



**ITER-India**  
**(Institute for Plasma Research)**



<b>Title</b>	<b>Section-C: Scope of Work, Scope of Supply and Technical Specifications</b>
--------------	---

**ITER-India, Institute for Plasma Research**  
**Block A, Sangath Skyz, Bhat-Motera Road, Koteswar,**  
**Ahmedabad 380005, Gujarat, India**



## Contents

<b>1. Introduction: INDUS</b>	<b>4</b>
<b>2. Scope of the Work</b>	<b>5</b>
<b>2.1. Scope of Work for Vendor</b>	<b>5</b>
<b>2.2. Software Requirement Specifications</b>	<b>5</b>
<b>2.2.1. User Login and Logout</b>	<b>5</b>
<b>2.2.2. User Authentication</b>	<b>5</b>
<b>2.2.3. User Logout</b>	<b>5</b>
<b>2.2.4. Password Management</b>	<b>5</b>
<b>2.3. User Management</b>	<b>6</b>
<b>2.3.1. User Account Management</b>	<b>6</b>
<b>2.3.2. User Listing and Search</b>	<b>6</b>
<b>2.3.3. Group Management</b>	<b>6</b>
<b>2.3.4. User Status Management</b>	<b>6</b>
<b>2.3.5. Metadata Configuration</b>	<b>6</b>
<b>2.3.6. Super User Access</b>	<b>6</b>
<b>2.4. Notification Management</b>	<b>7</b>
<b>2.4.1. Notification Settings</b>	<b>7</b>
<b>2.5. Mail Configuration</b>	<b>7</b>
<b>2.5.1. Email Settings</b>	<b>7</b>
<b>2.6. Folder Management</b>	<b>7</b>
<b>2.6.1. Folder Structure</b>	<b>7</b>
<b>2.6.2. Update Folder</b>	<b>7</b>
<b>2.6.3. Folder Options</b>	<b>7</b>
<b>2.6.4. Folder Operations</b>	<b>7</b>
<b>2.7. Administration</b>	<b>8</b>
<b>2.7.1. User Group Management</b>	<b>8</b>
<b>2.7.2. Password Management</b>	<b>8</b>
<b>2.8. Document Management</b>	<b>8</b>
<b>2.8.1. Advanced Document Search</b>	<b>8</b>
<b>2.8.2. Documentation System</b>	<b>8</b>
<b>2.8.3. Review Management System</b>	<b>8</b>
<b>2.8.4. Approval Management</b>	<b>9</b>
<b>2.9. Scope of work for ITER-India</b>	<b>9</b>
<b>3. DMS architecture:</b>	<b>9</b>
<b>4. Selection of Technology Stack</b>	<b>11</b>
<b>5. Project Key Activities:</b>	<b>12</b>
<b>6. Guidelines for submission of project proposal</b>	<b>14</b>

<b>7. Deliverables of the project:</b>	15
<b>8. Intellectual Property Rights (IPR):</b>	15
<b>9. Functional Requirements:</b>	16
<b>10. Non-Functional Requirements:</b>	18
<b>11. Other Conditions:</b>	21

## 1. Introduction: INDUS

INDUS is a functioning Web based Documentation Management System (DMS) for ITER-India Documentation. In 2006, INDUS was designed and developed for the purposes of storing, sharing, reviewing, approving and revising documents and is an integral part of day-to-day activity of ITER-India Project. INDUS is the backbone for managing of administrative as well as technical documentation of ITER Project and having a library of over 95,000 documents along with their metadata and comments, review process, version of documents etc. The proposal is to develop new or upgrade existing DMS with enhanced features on latest stable platform. INDUS is running on RHEL 7.X, which is developed using PHP5.5, Drupal 8.x and MySQL database. INDUS is used by ITER-India employees and on-site and off-site contractors. The documents are stored on the filesystem and the reference/path/pointer including metadata are stored in the database.

Following are the features available with INDUS

- Document Storage (Centralized repository for storing documents and hierarchical folder structure for organization)
- Metadata management (metadata for folder and document e.g. author, creation date, search string, etc)
- Version control (track and manage different versions of a document)
- Document retrieval (search, metadata search including tagging)
- Access control and security (define and manage user roles and permissions, restrict access to sensitive documents)
- Workflow automation (workflow for review and approval of documents)
- Audit trailing (track and record user activities and changes to documents)
- Reporting and analytics (gain insights into document related activity)
- Notification via email

Above functionalities of INDUS collectively contribute to efficient document management, enhancing collaboration and overall productivity within the organization.

Our objective of the bid is to develop new or upgrade existing DMS to have the latest technology stack to the latest stable version compatible with the latest browsers (e.g. Microsoft Edge, Chrome, Safari, Mozilla Firefox) and also to enhance the performance/ security with additional features/ functionalities which are described later in this document.

## 2. Scope of the Work

### 2.1. Scope of Work for Vendor

- To Understand the requirement of DMS system in detail and produce SRS (System Requirement Specification) document accordingly which will be mutually agreed upon.
- Design, Develop and Test the new DMS as per the agreed SRS and agreed technology stack.
- The vendor shall deploy the new proposed DMS on ITER-India server at ITER-India premises.
- Migration of existing data on INDUS including metadata, file/ folder/ user permissions to the new DMS solution,
- The vendor is responsible for successful rolling out the newly developed DMS to the end user.
- Training for ITER-India end-user and system admin shall fall under the scope of the vendor. As part of the training the vendor shall also deliver user manual for ITER-India end-user and system admin for the newly developed DMS.
- Once the new DMS is deployed and rolled out the vendor shall be responsible for operation and maintenance of the system for period of 5 years from the date of acceptance (Date of Project sign off/ closure), the initial six months of the support period after rollout of the DMS shall be for stabilization, minor enhancements to the existing functionality may be required and bug fixing.

### 2.2. Software Requirement Specifications

#### 2.2.1. User Login and Logout

#### 2.2.2. User Authentication

- Users must be able to log in using a valid user ID and password.
- The system must validate the user ID and password against stored credentials.

#### 2.2.3. User Logout

- Users must be able to log out at any time.

#### 2.2.4. Password Management

##### 2.2.4.1. *Forget Password*

- Users must be able to reset their passwords if they forget them.
- The system must verify that the user requesting the password reset is a valid, registered user.

##### 2.2.4.2. *IT Administrator Password Management*

- IT Administrators must be able to change the passwords of users.

## 2.3. User Management

### 2.3.1. User Account Management

- IT Administrators must be able to create, update, delete, and modify user accounts.
- IT Administrators must be able to create users and assign different roles.
- IT Administrators must be able to approve new user registration applications.

### 2.3.2. User Listing and Search

- IT Administrators must be able to list users with the following details:
  1. User ID
  2. User Name
  3. Account Creation Date
  4. Email Address
  5. Actions (with proper rights read or write)
- IT Administrators must be able to search for users by User ID, Account Creation Date, Email Address, Country, or Organization.

### 2.3.3. Group Management

- IT Administrators must be able to view and manage user groups (Group Name, Group Type).
- IT Administrators must be able to add and remove users from groups.
- IT Administrators must be able to create new groups.
- IT Administrators must be able to view the groups they belong to.

### 2.3.4. User Status Management

- IT Administrators must be able to activate or deactivate user accounts.
- IT Administrators must be able to select multiple records and perform batch confirmation or rejection of registrations.

### 2.3.5. Metadata Configuration

- IT Administrators must be able to configure and reconfigure the metadata of documents or folders.

### 2.3.6. Super User Access

- IT Administrators must be able to configure and reconfigure the metadata of documents or folders.

## 2.4. Notification Management

### 2.4.1. Notification Settings

- IT Administrators must be able to change notification settings and email templates.
- IT Administrators must be able to set notifications for various events such as document uploads or folder uploads.

## 2.5. Mail Configuration

### 2.5.1. Email Settings

- IT Administrators must be able to change settings for sending notification emails.

## 2.6. Folder Management

### 2.6.1. Folder Structure

- Users must be able to view folder details including type, status, path, size, created date, responsible officer (RO) name, version, and actions.
- Users must be able to view who has read and write access to the folder.
- Users must be able to view which groups have read and write access to the folder.
- Users must be able to access a report showing the number of documents, subfolders, and other folder statistics in graphical form.

### 2.6.2. Update Folder

- Users must be able to change folder details such as name, description, owner, category, types, and group permissions.
- Users must be able to select other users as folder owners.
- Users must be able to add custom options and select multiple groups for selection.

### 2.6.3. Folder Options

- Users must be able to access multiple options for folders such as viewing in a new tab or window, copying, moving, and deleting folders.
- Users must be able to see user lists in the form of group name, group type, username, and User ID.
- Users must be able to search for folders using folder name, created date, owner user, RO, and category.
- Users must be able to create shortcuts for folders and view the folder path.
- Users must be able to create and edit their favorite bookmarks for folders.

### 2.6.4. Folder Operations

- Users must be able to create new folders by specifying folder name, description, owner, category, types, and group permissions.
- Users must be able to upload documents to folders by specifying document ID, filename, description, status, and author.

## 2.7. Administration

### 2.7.1. User Group Management

- Users must be able to create, delete, and modify user groups if they have access.
- Users must be able to view group information such as group name, date of creation, type, and actions.
- Users must be able to search groups by group name, created date, and group type.

### 2.7.2. Password Management

- Users must be able to change their old password to a new password.
- The system must provide a password reset feature with necessary security measures for users who forget their passwords.

## 2.8. Document Management

### 2.8.1. Advanced Document Search

- Users must be able to search for documents by document name, type, category, and upload type.
- Users must be able to search documents using exact and specific parameters.
- Users must be able to view document details including name, created date, and actions.

### 2.8.2. Documentation System

- Users must be able to download and copy documents to desired locations.
- Users must be able to copy and download multiple documents at once.
- Users must be able to change document metadata without changing the version before approval.

### 2.8.3. Review Management System

- Users must be able to access review statuses such as pending review, last weekend reviewed, this week review, and review search.
- Users must be forced to update the document version.
- Users must be able to review pending documents with details such as document name, upload date, owner user, review by date, version, number of reviews, and actions.
- Users must be able to download reviewed documents.
- Users must be able to request folder access via email.
- Users must be able to view document attributes such as title, file name, selected authors, co-authors, reviewers, and approvers.
- Reviewers must be able to view other reviewers' reviews and reassign review tasks.
- Users must be able to view full document information and align/sort document listings by type, date, and name.
- Reviewer should be able to reassign the review task to any other account holder.

- Users/Reviewers must be able to search reviewed documents by document name, type, category, upload dates, author, co-author, reviewer, and approver.

#### 2.8.4. Approval Management

- Users must be able to manage document approval activities such as pending for approval, last week approved, this week approved, and approval search.
- Users must be able to approve multiple documents and download approved documents.
- Users/Approvers must be able to search approved documents by name, type, category, and upload dates.
- Users must be able to add/edit reviewers and approvers without re-uploading the document.
- Users must be able to search approved documents by author, co-author, reviewer, and approver.

Overview of the software requirements for DMS are as stated above, in addition the Functional requirements and the Non-Functional requirements are stated in Section 11 and Section 12 respectively.

### 2.9. Scope of work for ITER-India

ITER-India shall give access to the existing system and demonstrate the functionality. The newly developed DMS shall be deployed at ITER-India data centre at local premises at ITER-India, Gandhinagar. The Hardware Resources required to deploy DMS onsite shall be provided by ITER-India. The Operating System license, Network security, SSL certificate shall be under the scope of ITER-India. Technical documentation of DMS (INDUS) implemented at ITER-India would be given to the vendor for reference.

## 3. DMS architecture:

DMS typically integrates several technologies that work together to provide functionalities of document storage, retrieval, version control, security, collaboration. The technologies that will be utilized for implementation of DMS solution are listed below:

- **Client-End User Interface (UI):** DMS shall be a web-based solution supporting all the latest browsers e.g. Microsoft Edge, Mozilla Firefox, Opera, Google Chrome, Safari, Chrome based browser and shall be platform independent. No additional third-party browser plugins should be required for the DMS to work through browser.
- **Web server:** Processing user requests, managing secure session, interaction with backend. No files/ folder should be accessible without secure login.

- **Application layer:** application layer is the definition and execution of business logic for the DMS. It may also include modules for workflow automation, collaboration, search for files and folders in DMS and various other feature requirements of system.
- **Database server:** Data base server would store metadata about the documents/ folders/ users, version history, access control, comments, settings and audit trail of data etc.
- **Documents storage:** In addition of the database, the actual documents should be stored on a different repository or a files storage system for security compliance.
- **Search Engine (Search and Indexing):** The search feature should include provision of search using filename, metadata, author name, date, unique alphanumeric search id that is generated when uploading a file, file status, and other criteria.
- **Security Layer (Access Control):** This would constitute enforcing security policies and access control. Only the user accounts with access to the file or folder shall be allowed to create/download/modify a file/ folder based on the user access of that account.
- **Integration Layer (API Layer):** It is preferred to use REST APIs to connect client-side and server-side.
- **Notification Service:** Sending notification to user about the relevant activities and change to the file and folder to the related user. Notification is the essential component to the workflow of the DMS. The notification system is used to send notification to the approver, reviewer, author, co-author and all users having read and write permissions of the folder.
- **Workflow Engine:** A workflow automation or workflow engine automates the workflow process.
- **Document rendering:** The documents being uploaded to the new DMS should also be converted to PDF/A format for long time archival and also for cover page generation. This feature should also be available for the existing uploaded document on the proposed DMS should have an option to download the file in pdf format also.
- **Reporting and Analytics:** The feature would enable generation of reports and analytics on document usage, user activities, dashboard and overall system performance.
- **Device Access:** The proposed DMS solution that would be accessible via web browser should have a design that is also compatible with modern portable devices e.g. smart phones, tablets and should render accordingly.

The proposed DMS solution by the vendor should include the architectural design as part of the technical bid considering that the proposed DMS shall be run on RHEL 9.x (Linux based server). The proposed DMS should be based on open source technologies, free from any proprietary

licensed/ subscription based framework/ technologies. The submission of source code for the proposed DMS solution shall fall under the scope of the vendor.

## 4. Selection of Technology Stack

The selection of technological stack is very important for the success of the proposed project and hence the bidder should choose time tested, reliable, opensource technologies. The criteria the bidder should adhere to when proposing/ selecting the technology stack for the implementation of new DMS are listed below:

- Selection of appropriate programming languages (e.g. JavaScript, Python, C# ) and the related trusted, opensource frameworks (e.g. Express.js, , AngularJS, Flask, Bootstrap, etc) having native support for the MVC design pattern and REST architecture. Use of proprietary/ subscription based frameworks is not be permitted.
- Selection of modern frontend technologies (e.g. HTML5, CSS3, JavaScript frameworks like bootstrap/ React.js etc), Ensure cross browser compatibility and responsiveness across different devices and screen sizes. Use of proprietary/ subscription based technology is not be permitted.
- For database solution, the latest stable version of opensource RDBMS like MySQL/ PostgreSQL/MariaDB/MongoDB. Use of proprietary/ subscription based databased solution is not permitted.
- Using rich APIs, third party libraries, flexible and extensible to accommodate future changes and enhancements. Use of proprietary/ subscription based APIs is not permitted.
- Usage of opensource, reliable, time tested technologies should be utilized, propriety/ subscription based licensed software is not permitted.
- Should have built-in security features and mechanisms to protect against common vulnerabilities (e.g. XSS, CSRF, SQL injection, etc).
- The technology stack should have a modular structure, constituting of plug-in support and ease of adding new features. It must be long term viable, mature enough, stable and updated frequently and releases and having presence of roadmap for future development
- The technological stack should be scalable in terms of anticipating the future load on the proposed DMS providing scalability, load balancing, etc.
- Like most of the technologies used worldwide have communities and discussion groups, there should be active and supportive communities/ discussion groups online and having

enough documentation, forums and online resources that can help troubleshoot issues and learn best practices.

- For the technologies used in implementation of DMS, there should be availability of trained resources and ease of hiring the developers with expertise in the local market.

## 5. Project Key Activities:

The project key activities of DMS project keeps track of progress, ensures accountability and provides timeline. The project key activities are as listed below:

- **Project Kick-off:** Define the scope of the project, identify the project team and assign the roles to the team.
- **Requirement Gathering and analysis:** collect, analyse and document all project requirements, technical document of present DMS at ITER-India (INDUS) would be given for reference.
- **Wireframe and prototypes:** Develop wireframe and prototype to visualise the application structure. Design user interfaces that are intuitive, responsive, and aligned with the brand identity.
- **Backend development:** Develop robust backend logics and functionalities using appropriate programming languages (e.g. Node.js, PHP, Python, etc) and modern, trusted, opensource frameworks (e.g. Express, Laravel, Django, etc)
- **Frontend development:** Development of front-end UI as per approved design using modern, stable, opensource, frontend technologies (e.g. HTML5, CSS3, JavaScript frameworks like bootstrap/ React.js, etc), Ensure cross browser compatibility and responsiveness across different devices and screen sizes, being truly platform independent, get the approval of design elements, establish frontend components and integrate it with backend.
- **API Integration:** Seamless integration of APIs with the existing system to enable efficient communication between different software components. Utilize modern, stable, and open-source technologies to ensure robust and secure data exchange. Ensure the APIs are well-documented, allowing for easy implementation and maintenance. Focus on optimizing performance, handling errors gracefully, and ensuring compatibility across various platforms and devices. Establish a thorough testing process to validate the integration, ensuring it meets the approved specifications and performs reliably under different conditions.

- **Database Implementation:** Complete the backend design; ensure data integrity, security and scalability during database design. Get the approval from ITER-India before implementation, implement database schema and relationships as per the approved design. ITER-India shall give complete access to the database tables to the vendor which would be helpful in the database implementation for the new proposed DMS solution. For database solution, the latest stable version of open-source RDBMS like MySQL/ PostgreSQL/ MariaDB etc. Use of proprietary/ subscription-based database solution is not permitted.
- **Core functionality development:** Develop the core functionalities, implement user authentication and authorisation, 2FA (two factor authentication) based on the registered email address along with captcha-based security would be mandatory.
- **Development Phase:** This can be divided into three parts, Alpha release, Beta release and Final Release. **Alpha Release:** Alpha testing is the first phase of formal testing, during which the software is tested internally using white-box technique. **Beta Release:** Beta testing is the next phase in which the software is tested by a larger group of users, testing with a limited group of users. **Final Release/ Version:** This is also known as production release, the stable release has incorporated all the required features of the system, quashing all the bugs/ inconsistencies that were encountered in alpha and beta phase of development and has passed through all stages of testing and verification.
- **Migration:** Perform the migration of data from existing DMS (INDUS) using custom-written scripts or tools.
- **Deployment:** Prepare and deploy the application on the production environment following the best industrial practices, configure servers for optimal performance and security.
- **Post-deployment support:** Monitor the performance and address any post-launch issues, bug fixing, feature request for a period of 3 Months from the date of project sign-off.
- **Documentation:** Finalise the project documentation including the technical guides/ specifications, deployment documents and user and admin manuals. Ensure that the documentations are comprehensive and up-to-date.
- **Training and support:** Conduct training sessions for end-users, administrators and support staff as needed, provide ongoing technical support and maintenance service for 6 Months post-deployment.
- **Project Closure:** Conduct project review, obtain final acceptance note/approvals and close the project.
- **Testing and Quality assurance:**

- **Conduct comprehensive testing at each stage of development to identify and address any bugs or issues. Perform following testing:**
  - **User Acceptance testing (UAT):** conduct end-user testing for usability, address any issue identified during testing
  - **Performance Testing:** Conduct performance testing to ensure that the application can handle expected loads, Optimize the performance based on test results
  - **Security Testing:** Perform security testing to identify and address the vulnerabilities, implement necessary measure
- **Operation and management:** 5 years supports from the date of acceptance. Vendor support system should include ticketing, response times (SLA), and resolution processes for effective issue resolution.

## 6. Guidelines for submission of project proposal

Expected format for the proposal shall be as follows:

- Company profile, customers and Company web site URL.
- Explain why the project is essential for your company.
- System Design Document expressing Scope of work (brief features and integration).
- Database design document.
- Proposed technology stack: Define the technical architecture and infrastructure requirements for deployment/ developments, specify the technology stack to be used for frontend, backend, database and other required components.
- Project Timeline (Schedule) with key milestones includes the major project phases (such as requirement gathering, design, development, testing and deployments).
- Proposed Methodology and Approach, describe the development methodology (Agile, Scrum) to provide high-end collaboration and efficiency of project work, overall approach to the project.
- Project team with roles and responsibilities, mode of working (onsite, offsite, mixed), ensure that the proposed team has necessary skills for the proposed technology stack.
- Describe how collaboration and communication (Communication channel and frequency) will be managed during execution of the project.
- Quality assurance and Testing pathway.
- Software Documentation and user Training plan.

- Code configuration and change management (process, tools and techniques).
- Describe any specific tools or framework to be used for testing.
- Risk analysis and challenges plan.
- Specify the meeting schedules, reporting mechanisms and escalation procedure.
- Approval Process (How approval will be sought and obtain, who will be responsible for sign off).
- Project initiation process (Kick off meeting).
- Responsibilities / Scope of the ITER-India.
- Legal and compliance (Data protection and privacy measures).
- Project Closure (Ensure a smooth transition and handover of deliverables to ITER-India).
- Any other activities/items important to accomplishing the project.

## 7. Deliverables of the project:

- **Documents:** Software Requirements Specifications (SRS), System Architectural Documentation, Detail design document(s), User manuals for End user and System Administrator, Test Reports, UAT document.
- **Project Management Documentation:** Running Document management system with its components and modules.
- **License Perpetuity:** Licenses wherever required and commitment letter for non-infringement of Trademarks and Copy Rights. No proprietary or subscription based licensed software should be used.
- **Source Code:** Source Code document as per ISO 27001.
- **Database Design Document:** Software Database Design Document covering enterprise database level design.
- **User Training:** User Training for End-User and Administrator.
- **NDA:** Signed Copies of Confidentiality and Non-Disclosure Agreement.

## 8. Intellectual Property Rights (IPR):

It is crucial to establish clear agreements regarding IP ownership, usage and ownership of source code.

- Ownership of the code: ITER-India will be the sole owner of the code developed during the project. ITER-India shall have ownership of the developed application code, would be free to deploy any number of instances, free to modify and distribute the code to any

organization. The vendor/development partner may retain the rights to reusable components or framework they developed independently.

- Licensing and Usage Rights: ITER–India can use, modify, distribute and sublicense the code without any obligation.
- Work product and deliverables: The design assets, documentation and any custom development shall be owned by ITER-India. ITER-India shall have unrestricted access to the final deliverables up on completion of the project
- Confidentiality and Non-disclosure: The vendor will ensure protection of sensitive information shared during the development process. The vendor shall not disclose any proprietary information to third parties without written consent of ITER-India.
- Open-Source Software: Clarify identify any open-source components or third-party libraries used in the project and ensure the compliance with theirs terms and conditions of licensing. No proprietary or subscription based licensed software should be used.

## 9. Functional Requirements:

DMS will allow to organise, store, track and manage documents related to a project. ITER-India already has a DMS solution called INDUS, the end-user manual and admin manual of INDUS shall be provided to the vendor as a based document for reference. Following are the features required for the proposed DMS.

- Document Storage (Centralised repository for storing documents, Hierarchical folder structures for organisation, avoid duplication of documents).
- Metadata management (define and manage metadata for documents and folders, allow search document based on metadata).
- Version Control (track and manage different version of a document, capability to revert to previous versions).
- Document Retrieval (Quick and efficient search capabilities, metadata tagging to facilitate easy retrieval).
- Implementation of full text search based on user permissions.
- In the present DMS solution, the file size is limited to 300 MB right now, it should be increased to 1 GB.
- The new implemented DMS should upload/ store files in same format as the present DMS (INDUS) at ITER-India.

- In case the user forgets password, provision should be there for resetting password with the required security measure/s.
- Provision for having additional routing during review process by the approver.
- User should be able to add/edit the set of reviewers and approver, without re-uploading the document. The proposed DMS should send emails when the document is revised/ comments are added to the document to all users who are related to the document as approver, reviewer, author, uploader.
- The user should be able to send request via email from Document Management System to the RO of the folder requesting for access to the access to folder.
- The System Administrator (sysadmin) should be able to hide/ unhide folders as per requirement.
- Reviewer should be able to reassign the review task to any other account holder.
- Access Control (Define and manage user roles and permission, restrict access to sensitive documents, ensure the security of the stored documents).
- Collaboration and Sharing (Enable multiple users to collaborate on a document simultaneously, share documents within the organisation or with external parties).
- Workflow Automation (Design and implement document review and approval workflow).
- Audit Trails (Track and record user activities and change to documents, provide and audit trail for compliance and accountability).
- Document Lifecycle Management (allow to obsolete/ delete the documents and document versions). Delete option should only be available to the system administrator. The delete option available to the user will be soft delete, the system administrator can confirm delete the file/ folder or can restore the soft deleted file/ folder
- Reporting and Analytics (Generate reports on document usage, access pattern and other relevant metrics, gain insights into document related activities).
- PDF/A conversion (Convert the document to PDF/A format for long term archival).
- Automatic generation of First Page for each document uploaded on the DMS and it should be integrated with the PDF/A version of the document uploaded.
- Watermarking and Cover page generation (Watermark the content of the document version with DRAFT/OBSOLETE/Confidential based on the lifecycle status, generate the cover page for standardisation of documents).

- Electronic Signature (Provide the possibilities for attaching Digital Signature to the uploaded for purposes of validation, the certificates/token will be provided by ITER-India) with possibility to enable or disable this feature.
- Authentication (provide local users management and password-based authentication to secure access to DMS, No password in plain text while in transit for attestation, provide captcha for login page, provide facility for password management – reset password and change password, Profile management), two factor authentication based on registered email of the account holder.
- Authorisation (Provide to create groups, manage permissions on document and folder level, allow role-based access control, provide security inheritance)
- Secure file upload (scan the uploaded file for malware and virus, only allow files with particular file type/extensions).
- Audit trail (maintain an audit trail to record activities such as document uploads, downloads, edits and approvals. This will help track the changes and accountability)
- Document Preview (Include document preview feature for common file type (PDF, image, etc.). This will allow users to quickly review content without downloading.
- Search and Filtering (Incorporate a search functionality to quickly locate specific documents. Enable filtering options based on attributes such as date, search string, category, document type etc.
- Collaboration and comment (allow users to collaborate by adding/ replying comments on document version. Email notification on comments/ reply).
- Notification (Implementation of a notification system to alert users of important events such as document updates, comments or pending approvals).
- Dashboard implementation.
- Tagging (allow additional keywords to attach to documents to enhance search capabilities, this will also include users favourite for dashboarding capabilities).
- Subscription and notification (Allow users to subscribe folder or documents to get notification on specific update events).

## 10. Non-Functional Requirements:

### Security:

- Use of HTTPS is mandatory using a standard verified SSL certificate. ITER-India shall provide the required SSL certificate.

- There should not be any service login accounts and backdoor entry methods/channels present in the application.
- Use of secure password and password policy for change of user password at regular intervals to be notified to users separately.
- Prevent uploading of executable files undesired files (Not defined as MIME type).
- Application path and Data Storage Path is to be different and also actual file path should not be disclosed.
- The flaw in the application should not lead to insertion of unwanted junk messages into the application such as scripts, SQL injection commands etc.
- Once deployed will be audited by CERT-IN panel vendors and a report to be submitted to ITER-India.
- System should be free from the brute force attack on login page. (Account lock-in from a time period after certain failed login attempts).
- Cookies if used should not contain any sensitive information.
- Application configuration information should not be visible on the web.
- Source code of the application should not be displayed on the web under any circumstance.
- System should be free from DOS attack.
- All activities should be logged, archived and should be maintain.
- The entire web application must be declared Free from vulnerabilities from OWASP top 10 vulnerabilities as safe to host application. The same must be certified by any CERT-In empanelled vendor. Any major changes to source code need re-evaluation of the entire application.
- All uploaded documents should be checked for malware and Virus check. (The system should have pluggable mechanism for anti-virus scanning of uploaded documents. Any anti-virus solution should be easily plugged into the system).
- No duplicate documents are allowed to upload in the system (checksum-based checking).
- The new web portal to be designed and developed should be compliant and adhere to the Guidelines for Indian Government Websites (GIGW).
- It would be the vendor's responsibility to get the Security Audit done for the DMS toll/ web portal from authorized and empanelled agencies (CERT-In).
- The web portal should be built so as to meet the requirements of Open Government Data and must be Open by Design; more information may be sought from the web- link <https://data.gov.in/>.

- Data transfer & All web paths are to be well written using standard techniques such as routes, xml configurations and properly documented. Any path which is NOT defined should always give a ‘Resource Not found’ (HTTP 404 Response) without leaking any internal data.
- The application should have proper “Session Management” methods. After sign out or after closing the browser, the session must also terminate.
- Idle timeout for session should be implemented and the timeout can be configurable by admin.
- System should prevent all forms of SQL injection, Cross Site Scripting (XSS) and Cross Site Request Forgery (CSRF) attacks.
- Client-side verification should be in place in order to minimize server processing.
- Any data provided as input to any form/webpage must be validated based on client and server side. For e.g. an input element (Text box, Combo box, Radio button, etc.) to be validated for length, type character set and Range.
- The application should perform proper error handling.
- When a malicious user provides unexpected input to the application, the program should handle the error situation in such a way that it should not give error messages that reveal the database information.
- Error handling must be performed at different levels of applications such as Client, middle-tier and backend.
- All exceptions that can be possibly generated by the application must be taken care and handled with-in the application.
- Well defined and self-explanatory error messages must be built for each kind of exception.

Performance: The webpage must not take more than 3 second to load the whole page (Including rendering or page with text and images). The response time of any asynchronous call must not be more than 1 second with rendering of data on the reasonable client configuration.

- User caching techniques (Client Side, Server Side, Redis like tool for the data and session storage), Offload time-consuming tasks to background jobs or queues.
- Disaster Recovery and business continuity: Provide backup utility for database.
- Scalability: Can support up to 100 concurrent users and can be scaled easily with the required feature. (Support for Horizontal scaling by using load balancers HAProxy/ nginx). Design the application to handle a growing number of documents and users. Consider scalability in terms of both performance and storage.

- Disaster Recovery and Business Continuity (Implement measures to prevent data loss in case of failure.
- Portability: Must be deployable on Linux/ Windows machine.
- Usability: Must support latest version of web browsers (Chrome, Firefox, Safari, Opera and Edge) and on Windows, Linux and MacOS. Multi device support smartphones and tablets. The responsive application based on the aspect ratio. (Mobile-First design).
- Availability: Redundancy, backup and recovery.
- Reliability: No failure. If failed recovery.
- Must be reliable with transaction data while editing the same record by many clients at the same time. (Fault tolerance, always available – supports load balancer, distributed cache), zero downtime deployment – rolling deployment, 24x7 operations (99.99999 availabilities).
- Integrity: The system should maintain data integrity at all times.
- Compatibility: The proposed DMS solution shall be installed locally on server in ITER-India premises, but should be capable for migration to cloud infrastructure in future.
- Maintainability: Easy to maintain and deploy. Easy to fix the issues, meaningful errors and description on error. (Modular with framework, MVC architecture)

## 11. Other Conditions:

The vendor can have the team at onsite or offsite or mixed mode which can vary based on the project activities and phases. As and when required the vendor has to deploy the team (team members) onsite at client office (ITER-India office) and for the same the travel, boarding and lodging cost shall be borne by the vendor and ITER-India will not pay any additional amount for the same.

During execution (development) of the project the tools/infrastructure (Desktop, laptops, development tools, testing tools etc.) required to perform their day to day activities shall be provided by the vendor to the team. In case of change of team member, ITER-India holds the right to approve the joining team member by taking technical interview and only after approval of ITER-India shall the team member be allowed to be part of the development team. Any changes in development team during execution of the project shall require approval from ITER-India. ITER-India will only provide the required hardware infrastructure to deploy the production environment at ITER-India site including the Linux based Operating System(s).