions.
3. The metadata for the related case must exist in the system.
4. The system must be operational and connected to the storage server.

**Post-condition:**

1. The document is securely uploaded and indexed with a unique identifier.
2. The system updates the case record with the document status.
3. A confirmation notification is sent to the actor.
4. The document is available for search and retrieval by authorized users.
5. The upload activity is logged in the audit trail.