

Upgradation and AMC of MDL website for 05 years

I MDL website Brief Introduction

MDL website is hosted on NIC Cloud Meghraj to ensure high availability and secure environment. MDL has opted Platform as a Service (PaaS) from NIC Cloud for hosting MDL website. PaaS provides pre-installed web and database servers to publish website and its applications. In addition, PaaS also provides server vulnerability assessment, server backup & anti-virus and network / application firewall facilities.

MDL website comprises of high-end Web technology to make the website extra secure and free from possible virus threats.

Below are the details related to the web technologies currently used on the website:

- Current domain of Website is: <https://mazagondock.in>
- Website Pages: MDL website consists of a number of static and dynamic pages in Hindi and English. Website is hosted on Windows Server 2019 (IIS 10.0). Website is developed in .NET 6, Website Application Modules in .NET framework version 4.8 & database MSSQL 2019. MDL website has a CMS to manage the website content as well as a dynamic application module for uploading & displaying of Tender Notifications of various Commercial Departments, application for uploading & displaying Career Notifications for Executives, Non-Executives and Apprentices in the MDL Website Admin end.
- Front-end Tool to manage the Server side Scripts is ASP.NET
- The entire website contains various formats like HTML, SHTML, JPEG, GIF, MPEG, MP3, MP4, PDF, XLS, XLSX, ZIP, PEARL CGI, JAVA, PHP, ASP, ASPX etc.
- The website is bilingual - Updating in both English and Hindi version simultaneously.

II Scope for Upgrade and AMC of MDL website for 05 years

10. Upgrading Website and Website Application Modules to latest .NET Platform
20. Maintenance of website and its servers for 05 years
30. Security Audit of MDL website and applications by CERT-IN and STQC empanelled Auditor
40. GIGW latest version compliance Certification for MDL Website by STQC
50. GIGW latest version Annual Surveillance Audit of MDL website by STQC
60. Creation of New Dynamic Pages and Database
70. Modification of New Dynamic Pages and Database
80. Onsite Engineer
90. Star SSL Certificate



10.10 Upgrading Website and Website Application Modules to latest .NET Platform

The existing website pages are in .NET 6 (Core) platform and Website Application Modules are under .NET 4.8 Framework. The line item 10.10 is for the upgradation of website and application modules to the latest version of .NET platform.

‘Upgradation of website and its application modules to latest .NET Platform’ and ‘Maintenance of existing MDL website and application modules’ will be parallel activity. In addition to all upgradation activities, vendor shall maintain existing website to ensure uninterrupted support.

Code Upgrade:

- Upgrading of existing MDL website and application modules to latest .NET Platform.
- Upgradation of the .NET platform to be carried out as and when required on requirement of cyber security audit/VAPT Report for compliance purpose.
- Ensure compatibility with existing/latest libraries, functionalities, third party integration, payment gateway and custom codes.
- Ensure the new .NET Platform includes the latest security patches.
- Optimize and Refactor inefficient and redundant code to improve performance, maintainability and security.
- Leverage the latest .NET performance improvements.
- Ensure that existing database version is compatible with upgraded .NET version. If required, upgrade the database management system.
- Upgradation also involves changing design and the entire look and feel of the website application modules (Refer the **para III**) in line with current theme of website, including migration of existing applications and content on a new platform, complying with Guidelines for Indian Government Website (GIGW latest version Compliant).
- Update CSS/Java Script to support responsive and fluidic design of website and its modules.
- CMS using latest GUI design approach to adapt to various screen size, browser and device compatibility with AI/ML capabilities as per MDL requirements.
- Any development should follow the latest CERT-In Guidelines. (Refer Guidelines for secure Application Design, Development, Implementation & Operations currently available at https://cert-in.org/PDF/Application_Security_Guidelines.pdf and relevant latest versions)

Integration and System Testing

- Ensure all existing unit tests run successfully in upgraded environment.
- Verify all website functionalities (front end and back end) work as expected post-upgrade. Perform load testing to ensure the website can handle the same or greater volume of traffic.
- Website and Modules must be tested across various devices and screen sizes to ensure responsiveness and usability.
- Optimize Website performance for faster load times on all devices and browsers.

Deployment:

- Post development to a staging environment, Security Audit from CERT-IN empanelled auditor to be done and after compliance the site to be deployed on Production server.
- Timeframe for completion of upgradation of .NET platform will be 06 months plus 1 additional month for security clearance.
- The bidder has to provide the details of the platform versions and tools that will be used for the development as part of the bid. Also the bidder has to provide the detailed process of how this conversion/development of the upgradation will take place with milestones.



- The upgradation shall be subject to GIGW latest version certification post deployment. Efforts to be made during development that GIGW aspects are also taken care of in the development process itself for faster certification.
- Monitor the website after deployment to ensure stability and performance.

Deliverables:

- Updated Website with latest .NET Platform.
- Comprehensive testing and bug reports.
- Documentation and User Manual to be provided to MDL for smoother maintainability.
- Updated source code of website to be provided to MDL.

20.10 Maintenance of website and its servers for 05 years (i.e. 60 months):

Maintenance of existing website and its servers will be start from 24 May 2025 or from the date of start PO, whichever is later.

A. Maintenance of Website and its applications

Maintenance of website its applications involves ongoing activities aimed at ensuring the website remains functional, secure, up-to-date, and aligned with business goals.

(i) Regular maintenance activities:

- Updating website pages and related documents, database as and when required.
- Updating in both English and Hindi version simultaneously conformity with GIGW latest version guidelines.
- Continuously monitor website performance using tools and track site uptime and response time.
- Regularly update meta tags, alt texts, and descriptions to maintain SEO rankings.
- Post Website upgradation to latest .NET platform (as per line item 10.10), MDL website shall be upgraded to latest .NET platform, whenever new stable version is released and/or support for existing .NET platform is about to expire.

(ii) Resolution of Problems/Issues:

- Solving day-today issues related to MDL website & all its applications
- Bug Resolution:** If the website / applications needs to be bug fixed or any error occurs or any minor changes or minor upgradations need to be made in the website / applications, then vendor should maintain / modify the website and its applications as per requirement given by MDL.
 - Identify and fix bugs reported by users, detected during monitoring, or discovered during routine maintenance.
 - Prioritize bugs based on their impact on the website's functionality and user experience.
 - Document all bug fixes and update relevant sections of the code repository.
 - Replacement of obsolete software/codes and related drivers/application with latest compatible software/codes with latest drivers/application.

(iii) Security Management

- Implement all application level security patches
- Monitor the website for potential vulnerabilities and fix them before exploitation.



- c) Implementation Web Application Firewall (WAF) and testing of website performance under WAF to protect against threats like DDoS attacks, SQL injections and other malicious activities.
- d) **Feature Enhancements:**
 - Implement enhancements or new features as requested by the MDL, such as adding new plugins, modifying layouts, upgradation to latest .NET platform or updating site functionality.
 - Ensure all enhancements are tested in a staging environment before being deployed to production.
- e) **Logs:** Maintain and review following logs and provide as and when required by MDL
 - **Application Logs** – Error Logs, Warning Logs, Info logs and Debug Logs.
 - **Security Logs** – Authentication Logs, Authorization Logs, Intrusion Detection Logs
 - **User Activity Logs** – Session Logs, Audit Logs

B. Maintenance of Servers:

Maintenance of Servers includes ongoing support and management of hosting server environment. This includes ensuring servers' security, stability, performance and scalability while minimizing downtime and resolving technical issues that may arise.

(i) Monitoring and Performance Optimization:

- Continuous monitoring of Server performance, uptime, CPU, Memory and bandwidth.
- Optimize server resources and database performance.
- Archival of old file/data and organization of files/data available at path/directory.
- Clean and optimize website database to ensure fast query execution and minimal load time.
- Remove unnecessary data like old revisions, unused metadata and logs to improve database efficiency.
- Uptime, Traffic, Error Monitoring using tools whitelisted by CERT-In.

(ii) Backup and Restore of File System and DB:

- Schedule automated backups of server data (Web files, databases) with periodic testing.
- Monitoring backup process of website & applications.
- Vendor shall provide the complete backup of the data and also take backup on regular basis. Vendor shall collect backup of MDL website from NIC as and when required.

(iii) Security Management:

- Patching of Vulnerabilities related to Windows, Security Policy, Office Applications, other applications, etc. as per VA Report, CERT-In and other govt. agency guidelines.
- Updating of all Open Source or Proprietary -Applications, Frameworks, Software, Packages, IDEs, Databases, Reporting/BI/Analytical Tools, Services, APIs, Components, Libraries, Plugin etc., used on servers with the latest updates/patches.
- Installation of NIC Provided Antivirus Clients on all Servers. Full System scan should be done at least once in a week and Quick/Flash scans should be done at least once in a day.

(iv) Coordination with NIC cloud/support team for resolving server related problems/issues as and when required.



(v) Logs

- Maintain and review following logs and provide as and when required by MDL
 - Webserver Logs - Access and error logs
 - DB Logs – Access, Query, Error and Transactional Logs
 - FTP Logs
 - Backup Logs

C. Renewal of Domains:

Vendor shall provide support including renewal/registration costs during the period of the contract for the 8 domains: 8 domains currently registered with MDL –

Sr No.	Domain Name
1	mazdock.com
2	mazdock.co.in
3	mazdock.org
4	mazdock.in
5	mazdock.net
6	mazagondock.in
7	mazagondock.co.in
8	mazagondock.org

D. Deliverables:

- **Documentation:**
 - Maintain up-to-date documentation for all aspects of the website, including system architecture, software versions, and configuration settings.
 - Document all changes made during maintenance, including software updates, security patches, and configuration changes.
 - Document all reported problem/issues/bugs/vulnerabilities and their root cause with RCA and PCA.
 - Document version changes of any changes to code.
 - Provide the MDL this documentation as and when required.
- **Monthly Reports:**
 - Provide comprehensive monthly reports that include:
 - Summary of all maintenance activities performed including all logs.
 - Detailed performance metrics (load times, uptime, traffic, etc.).
 - Implementation of Security updates/Patches as per CERT-In and other govt. agency guidelines
 - Error logs and resolutions.
 - Recommendations for future improvements or upgrades.
- **Backup and Restore Documentation:**
 - Provide a comprehensive backup and restore guide, detailing the steps required to restore the website from a backup in the event of a failure.
 - Ensure that the MDL team is familiar with the backup and restore process.



30.10 Security Audit of MDL website / application by CERT-In and STQC empanelled auditor

As MDL website is hosted on NIC Server, security audit of the website/web applications by **CERT-In empanelled auditor** and **CIRA** is prerequisite whenever there are major changes in the website/web applications.

To avoid repetitive audits - **one** for CERT-In security audit and **another** security audit for GIGW latest version compliance for MDL Website, the auditor shall be the CERT-In empanelled auditor and also registered under Website Quality Certification Scheme in STQC. (Refer STQC rules and procedures – STQC/WQCS/D01 issue: 2.0 dated June 2023 and relevant latest updates)

Whenever **auditor** is mentioned, it should be considered as 'CERT-In and STQC empanelled Auditor'.

Before uploading the modified web contents (which includes dynamic web pages) on production server of NIC –

- a) The firm/vendor should get the website audited from **auditor** on testing URL hosted on development or NIC testing server. After patching all vulnerabilities and successful audit by **auditor**, Security Audit Report and "Safe to Host" Certificate shall be provided to MDL.
- b) NDA to be signed with **auditor** and MDL as per CERT-In and STQC guidelines.
- c) Post clearance from **auditor**, testing website shall be audited by CIRA. VAPT Audit shall be done by CIRA on request from MDL. Any observations/vulnerabilities reported by CIRA VAPT report shall be complied and re-audited by **auditor** again and fresh Test Report and Safe to Host (STH) certificate from **auditor** shall be obtained.
- d) The Audit count will be **one** only, irrespective of no. iterations of security audit required for closure of CIRA VAPT observations and 'safe to host' clearance from CIRA. (For one complete cycle).
- e) Post Security Audit clearance and Safe to Host Certificate received from 'CERT-In and STQC empanelled Auditor' and CIRA, clearance certificate from Application Security Group, NIC is to be obtained.

CERT-In empanelled auditor list is available at <https://cert-in.org.in/certEmpanelment.jsp>

Scope for website security audit includes:

First Phase (CERT-In and STQC Empanelled Auditor):

1st round of audit:

The website/web application contents Audit (1st round of audit) to be carried out on Vendor development server on the basis of the OWASP Top Ten - List of the 10 most dangerous current Web application security flaws along with effective methods of dealing with those flaws. As a scope of work, the following needs to be evaluated but not limited to:

- Invalidated input - Invalidated requests being used by a web application including Buffer overflows.
- Broken access control
- Broken authentication and session management - Evaluate the Proper Protection of Account credentials and session tokens.



- Cross site scripting (XSS) flaws
- Insecure Communications - Failure of web application to encrypt network traffic when it is necessary to protect sensitive communications.
- Injection flaws (particularly SQL injection) - Passing of parameters by Web applications access external systems or the local operating system.
- Information Leakage and Improper Error Handling - Error conditions that occur during normal operation are not handled properly.
- Insecure Cryptographic storage
- Denial of service (DOS) - Consumption of resources by MIS Application to a point where other legitimate users can no longer access or use the application.
- Insecure configuration management
- Cross Site Request Forgery (CSRF)
- Any other Vulnerabilities.

Any deviation from OWASP and vulnerability reported by the **auditor** during testing is to be fixed by the Vendor. OS level audits & system level VAPT should also be part of audit.

2nd round of audit: Audit (2nd round of audit) to be performed on the deviation from OWASP audit and vulnerability reported by the **auditor** in 1st round of audit.

After successful completion of website security audit, "Safe to Host" Certificate and Audit Report obtained from **auditor** to be submitted to MDL.

Second Phase (CIRA):

Post completion of phase one, testing website shall be audited by CIRA. VAPT Audit shall be done by CIRA on request from MDL.

Any observations/vulnerabilities reported by CIRA VAPT report shall be complied and re-audited by **auditor** again (as per **first phase**) and fresh Test Report and Safe to Host (STH) certificate from **auditor** shall be obtained, till VAPT Audit clearance for MDL Website is obtained from CIRA.

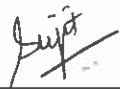
Third Phase (NIC Application Security Group):

Post completion of second phase, clearance certificate from Application Security Group, NIC is to be obtained for safe hosting on NIC Production Server.

The audited contents will be uploaded to NIC production server only after completion of third phase i.e. Website Security audit clearance obtained from 'CERT-In and STQC empanelled Auditor' and CIRA, followed by 'Safe to Host' Clearance certificate from Applications Security Group, NIC.

Deliverables:

- 'Safe to Host (STH)' Certificate and Audit Report from 'CERT-In and STQC Empanelled Auditor'.
- Clearance of CIRA VAPT Audit observations/vulnerabilities for Safe to Host Certificate and Audit Report by CIRA.
- Clearance from 'NIC Application Security Group' post clearance from 'CERT-In and STQC Empanelled Auditor' and CIRA.
- Website security audit by 'CERT-IN and STQC empanelled auditor' will be done -
 - Full audit once a year.
 - Any new developments or change in dynamic content or as and when requested by MDL.



40.10 GIGW latest version compliance Certification for MDL Website by STQC

- a) Wherever GIGW is indicated, it to be considered as '**GIGW latest version**' compliance.
- b) MDL website is required to be certified by the Standardisation Testing and Quality Certification (STQC) Directorate of the Ministry of Electronics and Information Technology (MeitY), Government of India, for compliance with GIGW guidelines.
- c) The final output must be audited against latest GIGW guidelines and detailed audit report along with compliance certificate from STQC must be obtained by the vendor and submitted to the Company.
- d) Any deviation from GIGW and vulnerability reported by the STQC team during testing is to be fixed by the Vendor.
- e) After satisfactory assessment results, the Certificate of Registration and Certification Mark is issued by STQC. GIGW compliance Certificate by STQC shall be valid for three years from the date of issue with annual surveillance audit.
- f) Vendor shall obtain GIGW Compliance Certificate by STQC and hand over the same to the MDL in original.

References: Refer STQC (<https://stqc.gov.in>) and GIGW website (<https://guidelines.india.gov.in>) for latest documents and procedures/updates.

Currently available documents are as follows:

- Preparation of Website Quality Manual as per the template provided on STQC Website (URL: https://stqc.gov.in/sites/default/files/tenders/WQM_0.pdf) in compliance with GIGW guidelines for submission to STQC.
 - GIGW Compliance & Certification Handbook can be referred for the process on URL: (<https://guidelines.india.gov.in>)
 - STQC website can be referred for Website Quality Certification Procedure (<https://stqc.gov.in/content/website-quality-certification-0>)
- g) Vendor should obtain Website Audit Certificate of MDL Website for digital accessibility compliance by an accessibility expert who holds certification from IAAP – International Association of Accessibility Professionals.
 - h) Vendor should comply with latest WCAG (Web Content Accessibility Guidelines) version AA standards, GIGW and other accessibility guidelines.

Deliverables:

- Website Quality Manual as per GIGW guidelines.
- GIGW latest version Compliance Certificate from STQC.
- Website Audit Certificate of MDL Website for digital accessibility compliance from IAAP (International Association of Accessibility Professionals) complying with latest WCAG (Web Content Accessibility Guidelines) version AA standards, GIGW and other accessibility guidelines.
- Accessibility Conformance Report (ACR): Deliver a formal report based on the latest Voluntary Product Accessibility Template (VPAT) that certifies MDL Website's compliance with accessibility standards.
- Accessibility Statement: Develop a clear, concise Accessibility Statement to be published on MDL Website.

50.10 GIGW latest version Annual Surveillance Audit for MDL Website by STQC

- a) Wherever GIGW is indicated, it to be considered as '**GIGW latest version**' compliance.
- b) Every year **surveillance Audit** for MDL website is required to be cleared by the Standardisation Testing and Quality Certification (STQC) Directorate of the Ministry of



Electronics and Information Technology (MeitY), Government of India, for compliance with GIGW guidelines.

- c) The final output must be audited against latest GIGW guidelines and detailed audit report along with compliance certificate from STQC must be obtained by the vendor and submitted to the Company.
- d) Any deviation from GIGW and vulnerability reported by the STQC team during testing is to be fixed by the Vendor.
- e) After satisfactory assessment results, the Certificate of Registration and Certification Mark is issued by STQC. Annual Surveillance Audit Certificate shall be valid for one year from the date of issue.
- f) Vendor shall obtain GIGW Annual Surveillance Compliance Certificate by STQC and hand over the same to the MDL in original.

References: Refer STQC (<https://stqc.gov.in>) and GIGW website (<https://guidelines.india.gov.in>) for latest documents and procedures/updates.

Currently available documents are as follows:

- Preparation of Website Quality Manual as per the template provided on STQC Website (URL: https://stqc.gov.in/sites/default/files/tenders/WQM_0.pdf) in compliance with GIGW guidelines for submission to STQC.
- GIGW Compliance & Certification Handbook can be referred for the process on URL: (<https://guidelines.india.gov.in>)
- STQC website can be referred for Website Quality Certification Procedure (<https://stqc.gov.in/content/website-quality-certification-0>)
- g) Vendor should obtain Website Audit Certificate of MDL Website for digital accessibility compliance by an accessibility expert who holds certification from IAAP – International Association of Accessibility Professionals.
- h) Vendor should comply with latest WCAG (Web Content Accessibility Guidelines) version AA standards, GIGW and other accessibility guidelines.

Deliverables:

- Website Quality Manual as per GIGW guidelines.
- GIGW latest version Annual Surveillance Compliance Certificate from STQC.
- Website Audit Certificate of MDL Website for digital accessibility compliance from IAAP (International Association of Accessibility Professionals) complying with latest WCAG (Web Content Accessibility Guidelines) version AA standards, GIGW and other accessibility guidelines.
- Accessibility Conformance Report (ACR): Deliver a formal report based on the latest Voluntary Product Accessibility Template (VPAT) that certifies MDL Website's compliance with accessibility standards.
- Accessibility Statement: Develop a clear, concise Accessibility Statement to be published on MDL Website.

60.10 Creation of New Dynamic Pages and Database

Any major change / any enhancement / new development should be carried out by Vendor as requested by MDL. The requirement shall be mapped into number of pages (unit of measurement) which shall be deployed as part of the changes/enhancement. The no. of pages shall be consumed at actual post completion of activities, based on MDL requirement.

70.10 Modification of New Dynamic Pages and Database

Any major change / any enhancement to the existing website and its applications should be carried out by Vendor as requested by MDL. The requirement shall be mapped into number of pages (unit of measurement) modified. The no. of pages shall be consumed at actual post completion of activities, based on MDL requirement.

80.10 Onsite Engineer

The scope of work of Onsite Engineer will be

- a) Regular day-to-day updating to MDL website - uploading of tenders/documents/photos/circulars/press release, etc.
- b) Uploading of developed applications to production server after cert-in audit/after testing
- c) Applying latest OS updates/patches & Compliance of security advisories including upgrades i.e. all admin related activities
- d) Monitor web access logs/database logs/user activity logs for any unusual activities
- e) check all files present under the Website root directory and Upload directory for any unauthorized file modifications and deletions on a daily basis
- f) Backup of web server, database server and logs
- g) Regular backup of Application Data, website and database
- h) And other activities as mentioned in Item 20. Maintenance of website and its applications for 5 years (i.e. 60 months):

Basically any updates to the MDL server hosted on NIC cloud will be done from MDL. New development can be done at vendor premises. The bidder shall share the modified / updated files/scripts and the onsite engineer shall then upload the same to the website.

Working Hours: Monday to Friday – 9 AM to 6 PM

If required, Engineer will have to be present on Saturdays, Sundays & MDL holidays as well or whenever presence is required under exigency. Engineer has to stay beyond normal working hours in case any urgent activities has to carried out. Necessary alternate arrangement to be made in case onsite engineer is on leave.

The onsite engineer should be technically qualified IT professional - Minimum Full-time Graduate or full-time Diploma in Engineering with two years' experience in software development.

Onsite Engineer has to report to MDL site within 05 working days' post start date of contract/PO.

90.10 Star SSL Certificate

Procurement, installation of Star SSL certificate and Annual Renewal of Star SSL certificate of a current domain of MDL Website.

Star SSL certificate to be procured shall be valid for maximum permissible period of validity as per rules applicable to Star SSL Certificates.

III Applications in MDL website

Following Online Applications are hosted on MDL website. These applications include aspx, .asp and supporting js files, css files, dll files & config files. The application contains various formats like html, .jpg, .jpeg, .pdf, .doc, .xls & .xlsx.



1. Online Recruitment for Executives, Non-Executives & Apprentices with online payment option through payment Gateway.

This module in the MDL website is an online facility for recruitment for 3 different categories – Executives, Non-Executives and Apprentice.

The system has User/candidate and Admin role. System has Separate Admin accounts for Executives, Non-Executives & Apprentices category.

The job and advertisement is posted by Admin. Admin will post the job opportunity from the backend which will reflect on the Job portal. The user will be able to apply for the Job from the portal and pay challan using offline mode or online mode using a payment gateway. The news and advertisement regarding jobs/post to be displayed on portal login page. Executives module will have additional roles for Medical and Security clearance in a workflow approach.

Executives / Non-Executives / Apprentice

User Login

1. Registration – creation of user account by the candidate.
2. Verification link for Validation of email-id for creation of user login
3. User login - Registered users can sign in using their login credentials
4. Job Registration - Register for the job/apply for advertised post
5. Submission of Application including uploading of documents/certificates, preview form
6. Payment challan and view payment status
7. Display/report of job posts applied with all details and view uploaded documents, payment status
8. Option to download Call Letter for written test/interview
9. Submit Travel Allowance claim form along with bank details

Following are the steps/actions that will be incorporated by the Admin:

1. Creation of Job post with details of opening, closing date, advertisement reference number, post, qualification, eligibility criteria, test centres etc.
2. Uploading of List - Standard Templates for giving particular message. Variables for the template uploaded through excel.
 - Shortlisting Candidates for Written Test
 - Shortlisting Candidates for Personal Interview
 - Shortlisting Candidates for PEME (Pre Medical Employment Examination) Exam
 - Shortlisting candidates for Final Merit List
 - Appointment Letter
 - Travel Allowance Claims
3. Processing of all documents and communicate with user through emails, sms and can also be viewed through user login

2. Online Vendor Registration:

This module in the MDL website is an online facility for vendor registration. Vendors can apply for the tenders by registering through the portal. The module has roles for User/Vendor and Admin. The entire Vendor portal can be managed by vendor portal admin in the backend.

Following are the steps/actions that will be incorporated by the user and the Admin:

- Online Vendor Registration
- Vendor login portal
- Vendor Renewals System

Step 1: The vendor first register themselves by entering basic details to get login id and password. Login is their email id. After registration, the login id and password are mailed to the given email id and an SMS notification also sent.

Step 2: The vendor then logs in using the credentials given and enters details - Organisation information, details of factory, legal information, financial information, uploading of relevant documents in pdf format as proof for details furnished.

Step 3: After vendor submits the form, the details are mailed to admin who can download the documents for scrutiny. In case of any clarification, admin through email communicates (offline) with vendor and vendor uploads required information through portal.

Step 4: After scrutiny and subsequent approval, vendor number is generated and communicated to vendor through email and same updated on vendor registration portal.

Email/SMS notification provision at every stage. But currently Email sent at every stage.

3. Online Bill Status/Tracking System:

The Vendors can track the bills online through the bill tracking system. The system has admin login for Uploading vendor billing data periodically. The vendors through their User/vendor login can check the status of bill by entering their login and password.

Option also given to vendor for reset of password

4. Online Vendor Balance Confirmation:

The system has admin login for uploading vendor balance.

The vendors through their User/vendor login can view the vendor balances report by entering their login and password.

5. Online Portal for Retired Employees:

This system is a Portal for Retired Employees. The system has access for user/employee, admin and super admin.

The admin login has access to create Employee Logins – single login creation or bulk login creation through bulk upload facility.

To add News and Notification.

To view and reply to grievances raised through the portal, triggering emails

To monitor Feedback response.

To monitor User status and to upload family member details.

To view Life certificate uploaded and provide approval status and remark if any

To upload Last Month Salary, PRP, Form 16

To provide status of OPD claims submitted

The retired employees' login to the portal using their P. No. and password. The user has access

To view News and Notifications

To Upload Life Certificate yearly

To view status of Uploaded certificate – approved/reason for disapproval

To send update request for any change in personal details

To give feedback

To submit grievance if any and also check for comments against their grievance or feedback.

To view Form16 (multiple forms), Salary slip and any other documents

To submit medical claims online and also track status of the claim

SuperAdmin Role to track/monitor grievances and reply given by admin

6. Employee Portal:

This system is a portal for all the working employees and is purely display of report without any processing. The user logs in with their employee id and can view information.

The portal has Employee, Admin and Super Admin roles. The employees can login using their employee ID, password and OTP for viewing of Payslip, pension details, leave balances, PF slip, different manuals and important company circulars etc.



The admin login is for uploading relevant data. The uploaded data/document is associated to different admins who have authority only for specific uploads.

The super admin has access to upload all relevant information.

Upload facility provided for uploading documents either as single entity or bulk upload.

7. Bank Investment Module: This module is to receive document from bank representatives. User login is for upload new document and view existing document and admin login for to view uploaded document, create bank (user) logins, enable the upload link.

These are the current applications. In addition to that, there might be one more module that may get added in due course of time. The same also to be part of the upgradation, maintenance and support. Bidder can approach MDL for more details of under developed module before submission of bid.

Period of contract

05 years from the date of start of contract/PO

Payment Terms

No Advance payment will be made. The payments for the line items shall be made only after the completion of the work at actual.

Line Item	Payment Terms
10.10	Post Go Live of website and application with latest .NET platform.
20.10	Quarterly basis after completion of quarter
30.10	Post receipt of Audit certificate and clearance from NIC for deployment on actual quantities consumed.
40.10	Post GIGW compliance certificate from STQC
50.10	Post GIGW Annual Surveillance Audit compliance certificate from STQC
60.10 & 70.10	After sign-off of the activities indicated in these line items based on actual quantity consumed respectively.
80.10	Quarterly basis after completion of quarter.
90.10	Post implementation of Star SSL Certificate

Timeline of completion of activities and Penalty clause:

The request / issues shall be forwarded by Executives of MDL User Departments (like CIT Dept., HR Dept, Materials Dept, Finance, Commercial etc.) via email to the Bidder.

The request / issue raised by MDL to the Bidder for following PR, Line Items should be completed within following given time period from the Date of request or registration of the problem, issue, bug, vulnerabilities, activity.

Time Frame for Completion of Work from the Date of request or registration of the problem, issue, bug, vulnerabilities, activity as given below.



Item No	Timeline of completion of activities	Penalty clause																								
10.10	06 months + 01 month for security Audit clearance	If completion timeline delays, penalty will be applicable. Post (06 + 01) months, penalty @ 0.5 % per week (max capped to 5%) of line item value shall be levied.																								
20.10	<table border="1"> <thead> <tr> <th>Sr. No</th><th>Resolution Priority</th><th>Resolution Time</th></tr> </thead> <tbody> <tr> <td>1</td><td>High*</td><td>4 Hours</td></tr> <tr> <td>2</td><td>Medium**</td><td>3 Days</td></tr> <tr> <td>3</td><td>Low***</td><td>5 Days</td></tr> </tbody> </table> <p>*High – Critical issues, vulnerabilities, maintenance activity affecting availability, security or core functionality of website.</p> <p>**Medium- These affects functionality or performance but do not completely disrupt core website process or pose immediate security risks. These includes medium vulnerabilities, issues, maintenance activity.</p> <p>***Low – These have minimal impact on website functionality or are pure cosmetic or non-urgent issues. They do not affect the users significantly. These includes low vulnerabilities, issues, maintenance activity.</p>	Sr. No	Resolution Priority	Resolution Time	1	High*	4 Hours	2	Medium**	3 Days	3	Low***	5 Days	<p>For any delay in resolution of bug, vulnerabilities, issue based on resolution priority, following penalty will be applicable.</p> <table border="1"> <thead> <tr> <th>Sr. No</th><th>Resolution Priority</th><th>Penalty (For Delay in Resolution)</th></tr> </thead> <tbody> <tr> <td>1</td><td>High*</td><td>Penalty @0.5% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.</td></tr> <tr> <td>2</td><td>Medium**</td><td>Penalty @0.25% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.</td></tr> <tr> <td>3</td><td>Low***</td><td>Penalty @0.10% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.</td></tr> </tbody> </table>	Sr. No	Resolution Priority	Penalty (For Delay in Resolution)	1	High*	Penalty @0.5% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.	2	Medium**	Penalty @0.25% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.	3	Low***	Penalty @0.10% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.
Sr. No	Resolution Priority	Resolution Time																								
1	High*	4 Hours																								
2	Medium**	3 Days																								
3	Low***	5 Days																								
Sr. No	Resolution Priority	Penalty (For Delay in Resolution)																								
1	High*	Penalty @0.5% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.																								
2	Medium**	Penalty @0.25% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.																								
3	Low***	Penalty @0.10% per issue per day (Max. capped to 5% per issue per month) of line item value shall be levied.																								
30.10	Time frame for completion of work is 08 Weeks per audit from the date of request for conducting CERT –in audit.	Post 08 Weeks, penalty will be 0.5% per week capped@ max 5% per audit - of line item value.																								
40.10	Time frame for completion of work is 16 Weeks from the date of request for conducting GIGW audit.	Post 16 Weeks, penalty will be 0.5% per week capped@ max 5% per audit - of line item value.																								
50.10	Time frame for completion of work is 04 Weeks from the date of request for conducting GIGW Annual Surveillance audit.	Post 04 Weeks, penalty will be 0.5% per week capped@ max 5% per audit - of line item value.																								
60.10	Within - Mutually agreed duration of completion.	For any delay in completion of activities for creation of new pages and database, penalty applicable will be as below.																								



		<table> <tr> <th>Sr. No</th><th>Issues</th><th>Penalty (For Delay in completion)</th></tr> <tr> <td>1</td><td>Incomplete or inadequate activity for creation of new pages and database</td><td>Penalty @0.5% per incomplete/inadequate activity per day (Max capped to 5% per incomplete/inadequate activity per month) of line item value consumed for these activities shall be levied.</td></tr> </table>	Sr. No	Issues	Penalty (For Delay in completion)	1	Incomplete or inadequate activity for creation of new pages and database	Penalty @0.5% per incomplete/inadequate activity per day (Max capped to 5% per incomplete/inadequate activity per month) of line item value consumed for these activities shall be levied.			
Sr. No	Issues	Penalty (For Delay in completion)									
1	Incomplete or inadequate activity for creation of new pages and database	Penalty @0.5% per incomplete/inadequate activity per day (Max capped to 5% per incomplete/inadequate activity per month) of line item value consumed for these activities shall be levied.									
70.10	Within - Mutually agreed duration of completion.	<p>For any delay in completion of activities for modification of pages and database, penalty applicable will be as below.</p> <table> <tr> <th>Sr. No</th><th>Issues</th><th>Penalty (For Delay in completion)</th></tr> <tr> <td>1</td><td>Incomplete or inadequate activity for modification of pages and database</td><td>Penalty @0.5% per incomplete/inadequate activity per day (Max capped to 5% per incomplete/inadequate activity per month) of line item value consumed for these activities shall be levied</td></tr> </table>	Sr. No	Issues	Penalty (For Delay in completion)	1	Incomplete or inadequate activity for modification of pages and database	Penalty @0.5% per incomplete/inadequate activity per day (Max capped to 5% per incomplete/inadequate activity per month) of line item value consumed for these activities shall be levied			
Sr. No	Issues	Penalty (For Delay in completion)									
1	Incomplete or inadequate activity for modification of pages and database	Penalty @0.5% per incomplete/inadequate activity per day (Max capped to 5% per incomplete/inadequate activity per month) of line item value consumed for these activities shall be levied									
80.10		<p>Onsite engineer absenteeism per day</p> <table> <tr> <th>Sr.No</th><th>Duration</th><th>Penalty</th></tr> <tr> <td>1</td><td>Half Day</td><td>Rs. 1250</td></tr> <tr> <td>2</td><td>One Day</td><td>Rs. 2500</td></tr> </table> <p>The penalty for absenteeism will be calculated every quarter and recovered from charges of that quarter.</p>	Sr.No	Duration	Penalty	1	Half Day	Rs. 1250	2	One Day	Rs. 2500
Sr.No	Duration	Penalty									
1	Half Day	Rs. 1250									
2	One Day	Rs. 2500									
90.10	Before expiring of existing SSL Certificate	Nil									



NDA to be signed with vendor.

Note: Bidder submitting the bid for the solution should not further subcontract the work of development and maintenance of MDL Website (excluding security audit of website by CERT-In empanelled auditor and GIGW compliance Certification by STQC.)

Upgradation and AMC of MDL website for 05 years w.e.f. 24 May 2025 or from start date of PO, whichever is later.



सुजित अमुलभाई शाह
SUJIT AMULBHAI SHAH
उप प्रबंधक (सीआईटी)
DEPUTY MANAGER (CIT)
माझगांव डॉक शिपबिल्डर्स लिमिटेड
MAZAGON DOCK SHIPBUILDERS LIMITED