Non Functional Requirements

Instructions

Rating Legend	
Explanation	Vendor's Response Reference
Standard	S
Alternative	A
Workaround	W
Cannot Accommodate	N

Weightage Legend		
Weightage	Symbol	Explanation
Mandatory	M	Refers to a functionality that is considered as mandatory and has to be implemented
Optional	O	Refers to a functionality that is desirable and not mandatory in nature, but having such function would be an added perk to the overall operating effectiveness of the system

Example

Criterion	M - Mandatory, O - Optional	Bidder's Response Reference	Comments
Module 1			
Category			
Criterion 1	M	W	Customization is required
Criterion 2	M	N	Not Supported
Criterion 3	O	A	Module A which is a add-on product which is required
Criterion 4	O	S	Module 1

Note 1: Bidder should take the sole responsibility of add-on products offered via third party solutions.

Hierarchy	Non Functional Requirements	Mandatory (M)/Optional (O)	Response	Comments
1	**User Profile Management**			
1.1	Ability to provide secure user authentication to ensure that only authorized individuals can submit guarantee applications.	M		
1.2	Availability of initial system generated random password.	M		
1.3	Ability to prompt the user to change the system generated password in the first login.	M		
1.4	Ability to prompt the user to change the password when required.	M		
1.5	Ability to parameterize the password complexity requirements.	M		
1.6	Ability to block re-assigning "X" number of previous Passwords. "X" should be parameterized.	M		
1.7	Generates reminders and forces the Users to change password after a predefined interval from the date of last-change. (Authorized person(s) should be able to define the no. of days for the password expiry)	M		
1.8	Ability to reset the password by an authorized person in case of loss of a user password.	M		
1.9	Availability of "forget password" functionality which links with the OTP and/or user email.	M		
1.10	On successful login attempt, the system should display atleast the last login time and date of the user.	M		
1.11	Ability to define the maximum number of unsuccessful login attempts per user at a given time.	M		
1.12	On completion of the maximum number of unsuccessful login attempts, the system should lock-out access to the user.	M		
1.13	Ability to temporarily or permanently deactivate the user profile.	M		
1.14	Ability to unlock locked user profiles should be restricted to an authorized person.	M		
1.15	Ability to restrict concurrent logins for a single user profile.	M		
1.16	Ability to automatically deactivate user accounts if the user profile is not used for "X" number of days. "X" should be parameterized.	M		
1.17	Availability of extensive Log of all activities	M		
1.18	The system should have the provision for implementing the workflow to manage creation of user account, assigning & modifying privileges and termination, disabling & enabling of user accounts with necessary approvals.	M		
1.19	Ability to capture all the necessary information of an individual user such as privileges, access details such as time, date and frequency.	M		
1.20	Ability to configure the reports/ inquiries related to user accounts and its privileges.	M		
1.21	Ability to capture the history of user accounts date of activation, changes made, enable & disable history, termination details, etc.	M		
2	**User Friendliness**			
2.1	Ability to provide on-line and off-line help facilities	M		
2.2	Ability to generate a meaningful error message rather than simply providing error codes when errors are processed (where applicable).	M		
3	**Access Control**			
3.1	Ability to create, modify, deactivate user access groups	M		
3.2	Ability to define access privileges (e.g.: add, modify, view, delete etc.) for each menu option for different user groups and assign users to a group.	M		
4	**System Monitoring**			
4.1	Ability to register any attempts (successful and unsuccessful) to access restricted areas/resources identifying the user, identification address, security violations, back-up & restoration events, system failures, date and time.	M		
4.2	Availability of complete audit trails for tracking transactions including master data changes through the system showing who entered the transactions and who authorized the transactions when they were entered	M		
4.3	Ability to be flexible in generating audit trails on any relevant selection criteria.	M		
4.4	Ability to prevent any modifications or deletion of audit logs	M		
4.5	Ability to track user's IP and Network Interface address.	M		
4.6	Ability to provide session log files. The user should be able to analyse the information (e.g.: account id, session time, transactions performed, etc.)	M		
5	**Remote Access**			
5.1	Ability for the system to be accessible via a web browser.	M		
5.2	Ability for the web interface to be compatible with all commonly used web browsers	M		
6	**System, Application and End User Performance**			
6.1	Ability for the system to provide the following minimum requirements: 1. The Login, authentication, and verification time - [4 Seconds] 2. Initial Screen Load - [3 Seconds] 3. Screen Navigation: field-to-field - [1 Second] 4. Screen Navigation: screen-to-screen - [5 Seconds] 5. Regular reports generation - [1 Minute Maximum] 6. Monthly reports generation - [5 Minute Maximum]	M		

7	**Interfacing and Integration Support**			
7.1	Ability to interface with mail server to generate emails to users and PFIs.	M		
7.2	Ability to interface with a payment gateway to accept payments.	M		
7.3	Ability to support any third-party integrations/ systems	M		
7.4	Ability to interface with SMS gateway to generate SMSs to users and PFIs	M		
7.5	Ability to integrate with international data sources and systems such as trading platforms, payment networks, and accounting systems to faciliate multicurrency transactions.	M		
8	**System Security Requirements**			
8.1	Ability to provide Access Control List (ACL) with the information of access levels.	M		
8.2	Ability to use antispyware tools.	M		
9	**Workflow Process**			
9.1	Ability to create/change/maintain organizational hierarchy/structures , job hierarchies, work flow (approval levels) etc.	M		
9.2	Ability to define customizable and flexible work flow matrices	M		
9.3	Ability to support parallel and multi-layer approval hierarchies	M		
9.4	Ability to design user-friendly interfaces for workflow initiation, tracking, and monitoring.	M		
9.5	Ability to re-route documents through the approval workflow	M		
9.6	Ability to obtain approval based on the workflow to the authorized personnel via SMS, e-mail etc.	M		
9.7	Ability to send alerts to the concerned authorities according to work flow	M		
9.8	Ability to provide justification for rejection of request at each and every step of the workflow	M		
9.9	Ability to modify any changes and include comments before approval	M		
9.10	Ability to display the status of each and every request at any point of time	M		
10	**Document Management**			
10.1	**Document Management Input**			
10.1.1	Ability to capture documents from the following sources and methods: Scanner, Email, manual upload, bulk upload, etc.	M		
10.2	**Bulk Upload**			
10.2.1	Ability to mass upload information using MS word, excel, PDF etc.	M		
10.2.2	Ability to upload scanned supporting documents as Doc, PDF ,image, etc.	M		
10.2.3	Ability for document creation from a batch: multiple page selection, range selection, individual selection	M		
10.2.4	Ability to view multiple pages of a batch in the same window(pane)	M		
10.3	**Scanning**			
10.3.1	Ability to scan and display images simultaneously	M		
10.3.2	Ability to scan and index document concurrently or batch scanning documents for later filing	M		
10.4	**Image View Options**			
10.4.1	Ability to provide the below options: 1. Magnification: Zoom in/out including fit width, 25%, 50%, 75%, 100%, etc 2. Viewing formats: 2D and 3D 3. Panning: Left, right, up, down 4. Rotation: 0,90,180,270 degrees 5. Grey Scale/ Fast scal support 6. Contrast: lighten, darken images 7. Paging: page up, page down, go to 8. Generate Thumbnail Images	M		
10.5	**Document Indexing**			
10.5.1	Ability to tag documents with specific user defined search terms.	M		
10.5.2	Ability to index all types of document by document upload date, type and other specific definable identifier	M		
10.5.3	Ability to generate automatic document numbering based on custom definition	M		
10.5.4	Ability to index text documents for full text search, to find phrases within the document	M		
10.5.5	Ability to enable indexing of documents using meta data (Ex: file size, created date, name of author, recent modifier, total edit time, etc.)	M		
10.5.6	Ability to index revisions of the documents	M		
10.5.7	Ability to date and time stamp all changes in the database enabling data availability on 'as on date/time' basis	M		

10.6	**Document Search and Inquiry**			
10.6.1	Ability to search using the following generic fields: Document Name, Document Number, Doc type, Division/Project, Author, Assigned Person	M		
10.6.2	Ability to filter search results	M		
10.6.3	Ability to sort documents based on different criterion	M		
10.6.4	Ability to search phrases in text document	M		
10.6.5	Ability to provide a scalable document search engine	M		
10.6.6	Ability to store all data in order to drill down each transaction to its source.	M		
10.6.7	Ability to identify similar documents via meta data	M		
10.6.8	Ability to retrieve all supporting documents related to a transaction.	M		
10.6.9	Ability to capture and import documents from various sources such as scanners, email attachments, and file uploads.	M		
10.7	**Document Maintenance**			
10.7.1	Ability to maintain following details about an individual document includes Document Number, Name, Version, Author, Assigned Person/s, Division/Project, Status - Read & Write, Read Only, Locked, Deleted, Date Created, Date/s & Time modified, Person modified, Date Time of archival, Date Time of Deletion, Description	M		
10.7.2	Ability to link document to specific records in the system	M		
10.7.3	Ability to maintain pre-defined document templates	M		
10.7.4	Ability to create document based on system templates	M		
10.7.5	Ability to define & maintain folder structures	M		
10.7.6	Ability to maintain document structure & hierarchy	M		
10.7.7	Ability to perform following activities for a document within the System, mainly Create, Edit/Change/Write, Display/Read & Delete	M		
10.7.8	Ability to print uploaded documents	M		
10.7.9	Ability to support different formats such as DOC, PDF, EXCEL,etc.	M		
10.7.10	Ability to support different format conversions	M		
10.7.11	Ability to read documents in different formats (E.g.: PDF reader facility)	M		
10.8	**Sharing and Version Control**			
10.8.1	Ability to define authorization matrix for document sharing and version control	M		
10.8.2	Ability to define read/write authority for different users sharing same document	M		
10.8.3	Ability to freeze write permission once a user has locked the document for editing	M		
10.8.4	Ability to forward, move & route documents based on defined authorized matrix	M		
10.8.5	Ability to maintain different versions of the same document	M		
10.8.6	Ability to maintain different formats of the same document name	M		
10.8.7	Ability to automatically unfreeze of editing for other users once committed by downloaded user	M		
10.8.8	Ability to override above access rights anytime by higher level user	M		
10.8.9	Ability to audit all current and historic actions on documents and routing	M		
10.9	**Folder Features**			
10.9.1	Ability to Create, Rename, Move & Delete folders	M		
10.9.2	Ability to drop/select/assign files to a folder	M		
10.9.3	Ability to display folder tree like File Manager	M		
10.9.4	Ability to retreive/pull up documents for display	M		
10.9.5	Ability to apply folder level authorizations	M		
10.10	**Security Features**			
10.10.1	Ability to control access to scanning, printing, indexing	M		
10.10.2	Ability to control access to folders and documents	M		
10.10.3	Ability to facilitate to encrypt documents	M		
10.10.4	Ability to provide support to view documents over the web	M		
10.10.5	Ability to capture information such as user IDs, timestamps, actions performed, and IP addresses for audit and forensic analysis.	M		
10.10.6	Ability to conduct regular security assessments, audits, and penetration tests to validate compliance with regulatory requirements	M		
10.11	**Document Archiving**			
10.11.1	Ability to put a document into an archive including adding metadata and tags to the archive	M		
10.11.2	Ability to seearch the archive for title/creator/date/ and various other metadata	M		
10.11.3	Ability to enable electronic archiving of selected documents or group of documents to a secondary storage	M		
10.11.4	Ability to search for specific document or group of documents in the electronic archive (based on document ID or metadata)	M		
10.11.5	Ability to retreive archived electronic documents	M		
10.11.6	Ability to restore electronic documents from the archive to the main document storage	M		