

THE JUTE CORPORATION OF INDIA LIMITED

(A GOVERNMENT OF INDIA ENTERPRISE)

CIN: U17232WB1971GOI027958



Tender No: JCI/IT/Web/2025-26 dated 07-08-2025

Pre-bid Meeting: 13-08-2025 at 03:00 PM at Patsan Bhavan

Closing date of submission of Bids: 23-08-2025 at 12:00 PM

Opening date of Bids: 25-08-2025 at 12:30 PM

E-Tender for the Development, Deployment, and Maintenance of a Comprehensive Web Portal, Integrated Mobile Applications, and an E-Commerce Platform for The Jute Corporation of India Limited

**The Jute Corporation of India Limited
Patsan Bhavan, 3rd and 4th Floor, Block-CF,
Action Area – 1, New Town,
Kolkata - 700156 India**

Contents

SECTION-I: Introduction	3
SECTION-II: Instructions to Bidders	4
Bid Submission and Compliance.....	4
Earnest Money Deposit (EMD) & Performance Security Deposit (PSD)	4
Pre-Bid Queries.....	5
SECTION-III: Scope of Work.....	6
SCOPE OF WORK.....	6
Technical Scope of Work.....	6
Design & Development Standards:.....	8
Audit Requirements.....	11
Hosting and Server Maintenance	12
Training	13
Documentation:.....	14
Exit Management:	16
Maintenance	17
Timeline:.....	20
Conditions for operational acceptance:.....	22
SECTION-IV: Evaluation Process	24
Evaluation Process	24
Pre-Qualification Criteria	26
Technical Evaluation Framework.....	26
SECTION-V: Terms & Conditions	29
Submission of Document	29
Payment Terms.....	29
General Conditions	31
Indicative List of Required Features to be included in the System	32
SECTION-VI: Service Level Agreement.....	33
TECHNICAL BID FORM.....	37
FINANCIAL BID FORM	40
Annexure - 1	41
Annexure - 2	42

SECTION-I: Introduction

The Jute Corporation of India Limited (JCI) invites bids from NICSI and State Agencies empanelled vendors for the comprehensive design, development, deployment, and maintenance of its integrated digital ecosystem. This ambitious project involves the complete revamp of JCI's public web-portal and the integration of a unified Content Management System (CMS) to manage content across all digital platforms.

The scope of work for this project includes the development of a new web portal with parallax scrolling and a device-neutral, mobile-responsive design, in full compliance with the Government of India's guidelines on web-portals. The solution will also seamlessly integrate a dedicated eCommerce platform for Jute Diversified Products (JDPs) and a secure Employee Portal, all accessible through the CMS.

A key component of this initiative is the modernization and integration of the mobile application suite, including the maintenance of the existing Android application and the launch of a new iOS version of "Paat-mitro". This integrated system will feature a new Farmer Slot Booking Module to significantly reduce waiting times and optimize resource utilization at JCI's purchase centers for raw jute procurement under the Minimum Support Price (MSP) scheme. This module will rely on key integrations with State Land Records, Aadhaar, and geospatial data platforms like ISRO Bhuvan for farmer and crop verification.

The successful bidder will be responsible for developing a solution that adheres to the latest accessibility (WCAG 2.0 Level AA) and security (CERT-in, OWASP Top 10) standards, is hosted on a MeitY Empanelled Cloud Server, and supports bilingual content in English and Hindi. The system must also fulfill all UIDAI requirements for OTP verification, with the selected vendor responsible for ensuring continuous compliance with any future regulatory changes.

Bidders are requested to submit their proposals in a two-bid system (Technical and Financial), exclusively through the Central Public Procurement Portal (CPPP), in accordance with the terms and conditions outlined in this document. The contract will have a maintenance period of three years following successful operational acceptance of the system.

Contact Person

Shri Saptarshi Mukhopadhyay,
Dy. Manager (IT)
The Jute Corporation of India Limited
Patsan Bhavan, 3rd Floor, New Town, Kolkata - 700156
Email: it@jcimail.in

SECTION-II: Instructions to Bidders

Bid Submission and Compliance

The Jute Corporation of India Limited (JCI) has detailed the minimum pre-qualification requirements and the process of selection in the Request for Proposal (RFP). The evaluation committee will evaluate the quality and capability of bidders based on their proposals and fulfilment of the eligibility criteria. Bidders shall submit their offers strictly in accordance with the Terms & Conditions of the RFP document. Any bid that stipulates conditions contrary to the conditions given in the RFP document will be disqualified.

Earnest Money Deposit (EMD) & Performance Security Deposit (PSD)

a) Earnest Money Deposit (EMD)

- 1.1.1 The bidder must upload proof of online payment of an EMD of ₹ 50,000/- (Rupees Fifty Thousands only) with the Technical Bid.
- 1.1.2 Earnest Money Deposit (EMD) should be paid online through NEFT/RTGS. The Bank details of JCI is given below:
Account no.: 0093000100297535
Name of Account: The Jute Corporation of India Limited.
Name of Bank & Branch: PNB, New Town, Rajarhat
IFSC Code: PUNB0143720
- 1.1.3 Bids submitted without the required EMD will be summarily rejected. However, exemption from payment of EMD will be given to Micro, Small & Medium Enterprises (MSMEs) subject to tendered item must be covered under the MSME's Udyam Registration certificate, Startups, Government ministries, departments, government-owned companies and Public Sector Undertakings (PSUs).

b) Refund of EMD

- 1.2.1 The EMD will be refunded to unsuccessful bidders without interest within 30 days after the award of the contract or the tender process is set aside.
- 1.2.2 The successful bidder's EMD will be refunded only after the contract is signed and the Performance Security Deposit (PSD) has been submitted, or upon extension of the EMD as a Bank Guarantee for furnishing the PSD as per Section 1.2.4.

c) Forfeiture of EMD

The EMD will be forfeited if:

- 1.3.1 The bidder withdraws or unilaterally amends their bid after submission or acceptance.
- 1.3.2 The bidder fails to comply with any of the provisions of the terms and conditions in the bid specification.
- 1.3.3 The selected bidder fails to execute the Service Level Agreement (SLA).
- 1.3.4 The selected bidder fails to furnish the Performance Bank Guarantee (PBG) within the prescribed time.
- 1.3.5 The bidder submits the offer with forged documents, alters the RFP terms, or engages in corrupt, coercive, or fraudulent practices.

d) Performance Security Deposit (PSD)

- 1.4.1 The successful bidder shall, within fifteen (15) days of the award of contract, provide a Performance Security Deposit (PSD).
- 1.4.2 Form and Amount of PSD: The PSD shall be in the form of a Bank Guarantee from a Scheduled Commercial Bank in India, equivalent to 5% of the value of the awarded contract.
- 1.4.3 Validity of PSD: The Performance Security must remain valid for a period of 60 days beyond the date of completion of all contractual obligations, including the three-year maintenance period and any warranty obligations.

- e) **Digital Submission (SFMS):** The PBG must be routed through the Structured Financial Messaging System (SFMS) from the issuing bank to JCI's bank account. The physical Bank Guarantee will be considered valid only after the IFN 760 COV Bank Guarantee Advice Message is received. The Bank details of JCI is given below:
Account no.: 0093000100297535
Name of Account: The Jute Corporation of India Limited.
Name of Bank & Branch: PNB, New Town, Rajarhat
IFSC Code: PUNB0143720
- f) **Forfeiture of PSD:** The PSD will be forfeited if the vendor breaches any term and condition of the contract or fails to provide deliverables and fulfill their obligations under the contract. This forfeiture is without prejudice to JCI's right to claim damages or take other actions, such as blacklisting.
- g) **No Interest:** No interest will be paid by JCI on the amount of EMD or PSD.

Pre-Bid Queries

All queries regarding this RFP must be emailed to JCI at it@jcimail.in with the subject line "Pre-bid Queries: RFP for Digital Ecosystem Revamp". Queries received through any other mode, after the 12/08//2025, or without the correct subject line will not be addressed. Interested bidders are required to send email to the id mentioned for pre bid link

SECTION-III: Scope of Work

SCOPE OF WORK

1. Overview

The project encompasses the development of a new Jute Corporation of India Web-portal with Parallax scrolling and a device-neutral, mobile-responsive design, complying with the Government of India's guidelines. The new digital ecosystem will also include a fully integrated eCommerce portal, a secure employee portal, and a modernized mobile application, all managed through a unified Content Management System (CMS).

2. Key Components of the Web Portal:

- a) The web portal will include the following pages and sections:
- b) Home Page with JCI Logo, accessibility icons, and a skip-to-main-content feature.
- c) A language bar for switching between English and Hindi.
- d) Menu list with sections like Home, About JCI, Training & Capacity Building, Partners, Business, Financial, Vigilance, and more.
- e) Dynamic features like a Slider banner, Announcements with new highlights, and live social media feeds.
- f) Essential sections for Minimum Support Price, Public Notice, Contact Us, and Careers.
- g) Functionalities for user counts, last updated date, and access to annual reports, a visit form, and a feedback form.

3. Farmer Slot Booking and Crop Verification System

A comprehensive, multi-channel slot booking system will be developed and integrated to allow registered farmers to book pre-defined time slots for selling raw jute at JCI's Purchase Centers. This system is designed to reduce waiting times, optimize resource utilization, and enhance transparency.

Technical Scope of Work

1. Core Web Portal Development

- a) The website should conform to accessibility standards, specifically WCAG 2.0 level AA compliance and GIGW 3.0 Compliance.
- b) Development will be based on DBIM Toolkit Guidelines.
- c) The website must be bilingual (English, Hindi).
- d) It must be compatible with all major browsers (Firefox, Internet Explorer, Opera, Google Chrome, Safari, etc.).
- e) The design should be contemporary and use the latest techniques to ensure quick loading times.
- f) All user input systems must have a neat and clean Captcha system.
- g) The website must be optimized for Search Engines, including Meta-tags and Dynamic Link Creations.
- h) Sufficient security measures, including hashing and salting passwords, must be applied against vulnerabilities (e.g., hacking, SQL injection) and conform to OWASP Top 10 vulnerabilities.

2. Content Management System (CMS) Integration

- a) The entire website, including the eCommerce and employee portals, will be CMS-based to allow authorized officials to easily maintain content themselves.
 - b) The CMS will provide a single, centralized platform for managing all content across the main website, eCommerce portal, and mobile applications, ensuring consistency and reducing redundant efforts.
 - c) Role-based access will be given to users to upload files and manage content.
3. **Paat-mitro Mobile Application (Android & iOS)**
- The selected bidder will be responsible for the ongoing maintenance and updates of the existing "Paat-mitro" Android mobile application. Additionally, the following scope is added:
- a) Launch of an iOS Version: Develop and maintain a new iOS version of the "Paat-mitro" application, mirroring the functionalities of the Android app and ensuring compliance with all necessary Apple App Store guidelines for hosting and functionality.
 - b) Dynamic Content Delivery: The existing static pages on the mobile application must be replaced. All new and existing content for both the Android and iOS applications will be managed through the CMS and served dynamically via secure APIs, ensuring real-time updates and consistent content across platforms.
 - c) Slot Booking and Management Module: A new module will be developed within the app, serving as the primary channel for farmers to book, view, cancel, and reschedule their time slots.
 - d) Farmer Verification Modules:
 - i. Land Record Verification: The app will be updated to integrate with state-specific land record APIs for real-time verification during farmer registration.
 - ii. Cultivation Verification: A new module will allow farmers to upload geo-tagged and timestamped photographs of their standing jute crop from the field for verification.
 - e) Farmer Dashboard: The application will include a dashboard for farmers to view their Annual Ceiling Limit and track their cumulative sales for the season.
 - f) Notifications: Enhanced SMS and push notification functionality will be implemented for booking confirmations and reminders.
 - g) Assisted Booking and Support: The app will facilitate assisted booking by DPC or CSC operators and provide access to a dedicated helpdesk for technical support.
4. **eCommerce Platform Integration**
- a) The existing JCI e-commerce portal will be fully integrated with the main web portal and its CMS to provide a seamless user experience for Browse and purchasing products.
 - b) The CMS will allow personnel to manage product listings, pricing, and inventory through a unified interface.
 - c) Secure payment gateway integrations must be implemented to support multiple payment options (e.g., credit/debit cards, net banking, UPI) and adhere to industry security standards.
 - d) An Order Management System (OMS) will be developed or integrated to track orders and manage shipments.
 - e) Robust shopping cart and checkout functionalities will be implemented.
5. **ERP Integration**
- a) The web portal will integrate with JCI's in-house Enterprise Resource Planning (ERP) systems to dynamically fetch and display various reports using secure APIs.

- b) The bidder will develop or consume existing APIs to establish a secure connection between the web portal and the ERP system.
 - c) Role-based access controls will govern which users can view specific ERP-generated reports.
6. **Identity and Access Management**
- a) **MS365 LDAP Integration:** A provision for integrating with JCI's Microsoft 365 LDAP/Azure Active Directory will be included to provide secure, centralized user access to the portals, especially for authorized JCI users, leveraging existing corporate credentials. This will streamline user management and enhance security.
 - b) **UIDAI Compliance:** The developed system, including the CMS and mobile application, must adhere to all UIDAI compliance requirements for OTP verification and authentication. The selected bidder will be responsible for implementing necessary updates and changes to ensure continuous compliance with any future revisions or new guidelines issued by UIDAI.

Design & Development Standards:

1. **Compliance with Government Guidelines:** The selected web developer shall follow the design, Development and Technical standards specified in the Guidelines for Indian Government Websites (GIGW) issued and updated from time to time by NIC. The new website, including its integrated eCommerce and employee portals, should be accessible to persons with Disabilities (PwD) as per the guidelines issued by DARPG (GIGW i.e. <https://web.guidelines.gov.in/assets/gigw-manual.pdf>) and W3C (WCAG i.e. <https://www.w3.org/TR/WCAG20/>).
- a) The website should conform to accessibility standards so that it caters to every single citizen irrespective of their disability (WCAG 2.0 level AA compliance)/GIWG 3.0 Compliance.
- b) For compliance in GIGW, the selected bidder has to compliance the new website as per the GIGW standards. The Selected bidder has to provide own certificate for compliance of GIGW standard.
2. **DBIM Toolkit Guidelines:** The website should be developed using DBIM Toolkit Guidelines.
3. **Device Neutrality and Responsiveness (One Web Concept):**
4. The website (including eCommerce and employee portals) must be device neutral / mobile responsive and should adapt to various resolutions, including landscape and portrait orientation.
5. Accessibility across multiple devices (particularly mobile, tablet & Desktop) is crucial.
6. The website should be device agnostic.
7. To improve the experience of the Web on mobile devices and other handheld devices like iPad, tablets etc., the website needs to be developed with “One Web” concept. (One Web means making, as far as is reasonable, the same information and services available to users irrespective of the device they are using).
8. All the websites should be compatible to smartphone devices and should have responsive GUI. The website should adapt to lower resolution such that smartphone users can seamlessly browse the site based on smartphone user experience and Browse behaviour. It

is imperative that the website has evolved to cater to various form factors like smart phones, tablets, desktops and any other handheld devices.

9. **Bilingual Support:** The Website shall be bilingual (English, Hindi). Website will be developed in two different languages (English and Hindi) with an option for the users to switch between the languages. The content for both languages will be provided by department.
10. **Browser Compatibility:** Website should be compatible to all major browsers (i.e. Firefox, Internet explorer, opera, Google Chrome, Safari etc.).
11. **User Interface (UI) and User Experience (UX):**
 - a) Improved site usability through simplified and improved navigation.
 - b) Streamline content to clearly and efficiently convey information of key areas.
 - c) The design should be contemporary in all respects to the extension possible.
12. **Security Measures:**
 - a) Sufficient security measures should be applied against vulnerabilities e.g. hacking / sql-injection-attack etc.
 - b) Any user input system must have captcha system (Captcha must be neat and clean).
 - c) Password should not be hardcoded in any website configuration files or stored in plain text. Passwords should be properly hashed and salted (encrypted) to reduce the effectiveness of password cracking.
 - d) Incorporation of Security features as per the guidelines of empanelment by cert-in and free from OWASP Top 10 vulnerabilities.
 - e) The Website Developer should be responsible for ensuring that all the Software, Plugins, Scripts etc., used for the development of the Website is updated with the latest patches and are free of any known vulnerabilities. The updation of patches should be carried out within 15 days from the date of announcement of the patch by OEM (in case of High Critical Vulnerabilities) and 30 days (in case of other vulnerabilities) in consultation with IT Department, JCI.
13. **Content Management System (CMS) Specifics:**
 - a) This website should be CMS based. Website should be integrated with Content Management System.
 - b) Website should be in specific manner so that authorize official can easily maintain the respective content themselves.
 - c) Role based access to be given to user to perform activities like upload files, create & update the content etc.
 - d) There should be clear distinction in content for authorized user and general public. i.e. Authorized users will be created for the websites by CMS.
 - e) The information on the mobile version should also be managed by content management system - CMS.
 - f) **Unified Content Management:** The CMS shall provide a single, centralized platform for managing all content across the main website, eCommerce portal, and mobile application, ensuring content consistency and reducing redundant efforts.
 - g) **API-Driven Content Delivery for Mobile:** The CMS must be capable of delivering content to the mobile application via secure and high-performance APIs, ensuring efficient and real-time content updates.

- h) **Mobile-Specific Content Adaptation:** The CMS shall include features for content editors to adapt or format content specifically for optimal display and user experience within the mobile application.
 - i) **Content Workflow Management:** Implement robust content workflow management within the CMS, supporting stages such as draft, review, approval, and publishing for all content, including mobile application content.
 - j) **Content Versioning and Rollback:** The CMS should support content versioning, allowing for easy rollback to previous content versions across all managed platforms.
14. **Mobile Application Specifics:**
- a) **Responsive Web Design (RWD) & Web Syndication:** Website must have Web Syndication (RSS/Atoms) and mobile and Tablet Responsive web design (RWD).
 - b) **Mobile Version Content Delivery:** Mobile version should deliver information contextual to the mobile users.
 - c) **Mobile Browser Compatibility:** Mobile website must work on all mobile based browsers such as Opera and Chrome etc.
 - d) **Mobile Website Loading Speed:** Mobile website loading and viewing should be quick by using latest compression system from time to time during contract period.
15. **Performance Optimization:**
- a) Web developer should develop a website with the concept of less web space and memory. So, web pages can load quickly but this shall also accommodate requirement of Department.
 - b) Use of graphics / pictures / animation in a manner that the page should be loaded within least possible time.
16. **Open-Source Software (OSS) Preference:** The Website Developer may strive to use Open-Source Software to design Websites. The use of Open-Source Software should be as per the Framework on Open-Source Software issued by Govt. of India. For selection of Technology, Bidder has to propose the best technology platform for the said website.
17. **Search Functionality:** Website must be optimized for Search Engines (Meta-tags, Dynamic Link Creations, and Dynamic Titles etc.) and search ability within website. Searching facility in the website for internal website search as well as advance search option.
18. **Printer Friendly Pages:** The pages should be printer friendly i.e. all the pages shall be displayed and printed upon demand by user.
19. **User Operating System Compatibility:** User should be able to operate on various Operating Systems like Windows, UNIX, LINUX, etc.
20. **IPv6 and SSL Compliance:**
- a) Website should be IPv6 compliant.
 - b) Website should be running on SSL i.e. http request should automatically get redirected to https. SSL certificate for new website will be provided by the department. The Selected bidder has to install the same on the new website.
21. **Copyright Compliance:** Developer must ensure that, not to violate any copyright law related to images, templates, code etc.
22. **No Third-Party Tracking Scripts:** No Installation of third-party scripts to track user activity ad-scripts, hidden back links to other irrelevant website.

Audit Requirements

1. **Website Security Audit:**

The website should be hosted and released only after undergoing the Website Security Audit as per the guidelines of Government of India and obtaining a Security Audit Clearance certificate from CERT-in empanelled IT Security Auditors. The web developer should be responsible to fix the vulnerabilities found even after the hosting is completed till the completion of its contract period with The Jute Corporation of India Limited. This audit will cover:

- a) **Vulnerability Assessment & Penetration Testing (VAPT):** Comprehensive testing to identify security vulnerabilities, including those related to SQL injection, cross-site scripting (XSS), broken authentication, and other common web application flaws.
- b) **Configuration Review:** Assessment of server, network, and application configurations to ensure they adhere to security best practices.
- c) **Code Review:** Examination of the source code for security flaws and adherence to secure coding standards.
- d) **Compliance with OWASP Top 10:** Ensuring the website is free from the OWASP Top 10 vulnerabilities.
- e) **Data Privacy Compliance:** Audit of data handling practices to ensure compliance with relevant data privacy regulations and JCI's privacy policy.

2. **Functional Audit:**

A comprehensive functional audit shall be conducted to verify that all features and functionalities of the website, eCommerce portal, employee portal, and mobile application perform exactly as specified in the Scope of Work and user requirements. This includes:

- a) **User Acceptance Testing (UAT):** Formal testing with JCI stakeholders to ensure the system meets business requirements and user expectations.
- b) **Workflow Testing:** Verification of all automated and manual workflows, such as content publishing workflows, order processing, and employee self-service processes.
- c) **Content Integrity Audit:** Verification that all content is displayed correctly, is up-to-date, and maintains integrity across the website, e-commerce, employee portal, and mobile application.
- d) **Bilingual Functionality Audit:** Testing of the language switching functionality and ensuring all content is correctly translated and displayed in both English and Hindi.
- e) **Accessibility Audit:** Verification of WCAG 2.0 level AA compliance and GIGW 3.0 Compliance to ensure the platform is accessible to persons with disabilities.

3. **Payment Gateway Integration Audit:**

For the integrated eCommerce portal, specific audits related to the payment gateway shall be conducted:

- a) **PCI DSS Compliance Assessment:** Verification that the payment gateway integration and handling of cardholder data comply with Payment Card Industry Data Security Standard (PCI DSS) requirements. While JCI may not directly store card data, the integration process must ensure secure transmission.
- b) **Transaction Security Audit:** Review of the entire transaction flow from product selection to payment confirmation, ensuring encryption, fraud detection mechanisms, and secure communication protocols are in place.

- c) **Data Integrity of Financial Transactions:** Audit to confirm that all financial transaction data (order details, payment status) is accurately captured and reconciled with the ERP system.
- d) **Error Handling and Reversal Mechanisms:** Testing of error handling during payment failures and the implementation of secure and auditable transaction reversal/refund processes.
- 4. **Third-Party Integration Security:** Assessment of the security posture of the third-party payment gateway provider and the integrity of the API connections between JCI's system and the payment gateway.

Hosting and Server Maintenance

- 1. **Hosting Environment for New Systems:**
 - a) During the development and security audit phase, the Bidder must host the services from its own testing server.
 - b) In the Go-live phase, Bidder will have to manage and roll out a beta stage where the system will be made available and restricted only to the users in the department through an appropriate mechanism on the web.
 - c) After the successful completion of the security audit, the new web portal (including the integrated eCommerce and employee portals) and the mobile application backend must be transferred and hosted in a MeitY Empanelled Cloud Server.
- 2. **Interim Hosting for Existing WordPress Website:**

The bidder shall manage the hosting of the current WordPress website until the successful launch and operational acceptance of the new web portal. This involves ensuring continuous uptime, sufficient bandwidth, and a secure server environment for the existing site. Details regarding the current hosting provider and access credentials will be provided by JCI.
- 3. **Server Specifications and Scalability:**
 - a) The hosting environment for all components (web portal, eCommerce, employee portal, mobile app backend) must be robust, scalable, and capable of handling anticipated user traffic and data load.
 - b) The infrastructure should allow for future expansion and increased capacity without significant disruptions.
 - c) The bidder should propose the best technology platform for the said website, which implicitly includes the underlying hosting infrastructure.
- 4. **Security of Hosting Environment:**
 - a) The hosting environment must adhere to high security standards, including physical security, network security (firewalls, intrusion detection/prevention), and data encryption.
 - b) Regular security patching and vulnerability management of the server infrastructure are mandatory.
 - c) The website should be hosted and released only after undergoing the Website Security Audit as per the guidelines of Government of India and obtaining a Security Audit Clearance certificate from CERT-in empanelled IT Security Auditors.
- 5. **Data Backup and Recovery:**

- a) Implement comprehensive data backup and disaster recovery mechanisms for all hosted data and applications. This includes regular backups (daily/weekly/monthly as per criticality) and a defined recovery point objective (RPO) and recovery time objective (RTO).
 - b) Backup strategies should cover the website content, databases (for all portals), and the mobile application backend data.
- 6. Uptime and Performance:
 - a) The hosting provider must guarantee a high level of uptime (e.g., 99.5% or higher) for all hosted services.
 - b) The server performance should ensure quick loading times for web pages and efficient data retrieval for the mobile application.
- 7. Server Maintenance and Monitoring:
 - a) During operation and maintenance phase, Service Provider's onsite team should coordinate with JCI in order to ensure that the website is functioning as per standard norms.
 - b) The bidder will be responsible for continuous monitoring of server health, resource utilization, and performance, along with proactive incident management.
 - c) Regular maintenance tasks, including operating system updates, software patching, and log management, are to be performed.
- 8. SSL Certificate Management:
 - a) The website should be running on SSL i.e. http request should automatically get redirected to https.
 - b) SSL certificate for new website will be provided by the department. The Selected bidder has to install the same on the new website. The bidder is responsible for the proper installation and configuration of the SSL certificate.
- 9. Domain Name System (DNS) Management:

The bidder will assist JCI with DNS configuration and management to point domain names to the hosted servers.

Training

- 1. Overview of the Website and Integrated Portals:

The successful bidder shall provide an overview of the entire digital ecosystem, including the main web portal, eCommerce portal, and employee portal, to all departmental users. This training should cover the overall structure, navigation, and key functionalities.
- 2. Detailed Technical Demonstration:

A detailed technical demonstration will be provided to the nodal officer(s) of The Jute Corporation of India Limited on:

 - a) Website administration, including server-side configurations and deployment procedures.
 - b) Backend management of the eCommerce portal.
 - c) Backend management of the employee portal.
 - d) Management of the mobile application backend and its content delivery mechanisms (APIs).
- 3. CMS Tools Training:

Comprehensive training will be provided to the nodal officer(s) and other designated officials of JCI on the Content Management System (CMS) tools. This training should cover:

- a) Content creation, editing, publishing, and archiving for the main website.
 - b) Product listing, inventory management, order processing, and promotional activities for the eCommerce portal.
 - c) Employee data management, internal announcements, and relevant content updates for the employee portal.
 - d) Managing and publishing content specifically for the mobile application, including understanding mobile content formatting and API-driven publishing workflows.
 - e) User management and role-based access control within the CMS.
 - f) Content workflow management within the CMS (draft, review, approval, publish).
 - g) Managing bilingual content.
4. **ERP Integration Report Management Training:**
Training on how to access, interpret, and manage the display of ERP-generated reports on the website through the CMS, including understanding data refresh mechanisms.
 5. **Audit Report Interpretation Training:**
Training on how to understand and interpret security audit reports, functional audit reports, and payment gateway integration audit reports, including identifying and tracking vulnerability resolutions.
 6. **Training Logistics:**
 - a) Approximately 10 officials need to be trained.
 - b) Training will need to be provided at a single location within JCI facilities.
 7. All necessary arrangements like projector and training space will be given by JCI.

Documentation:

The project team shall provide the following documentations in hard as well as soft copies:

1. **Detail Project Plan:** Comprehensive project plan outlining timelines, milestones, resource allocation, and key deliverables.
2. **Fortnightly Progress Reports:** Regular updates on project status, challenges, and upcoming tasks.
3. **System Requirement Specification (SRS) Document:** A detailed document containing comprehensive requirement capture and analysis, including:
 - a) Functional requirements for the website, eCommerce portal, employee portal, and mobile application.
 - b) Non-functional requirements (performance, scalability, security, usability).
 - c) Interface Specifications (internal and external APIs, particularly for ERP and payment gateway integration).
 - d) Application security requirements for all integrated platforms.
4. **Complete Source Code with Required Documentation:**
 - a) The source code (published and unpublished) of the website, eCommerce portal, employee portal, and mobile application backend shall be provided.

- b) The source code supplied to the Department shall at all times be a complete, accurate, and up-to-date copy corresponding exactly to the current production release of the software.
 - c) Version Control System Documentation: Documentation detailing the version control system used during development (e.g., Git), including branching strategies, commit guidelines, and how to access and retrieve specific versions of the code. All code changes should be tracked through this system.
 - d) In-code documentation (comments) and separate technical design documents explaining the architecture, modules, algorithms, and database schema for all integrated systems.
5. User Manuals:
- a) Two sets of User manuals (i.e. two hard & soft copies in English language and hard & soft copies in Hindi language) for administration and management of the entire web portal, eCommerce portal, and employee portal.
 - b) Specific user manuals for content management within the CMS, including mobile application content.
 - c) Manuals for managing the payment gateway and order processing.
6. Test Plans and Test Cases:
- a) Unit Test Plan.
 - b) System/Integration Test Plan (covering integration points between website, eCommerce, employee portal, mobile app backend, ERP, and payment gateway).
 - c) User Acceptance Test Plan (UAT).
7. Test Reports:
- a) Test report w.r.t. functionality of all components.
 - b) Compliance to W3C Standard & WCAG2.0 level AA.
 - c) Reports for functional audits conducted on the website, eCommerce, employee portal, and mobile application.
8. Security Audit Reports and Clearance Certificates:
- a) Original security Audit report and Clearance Certificate from CERT-in empanelled IT Security Auditors for the entire platform.
 - b) Reports from Payment Gateway Integration Audit, including PCI DSS compliance assessment.
9. Training Manuals and Literature: Comprehensive materials that will include all details pertaining to:
- a) System Administration (for all components).
 - b) CMS Tool usage for all content types and platforms.
 - c) Website, eCommerce, and Employee Portal Users.
 - d) Installation procedures.
 - e) Operations and Maintenance procedures.
 - f) Security policy and procedures for the website, including Password security, logical access security, operating system security, data classification, application security, and data backups.
10. Deployment and Release Notes:
Documentation detailing the deployment process, configuration steps, and release notes for each major version of the software.
11. Technical Architecture Document:

A comprehensive document outlining the overall system architecture, technology stack used, and interdependencies of various components (website, eCommerce, employee portal, mobile app backend, ERP integration, payment gateway).

12. **Database Schema Documentation:**

Detailed documentation of all database schemas, including tables, relationships, and data dictionaries for all relevant databases.

Exit Management:

1. **Identification of Existing Assets and Documentation:**

- a) The successful bidder, in coordination with JCI, will work with the existing website and mobile application vendors to identify and obtain all relevant assets, including:
- b) All source code (published and unpublished) for the current website and mobile application.
- c) Database backups and schemas for both the website and mobile application.
- d) All necessary documentation (technical specifications, user manuals, administrative guides) for the current website and mobile application.
- e) Hosting credentials and server configurations for the existing website.
- f) Google Play Store (and Apple App Store, if applicable) developer account access and application signing keys.
- g) Any third-party licenses, APIs, or integrations used by the existing systems.
- h) Domain registration details and DNS configurations.
- i) Historical data, including user statistics, content archives, and previous audit reports.

2. **Knowledge Transfer and Training:**

- a) The successful bidder shall facilitate and participate in comprehensive knowledge transfer sessions with the incumbent vendors to understand the architecture, functionalities, and maintenance procedures of the existing website and mobile application.
- b) This includes understanding any custom code, specific configurations, and operational workflows.

3. **Data Migration Strategy (if applicable):**

If any data from the existing website or mobile application (e.g., user profiles, historical content, specific reports) needs to be migrated to the new web portal or mobile application backend, the bidder shall propose a detailed data migration strategy, including:

- a) Data identification and cleansing.
- b) Migration tools and methodologies.
- c) Data validation and reconciliation post-migration.
- d) Downtime planning for migration, if necessary.

4. **Transition Timeline and Milestones:**

Develop a clear timeline for the exit process, including key milestones for asset handover, knowledge transfer, and eventual decommissioning of the old systems. This timeline should be coordinated with the launch plan of the new system.

5. **Decommissioning Plan:**

Outline a plan for the secure decommissioning of the old website and mobile application infrastructure, ensuring all sensitive data is securely wiped or archived as per JCI's data retention policies.

6. **Coordination with Incumbent Vendors:**

The successful bidder will actively coordinate with the incumbent vendors, under JCI's guidance, to ensure their full cooperation in the exit process, including providing all requested information and access in a timely manner.

7. **Support during Transition:**

8. Provide necessary support and troubleshooting during the transition period to ensure minimal disruption to JCI's operations and public access.

Maintenance

The major activities covered for the existing website (until launch of new), new website, eCommerce portal, and mobile application are as under:

1. **Interim Support for Existing WordPress Website:** The operation and maintenance activities will extend to the current WordPress website, including resolution of any errors/bugs, addressing security vulnerabilities specific to the WordPress platform, and ensuring data integrity, until the successful launch and operational acceptance of the new web portal.
2. **Interim WordPress Plugin and Theme Management:** The bidder will be responsible for periodically updating and managing all plugins and themes used on the existing WordPress website, ensuring compatibility and security, until the successful launch and operational acceptance of the new web portal.
3. **Maintenance of Existing Android Mobile Application "Paat-Mitro"**
 - a) Proactive Monitoring and Performance Optimization:
 - i. Implement continuous monitoring of the "Paat-Mitro" app's performance, including crash analytics, ANRs (Application Not Responding) rates, and overall user engagement metrics.
 - ii. Proactively identify and resolve performance bottlenecks, optimize app loading times, and reduce memory footprint to ensure a smooth user experience.
 - b) Feature Enhancements & Bug Resolution:
 - i. Address and resolve any existing or newly identified bugs, glitches, or functional issues within the Android application.
 - ii. Implement minor feature enhancements or adjustments to improve usability and align with user feedback, as agreed upon with JCI.
 - c) Security Updates and Vulnerability Management:
 - i. Regularly apply security patches and updates to the Android application to protect against emerging threats and vulnerabilities.
 - ii. Conduct periodic security audits specific to the mobile application to identify and remediate any potential security flaws.
 - d) API and Backend Synchronization Monitoring:
 - i. Continuously monitor the integration between the "Paat-Mitro" app and its backend (which is integrated with the new web portal's CMS), ensuring seamless data synchronization and API performance.
 - ii. Troubleshoot and resolve any data integrity or synchronization issues that may arise.

- e) Android OS Version Compatibility:
 - f) Ensure the "Paat-Mitro" app remains compatible with new Android operating system versions as they are released, performing necessary updates and testing to maintain functionality across a wide range of devices.
4. **Regular Updation & Maintenance:**
- a) Content Updates: Regular updates and maintenance based on requests from the department. Website content should be updated at least once in 15 days. If the maintenance agency does not get any intimation about the updation from the department, they have to proactively ask the department for the same. Website content should be updated in consultation with the concerned authority, which will be informed from time to time. This applies to all content across the main website, eCommerce portal (product information, pricing), employee portal (internal notices, documents), and mobile application.
 - b) Announcement Management: Mechanism is in place to ensure that all outdated announcements are removed from the website or moved to archive.
 - c) Data Integrity: Ensuring the accuracy and consistency of all data across the web portal, eCommerce portal, employee portal, and mobile application, including data synchronized from the ERP system.
5. **Software Updates and Patch Management:**
- a) The successful bidder shall maintain and support the supplied software (Website) for a period of 3 years after the successful operational acceptance.
 - b) Providing all software updates and patches released by the OEM, update and patch management, resolution of any issues / problems with the software etc..
 - c) The Website Developer should be responsible for ensuring that all the Software, Plugins, Scripts etc., used for the development of the Website is updated with the latest patches and are free of any known vulnerabilities.
 - d) The updation of patches should be carried out within 15 days from the date of announcement of the patch by OEM (in case of High Critical Vulnerabilities) and 30 days (in case of other vulnerabilities) in consultation with composite team of NIC.
 - e) This includes updates for the CMS, operating systems, web server software, database systems, security components, and any third-party libraries or frameworks used in the development of the new website, eCommerce portal, employee portal, and mobile application backend.
 - f) For the existing WordPress website (until launch of new), this includes WordPress core updates, theme updates, and plugin updates.
6. **Bug Resolution and Error Management:**
- a) Resolution of errors/bugs (if any) identified in the new website, eCommerce portal, employee portal, or mobile application.
 - b) The web developer should be responsible to fix the vulnerabilities found even after the hosting is completed till the completion of its contract period with The Jute Corporation of India Limited.
 - c) For the existing WordPress website (until launch of new), resolution of any bugs or functional issues detected.
7. **Performance Monitoring and Optimization:**
- a) Regular monitoring and assessment to ensure content authentication and updation.

- b) Continuous monitoring of server health, resource utilization (CPU, memory, disk I/O, network bandwidth), and application performance (page load times, API response times) for all hosted components.
 - c) Proactive identification and resolution of performance bottlenecks.
 - d) Optimization of database queries, code, images, and other assets to ensure quick loading times and efficient operation.
 - e) Ensuring mobile website loading and viewing is quick by using latest compression system from time to time during contract period.
8. **Security Monitoring and Management:**
- a) Continuous monitoring for security threats, anomalies, and potential breaches.
 - b) Regular security audits and vulnerability assessments (VAPT) as per schedule.
 - c) Immediate response and remediation of any security incidents or identified vulnerabilities.
 - d) Adherence to all government security guidelines and best practices.
9. **Backup and Disaster Recovery Management:**
- a) Implementation and ongoing management of robust data backup and recovery procedures for all website content, databases, and application files.
 - b) Regular testing of backup restoration processes to ensure data integrity and system recoverability.
10. **Server and Hosting Environment Maintenance:**
- a) Ensuring that the website is functioning as per standard norms.
 - b) Periodic updates and maintenance of the MeitY Empanelled Cloud Server environment, including OS patching, security configurations, and resource scaling as needed.
 - c) For the existing WordPress website (until launch of new), management and maintenance of its current hosting environment to ensure stability and performance.
11. **Third-Party Integrations Maintenance:**
- a) Monitoring the stability and performance of integrations with ERP systems, payment gateways, and social media platforms.
 - b) Troubleshooting data synchronization issues and ensuring accurate data flow between integrated systems.
 - c) Addressing any updates required due to changes in third-party APIs or services.
12. **Compliance Monitoring:**
- a) Ongoing verification of compliance with GIGW Guidelines, WCAG 2.0 Level AA, and other relevant government standards for all platforms.
 - b) Ensuring adherence to Google Play Store, Apple App Store policies for the mobile application.
 - c) Monitoring PCI DSS compliance for the eCommerce portal's payment gateway integration.
13. **Reporting and Analytics:**
- a) Web developer should be responsible to provide detailed web statistics report as and when required to the concerned officials in written or through e-mail after full-fledged Development of website.
 - b) As per the Government Guidelines, the selected bidders may or may not use Google analytics for generating the Web statistics reports. Department may require permission

from GSDC to use google analytics. In case of deny by GSDC, Bidder has to propose the best solution for web statistics report.

- c) This includes reporting on user counts (daily, weekly, monthly, yearly).
- d) Provide analytics and performance reports for the mobile application, including crash reports and user engagement data.

14. Dedicated Project Management:

Successful bidder shall provide a dedicated project manager (though not required to be deployed full time) during the period of the contract that should be present for discussions, important meetings and should act as one- point contact for JCI.

15. Resources for Maintenance:

Resources (need not be onsite) for maintenance of Website.

16. Maintenance Period and Review Cycle:

The maintenance period for the new web portal (including the integrated eCommerce and employee portals) and the mobile application backend will be **3 years after successful operational acceptance.**

Reviews of the maintenance activities, performance, and compliance will be conducted on a half-yearly basis. These reviews will assess:

- a) Content authentication and updation frequency.
- b) Resolution of errors/bugs and security vulnerabilities.
- c) Performance metrics and optimization efforts.
- d) Security monitoring and adherence to government guidelines.
- e) Backup and disaster recovery management effectiveness.
- f) Server and hosting environment maintenance, including OS patching and security configurations.
- g) Stability and performance of third-party integrations (ERP, payment gateways, social media).
- h) Ongoing compliance with GIGW Guidelines, WCAG 2.0 Level AA, Google Play Store policies, and PCI DSS.
- i) Accuracy and availability of web statistics and analytics reports.

The half-yearly reviews will involve JCI officials and the dedicated project manager from the successful bidder. Any findings or recommendations from these reviews will be addressed within an agreed-upon timeframe.

Timeline:

Tentative Timeline for JCI Web Portal & Integrated Systems Development

1. Phase 1: Planning & Setup (Month 1: Weeks 1-2)

a) Week 1:

- i. **Exit Management of Old Contracts:** Formalize the exit from previous vendors, ensuring all assets are transferred and old systems are decommissioned securely.
- ii. **Existing Systems Audit & Documentation Collection:** Begin collaboration with existing website and mobile application vendors for asset identification, documentation collection (source code, databases, credentials), and initial knowledge transfer.

- iii. **MeitY Empanelled Cloud Server Transfer:** Transfer the existing website and mobile application CMS to the designated MeitY Empanelled Cloud Server.
 - iv. **Project Kick-off Meeting:** Detailed discussions with JCI stakeholders to finalize requirements, understand existing systems, and establish communication protocols.
 - v. **Requirement Refinement & SRS Finalization:** Deep dive into all functionalities for the new website, eCommerce portal, employee portal, and mobile application backend. Finalization of System Requirement Specification (SRS) document.
 - vi. **Technology Stack Proposal & Approval:** Bidder proposes the best technology platform for the website and integrated portals, for JCI's approval.
- b) **Week 2:**
- i. **Detailed Project Plan Submission:** Bidder submits the Detail Project Plan, including revised timelines and resource allocation.
 - ii. **Interim WordPress & Mobile App Maintenance Setup:** Bidder takes over interim maintenance and hosting responsibilities for the existing WordPress website and mobile application.
 - iii. **Environment Setup:** Set up development and testing environments on the bidder's premises.
- 2. Phase 2: Design & Development (Month 1: Weeks 3-4 & Month 2: Weeks 1-4)**
- a) **Week 3-4 (Month 1):**
- i. **Macro & Micro Level Design:** Initiate macro-level and micro-level design of the new website, eCommerce portal, and employee portal, ensuring contemporary aesthetics and adherence to GIGW, WCAG 2.0, and DBIM Toolkit guidelines.
 - ii. **UI/UX Prototyping:** Development of wireframes and mock-ups for all portal sections, including mobile application interfaces, for JCI review and approval.
 - iii. **Database Design & Architecture:** Design and implementation of the database schema for the new integrated system.
 - iv. **CMS Setup & Core Development:** Initial setup and configuration of the Content Management System (CMS).
- b) **Month 2 (Weeks 1-4):**
- i. **Modular Development (Concurrent):**
 - ii. **Website Core Development:** Building out the main website functionalities, parallax scrolling, language bar, navigation, and static content sections.
 - iii. **eCommerce Portal Development:** Implementation of product listings, shopping cart, checkout process, and secure payment gateway integration.
 - iv. **Employee Portal Development:** Development of internal content sections, role-based access, and employee-specific functionalities.
 - v. **Mobile Application Backend Development:** Development of APIs for content delivery to the mobile application and integration with the centralized CMS.
 - vi. **ERP API Integration:** Development/consumption of APIs for integrating with JCI's in-house ERP system for reports.
 - vii. **Bilingual Content Integration:** Begin integration of English and Hindi content provided by JCI.
 - viii. **Fortnightly Progress Reports:** Submission of progress reports to JCI.
- 3. Phase 3: Testing & Audits (Month 3: Weeks 1-2)**
- a) **Week 1-2 (Month 3):**

- i. **Unit & Integration Testing:** Comprehensive testing of all developed modules and their interconnections (website, eCommerce, employee portal, mobile app backend, ERP integration, payment gateway).
 - ii. **System Testing:** End-to-end system testing to ensure all functionalities work as per SRS.
 - iii. **Accessibility Testing:** Verification against WCAG 2.0 Level AA and GIGW compliance.
 - iv. **Initial Security Audit Preparation:** Prepare the system for formal security audits.
 - v. **Payment Gateway Integration Audit (Preliminary):** Initial checks and internal audits for PCI DSS compliance aspects.
 - vi. **Phase 4: UAT, Final Audits & Deployment (Month 3: Weeks 3-4)**
- b) **Week 3 (Month 3):**
- i. **User Acceptance Testing (UAT) - Beta Stage:** Release a beta version to JCI users for UAT based on bidder-developed test cases validated by JCI.
 - ii. **Functional Audit:** Conduct a comprehensive functional audit based on UAT feedback and requirements.
 - iii. **Security Audit by CERT-in Empanelled Auditors:** Initiate the formal security audit process.
 - iv. **Bug Fixing & Iteration:** Address issues identified during UAT and functional audit.
- c) **Week 4 (Month 3):**
- i. **Final Bug Fixing & Optimization:** Rectify all remaining issues.
 - ii. **Security Audit Clearance Certificate:** Obtain the Security Audit Clearance certificate from CERT-in empanelled IT Security Auditors.
 - iii. **MeitY Empanelled Cloud Server Transfer:** Transfer the developed system to the designated MeitY Empanelled Cloud Server.
 - iv. **Operational Acceptance & Official Launch:** Upon JCI's complete satisfaction and successful operational acceptance, the department website will be officially launched and operational acceptance will be complete.
 - v. **Source Code Handover:** Relinquish the source code of the developed Website within Five (5) days from the date of acceptance of the system.
 - vi. **Documentation Submission:** Submit all required documentation (SRS, source code, manuals, test reports, audit reports).
4. **Post-Launch: Maintenance & Training (Ongoing after Month 3)**
- a) **Training Delivery:** Conduct training sessions for JCI officials on website administration, CMS usage (for all portals), and ERP report management.
 - b) **Operations & Maintenance Phase:** Begin the 1-year maintenance period, including bug resolution, software updates, content updates (at least once in 15 days), performance monitoring, and security management.

This timeline is tentative. Actual durations may vary based on the complexity of specific features, JCI's feedback cycles, and the efficiency of collaboration with existing vendors.

Conditions for operational acceptance:

Operational acceptance for the integrated website with e-commerce portal, employee portal and mobile application will be complete upon:

1. **Successful Security Audit and Clearance Certificate:** Obtaining a Security Audit Clearance certificate from CERT-in empanelled IT Security Auditors for the entire platform. The website should be hosted and released only after undergoing this audit.
2. **Successful Functional Audit:** Completion of a comprehensive functional audit, verifying that all features and functionalities of the website, eCommerce portal, employee portal, and mobile application perform exactly as specified in the Scope of Work and user requirements. This includes User Acceptance Testing (UAT), workflow testing, content integrity, bilingual functionality, and accessibility compliance.
3. **Successful Payment Gateway Integration Audit:** For the integrated eCommerce portal, specific audits related to the payment gateway must be conducted, including PCI DSS Compliance Assessment, Transaction Security Audit, Data Integrity of Financial Transactions, Error Handling and Reversal Mechanisms, and Third-Party Integration Security. Reports from this audit are required.
4. **Resolution of Identified Issues:** All bugs identified during UAT and functional audits must be rectified. The web developer is responsible for fixing vulnerabilities found even after hosting until the completion of the contract period.
5. **MeitY Empanelled Cloud Server Transfer:** The developed system (new web portal, integrated eCommerce and employee portals, and mobile application backend) must be transferred and hosted on a MeitY Empanelled Cloud Server.
6. **Source Code Handover:** Relinquishing the complete source code (published and unpublished) of the website, eCommerce portal, employee portal, and mobile application backend within five days from the date of system acceptance. This includes ensuring the supplied code is a complete, accurate, and up-to-date copy corresponding to the current production release, along with version control system documentation and in-code documentation.
7. **Documentation Submission:** Submission of all required documentation, including the System Requirement Specification (SRS) Document, User Manuals, Test Plans and Test Cases, Test Reports, Security Audit Reports and Clearance Certificates, Training Manuals and Literature, Deployment and Release Notes, Technical Architecture Document, and Database Schema Documentation.
8. **JCI's Complete Satisfaction:** Official launch and operational acceptance will occur upon JCI's complete satisfaction.

SECTION-IV: Evaluation Process

Evaluation Process

JCI shall constitute a Tender Evaluation Committee to evaluate the responses of the bidders. The Tender Evaluation Committee shall evaluate the responses to the RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence by bidders may lead to rejection of their bids.

The decision of the Tender Evaluation Committee in the evaluation of bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee. The Tender Evaluation Committee may ask for meetings or presentation with the Bidders to seek clarifications or conformations on their bids.

The Tender Evaluation Committee reserves the right to reject any or all bids. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP. The steps for evaluation are as follows:

a) Stage 1: Pre-Qualification

- i. A pre-qualification criterion will be applied to short-list the bidders for technical and financial evaluation.
- ii. Technical and Financial bids for those bidders who don't pre-qualify will not be opened. Financial bid will not be opened for those bidders, who don't qualify the technical evaluation.

b) Stage 2: Technical Evaluation

- i. "Technical bid" will be evaluated only for the bidders who succeed in Stage 1.
- ii. JCI will review the technical bids of the short-listed bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at JCI's discretion.
- iii. The bidders' technical solutions proposed in the bid document shall be evaluated as per requirements specified in RFP and technical evaluation framework as mentioned in Section below.
- iv. Bidders submit in detailed – "Approach & Methodology & Solutions proposed "
- v. Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only the bidders who get an Overall Technical score of 70 will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid.

c) Stage 3: Commercial Evaluation

- i. All technically qualified bidders will be notified to participate in Commercial Bid opening process.
- ii. Commercial bids for the technically qualified bidders shall then be opened on the notified date and time and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at JCI's discretion.
- iii. Commercial Bids that are not as per the format provided shall be liable for rejection.

- iv. **Normalized Commercial Score of a Bidder = {Lowest TCB/ Bidders TCB} X 100 (adjusted to 2 decimals)**

Example:

Bidders	Total Cost of Bid	Calculation	Normalized Commercial Score
Bidder-1	110	$(110/110)*100$	100
Bidder-2	140	$(110/140)*100$	78.57
Bidder-3	160	$(110/160)*100$	68.75
Bidder-4	130	$(110/130)*100$	84.61
Bidder-5	150	$(110/150)*100$	73.33

The bidder that has quoted the lowest Total Price (Capex price + Opex price) shall be treated as L1. The bid price shall include all taxes and levies and shall be in Indian Rupees and mentioned separately.

d) Stage 4: Final score calculation through QCBS

The final score will be calculated through Quality and Cost selection method based with the following weightage:

Technical: 60%

Commercial: 40%

Final Score = (0.60* Technical Score) + (0.40* Normalized Commercial Score)

Example:

Bidders	Technical score	Normalized commercial score	Final Score (60:40)
Bidder-1	80	100	88.00
Bidder-2	100	80	92.00
Bidder-3	90	90	90.00

The bidder with the highest Final score shall be treated as the Successful bidder. In the above example, Bidder-4 will be treated as successful bidder.

In the event the Final scores are 'tied', the bidder securing the highest technical score will be adjudicated as the Best Value Bidder for award of the Project.

The JCI has detailed the minimum pre-qualification requirements and the process of selection in the RFP. The evaluation committee will evaluate the quality / capability of Bidders on the criteria mentioned in the RFP based on their proposals received and fulfilment of eligibility criteria.

The bidders shall submit their offers strictly in accordance with the Terms & Conditions of the RFP document. Any bid that stipulates conditions contrary to the conditions given in the RFP document will stand disqualified.

Pre-Qualification Criteria

No	Criteria	Submission
1	The bidder should be empanelled with NICSI or any other state agencies for providing “Application & Website Development” service	Copy of valid empanelment certificate
2	The Bidder should be a company registered in India under the Companies Act, 2013 or a partnership/proprietor firm registered under the Indian Partnership Act 1932 or LLP registered under LLP Act 2008 with their registered office in India for at least 7 years before date of submission of Bid	Copy of Certificate of Incorporation/ Registration / MoA as applicable
3	The bidder should be profit making and shall have positive net worth in each of last 3 financial years (2022-23, 2023-24 & 2024-25)	Audited balance sheet Statement
4	The Bidder should not have been blacklisted by any Central and/or State Government departments, PSU's and/or any other Statutory or autonomous body/undertaking.	No Conviction Certificate to be submitted on behalf of the Bidder as well as its Directors/Partners/Founders, duly signed on the Agencies Letter Head and Stamped.
5	The Bidder should have a valid and active PAN and GST in India	Copy of PAN card and Goods & Service Tax Registration certificate
6	Technical Expertise & Experience: The bidder must demonstrate proven experience in the following areas: a) Developing and maintaining websites in compliance with GIGW 3.0 and WCAG 2.0 Level AA accessibility standards. b) Implementing a CMS-based system that can manage content for a main website, an eCommerce portal, and a mobile application from a single platform. c) Developing and managing both Android and iOS mobile applications , ensuring compliance with app store hosting guidelines. d) Integrating secure eCommerce portals with payment gateways that adhere to industry security standards. e) Implementing secure Application Programming Interfaces (APIs) for data synchronization and content delivery.	Detailed list of relevant projects completed in the last 5 years, with client references and a brief description of the scope, including specific technologies used and compliance achieved. In addition, provide at least <u>3 (three) client testimonials or letters of recommendation</u> from similar projects.
7	Human Resources & Documentation Capability: The bidder must have the capacity to provide a dedicated project manager and a qualified technical team for the project duration. The bidder must also have a proven track record of providing comprehensive documentation and training.	Resumes of the proposed Project Manager and key technical personnel, along with sample documentation (e.g., SRS, User Manuals) from previous projects.

Technical Evaluation Framework

Clause	Criteria / Sub-Criteria	Marking Systems	Maximum Marks
1	The Bidder should possess following valid certifications <ul style="list-style-type: none"> ISO 9001:2008 or higher ISO 27001 or Higher 	Any 1 Certificate = 2 Marks Any 2 Certificates = 4 Marks All 3 Certificates = 5 Marks	5 Marks

	<ul style="list-style-type: none"> • CMMi3 or Higher 		
2	Relevant Project Experience The bidder should have experience in providing customised web portals and integrated digital platforms (directly or indirectly) for Central/State Government/PSUs/Statutory bodies in the last 5 years prior to the bid submission date. The value of each project should be at least ₹20 lakhs . The projects must demonstrate experience with: a) Large-scale web portal development with CMS integration b) eCommerce portal integration c) Mobile application development (Android/iOS) and CMS integration	1 Project = 5 Marks 2-3 Projects = 15 Marks 4-5 Projects = 25 Marks Above 5 Projects = 30 Marks	30 Marks
3	Average annual turnover for last 3 financial year ending 2023-24	Upto ₹50 Crore = 5 marks ₹51 Crore – 200 Crore = 10 marks Above ₹200 Crore = 15 marks	15 marks
4	Approach & Methodology a) Understanding of the Project requirement based on the RFP and Scope of Work. b) Identified project risks and a comprehensive Mitigation plan. c) Customized Approach & Methodology based on local State conditions, especially for farmer verification. d) Detailed Work plan and Gantt Chart for project execution.	a. Understanding: 5 marks b. Risk & Mitigation plan: 5 marks c. Localized Approach & Methodology: 5 marks d. Detailed Work plan: 5 marks	20 Marks
5	Technical Presentation A presentation covering the following aspects: a) Company profile and past experience. b) Proposed technology stack for the project (e.g., preference for OSS). c) Proposed process of quality assurance and adherence to development standards. d) Proposed innovation and deployment of new-age technology like AI/ML for enhanced search or analytics.	Based on the quality and depth of the presentation and its alignment with JCI's vision.	15 Marks
6	Specific Technical Integrations & Compliance Experience The bidder's experience in developing software solutions for Central/State Government/PSUs involving any two of the following integrations: a) UIDAI/Aadhaar OTP verification.	1 Integration = 3 Marks 2-3 Integrations = 6 Marks 4-5 Integrations = 15 Marks	15 Marks

	b) State Land Records APIs for digital verification. c) GIS platforms like ISRO Bhuvan or similar services for crop verification. d) MS365 LDAP/Azure AD for secure access. e) Deploying and managing systems on a MeitY Empanelled Cloud Server.		
--	--	--	--

SECTION-V: Terms & Conditions

Submission of Document

The Technical Bid submission will consist of the following documents to be uploaded on the e-tendering portal:

- Copy of Empanelment Certificate with NICS or any State Agencies
- Copy of Certificate of Incorporation.
- Copy of PAN and GSTIN.
- Copy of Udyam Aadhar Registration (if any).
- Copy of Start-up Registration (if any).
- Copy of valid ISO 9001, ISO 27001, and CMM Level Certificates.
- Understanding of the project scope.
- Proposed Solution.
- Technology Stack.
- Key Innovations.
- Infrastructure Requirements.
- Work Plan.
- Details of prior experience in building government platforms.
- Declaration about non-blacklisting and non-conviction separately on a Non-Judicial Stamp paper.
- Representative Authorization Letter with Power of Attorney.
- Signed Tender Documents and Corrigendum (if any).

Payment Terms

a) Payment of the one-time development fee will be linked to the following milestones:

- i. **50% – Post UAT Sign-off, Source Code Delivery and Training**
 - Formal acceptance of the Software Requirements Specification (SRS) document.
 - Successful migration, deployment, and commissioning of the existing website and mobile application Content Management System (CMS) to the designated MeitY-empanelled cloud infrastructure.
 - Successful completion of User Acceptance Testing (UAT) and formal sign-off by the client (JCI).
 - Handover of complete, documented source code repositories for the website, CMS, mobile applications, and associated backend services.
 - Submission of user manuals, system administration guides, and API documentation.
 - Completion of training sessions for JCI staff covering CMS usage, eCommerce operations, employee portal management, and mobile app administration.
- ii. **40% – Post Go-Live and Compliance Certification**
 - Submission and approval of third-party audit certificates.
 - Successful production deployment (Go-Live) of the integrated platform, including - Website with CMS, eCommerce module, Employee Portal, Mobile

applications (audited version) published on Google Play Store and Apple App Store

- Submission of final deployment documentation and operational runbooks.

iii. **10% – Post Operational Acceptance**

- After six (6) months of stable operations post Go-Live.
- Subject to satisfactory performance and resolution of any critical issues during the operational support period.

b) Payment of Maintenance Cost

Annual operation & maintenance and cloud infrastructure fees will be billed on a quarterly basis after the Operational Acceptance. For each quarterly invoice for maintenance, the bidder should submit a comprehensive maintenance report supported by the following documentation:

i. **Service Delivery and Performance Reports:**

- **System Uptime Report:** A report detailing the uptime and availability of all hosted services (website, portals, mobile app backend) to verify compliance with the uptime guarantee.
- **Performance Monitoring Report:** A report on key performance indicators such as page load times and API response times for the billing period.
- **Content Update Log:** A detailed log showing all content updates and changes made to the website, eCommerce portal, and mobile application content, demonstrating that updates were performed at least once every 15 days.
- **Backup Status Report:** A confirmation report verifying that regular data backups have been performed as per the defined schedule (e.g., daily) and that recovery mechanisms are in place.

ii. **Incident and Issue Management Records:**

- **Bug Resolution Log:** A detailed log of all bugs, errors, and functional issues reported and resolved during the billing cycle, including their severity and resolution time. This should be tied to the bug reporting and tracking mechanism in the system.
- **Patch and Update Management Report:** A report confirming that all software, plugins, and scripts have been updated with the latest security patches within the stipulated timelines (15 days for high-critical and 30 days for others).

iii. **Compliance and Security Reports:**

- **Security Monitoring Log:** A log of continuous monitoring for security threats, anomalies, and potential breaches.
- **Compliance Verification Report:** A brief report confirming ongoing adherence to GIGW, WCAG 2.0 Level AA, and UIDAI compliance requirements.
- **Third-Party Integration Status Report:** A report confirming the stability and performance of integrations with the ERP, payment gateways, and other external systems.

iv. **Financial and Administrative Documents:**

- **Invoice:** The formal invoice for the maintenance fee for the billing period.

- **Reimbursement Invoices:** For any pre-approved third-party expenses (e.g., hosting, audits), original invoices and proof of payment must be submitted quarterly for reimbursement.

c) Payment for Third-Party Expenses (Reimbursement Basis)

For the following essential third-party services and allied activities, the bidder will incur the costs directly. These costs are not to be included in the lump-sum development fee quotation.

- Security and Functional Audits:** The bidder is responsible for engaging a **STQC or CERT-IN certified agency** to conduct the required security and functional audits. JCI will reimburse the actual invoice amount paid to the auditing agency upon successful submission of the audit certificates.
- Hosting Charges:** The bidder will manage the hosting of the entire system on a **MeitY empanelled Cloud Service Provider**. JCI will reimburse the hosting charges based on actual usage and submission of original invoices from the service provider.
- SMS Services:** The costs for SMS services required for notifications (e.g., booking confirmations and reminders) will be reimbursed based on actual consumption (to be supported with log) and submission of original invoices.
- Allied Services:** Costs for other value-added services such as **domain registration and SSL certificates** will be reimbursed upon submission of original invoices.

d) Reimbursement Process:

For any third-party software, licenses, or services, the following reimbursement procedure will apply:

- The bidder must obtain **prior written approval** from JCI for any such expense.
- JCI will reimburse the bidder the exact cost incurred upon submission of the original invoice and proof of payment.
- The bidder shall not charge any mark-up or administrative fee on these reimbursed expenses.
- All licenses and subscriptions for such reimbursed services will be procured in the name of The Jute Corporation of India Limited, ensuring JCI retains full ownership.

Note: The bidder's quoted price must already include the one-time development fee, security, functional and Payment Gateway integration audit fees, hosting charges (both interim and final), 3 years' maintenance, SMS Services, Allied Services, software, licenses, or services that are deemed essential for the project's proper functioning or compliance.

General Conditions

- Bidders are requested to submit proposals as per the attached documents. Deficiency in the required documents may lead to the rejection of bids.
- Bidders must comply with the pre-qualification criteria and technical evaluation criteria mentioned in the attached documents.
- Bidders are not allowed to form a consortium or submit multiple bids. Any such detection will lead to the rejection of the bid(s).
- JCI reserves the right to award or cancel the work without assigning any reason. In case of any differences, the decision of JCI shall be final and binding.

- e) Any services, functions, or responsibilities not specifically described but considered an inherent, necessary, or customary part of the services shall be deemed to be included within the scope of work for the agreed charges.
- f) The vendor will provide the latest and complete source code of the running software along with all necessary libraries and IDEs. JCI will be the sole proprietor of the developed system and its Intellectual Property Rights.

Indicative List of Required Features to be included in the System

The system must include the following features, with detailed requirements to be finalized in consultation with JCI user departments:

- a) Finalization of a backup policy and Disaster Recovery Management.
- b) Secure login for each user with an audit/log trail.
- c) Role-based access control.
- d) A normalized database with referential integrity, primary keys, and explanatory data fields.
- e) A feature for auto-periodic backup of the database.
- f) Support for Single Sign-On (Connect Once-Access Everywhere) so a single user login can access different modules/functions.
- g) A mechanism for Version Control and Bug Reporting & Tracking.
- h) The system must be easy to navigate and accessible on all platforms and major popular browsers.
- i) The system must include security features such as protection from OWASP vulnerabilities, strong password policy, encrypted storage of credentials/transactional data, and session management.
- j) Audit trails must be maintained as per CERT-IN guidelines, logging login attempts and data changes with timestamps and IP addresses.

SECTION-VI: Service Level Agreement

Service Level Agreement (SLA) for Jute Corporation of India (JCI) Web Portal and Integrated Systems

This Service Level Agreement ("SLA") is entered into by and between The Jute Corporation of India Limited ("JCI" or "Client") and [Bidder/Service Provider Name] ("Service Provider").

1. Purpose This SLA defines the levels of service, performance metrics, responsibilities, and escalation procedures for the development, deployment, and ongoing maintenance of the JCI Web Portal, including its integrated eCommerce portal, employee portal, and mobile application backend, as well as the maintenance of the existing Android mobile application.

2. Services Covered The services covered by this SLA include:

- Development, testing, and deployment of the new JCI Web Portal, eCommerce Portal, Employee Portal, and Mobile Application Backend.
- Interim maintenance and hosting of the existing WordPress website until the new portal's operational acceptance.
- Ongoing maintenance and updates for the existing JCI mobile application "Paat-mitro".
- Hosting services for the new systems on a MeitY Empanelled Cloud Server.
- Regular content updates, bug resolution, performance monitoring, and security management for all deployed systems.
- Provision of web statistics and analytics reports.
- Knowledge transfer and training.
- Documentation as specified.

3. Service Availability (Uptime Guarantee)

- **Target Uptime:** The Service Provider guarantees a minimum uptime of **99.5%** for all hosted services (new web portal, eCommerce, employee portal, and mobile app backend).
- **Measurement:** Uptime will be measured monthly, excluding scheduled maintenance windows.
- **Scheduled Maintenance:** The Service Provider shall provide JCI with at least 48 hours' notice for any scheduled maintenance that may impact service availability. Scheduled maintenance will ideally occur during off-peak hours.

4. Performance Metrics

- **Page Load Time:** All web pages (main website, eCommerce, employee portal) shall load within **3 seconds** on standard broadband connections (e.g., 5 Mbps or higher) for the majority of users (e.g., 90th percentile).
- **Mobile App Response Time:** API response times for critical mobile application functionalities (e.g., data retrieval, content display) shall not exceed **2 seconds**.

- **Search Functionality Response:** Internal website search and advanced search options shall return relevant results within **2 seconds**.

5. Response and Resolution Times for Issues/Bugs

Issues will be categorized by severity, with defined response and resolution targets:

Severity Level	Definition	Response Time	Resolution Time
High (Critical)	A critical function or security feature is completely inoperable. E.g., Payment Gateway down, entire website inaccessible.	1 Hour (24/7)	4 Hours (24/7)
Medium	Significant impairment of non-critical function, or minor security vulnerability. E.g., Some content updates failing, minor display issues.	4 Hours (Business Hours)	24 Hours (Business Days)
Low	Cosmetic error, minor usability issue, or enhancement request. E.g., Typo, broken link on an obscure page.	8 Hours (Business Hours)	72 Hours (Business Days)

- **Business Hours:** 9:30 AM - 6:30 PM IST, Monday to Friday, excluding public holidays.
- **Business Days:** Monday to Friday, excluding public holidays.
- **Escalation:** The Service Provider shall define a clear escalation matrix (including contact names and numbers) for each severity level, ensuring appropriate personnel are notified.

6. Data Backup and Recovery

- **Backup Frequency:** Full backups of all website content, databases (for all portals), and mobile application backend data shall be performed **daily**. Differential backups (if applicable) may be performed more frequently.
- **Retention Period:** Backups shall be retained for a minimum of **30 days**.
- **Recovery Point Objective (RPO):** Maximum allowable data loss in the event of a disaster shall be **24 hours**.
- **Recovery Time Objective (RTO):** Critical systems shall be restored and operational within **4 hours** of a disaster declaration.
- **Verification:** Backup restoration processes shall be tested at least **quarterly** to ensure data integrity and system recoverability.

7. Content Updates and Maintenance

- **Frequency:** The Service Provider shall ensure website content is updated at least **once every 15 days**. If no intimation is received from JCI, the Service Provider shall proactively request updates.

- **Response Time for Content Updates:** Urgent content updates (e.g., critical announcements) requested by JCI shall be published within **4 hours** during business hours. Regular content updates shall be completed within **24 hours**.
- **Archiving:** Outdated announcements shall be moved to an archive section with search functionality.

8. Security Management

- **Security Patches:** Software, plugins, scripts, and all components used in the website's development and operation shall be updated with the latest patches within **15 days** for High Critical Vulnerabilities and **30 days** for other vulnerabilities from the OEM announcement date, in consultation with NIC.
- **Vulnerability Remediation:** All vulnerabilities identified through security audits (VAPT) shall be fixed by the Service Provider within an agreed-upon timeframe based on severity, even after hosting is completed, until the end of the contract period.
- **Continuous Monitoring:** The Service Provider shall continuously monitor for security threats, anomalies, and potential breaches. Immediate response and remediation of security incidents are mandatory.

9. Compliance

- **Accessibility:** The website shall maintain WCAG 2.0 Level AA compliance and GIGW 3.0 Compliance throughout the maintenance period.
- **Hosting:** Hosting will be on a MeitY Empanelled Cloud Server.
- **Payment Gateway:** PCI DSS compliance for the eCommerce portal's payment gateway integration will be continuously monitored.
- **Mobile Application:** Compliance with Google Play Store guidelines will be maintained for the existing Android app.

10. Reporting

- **Web Statistics Reports:** Detailed web statistics reports, including user counts (daily, weekly, monthly, yearly), shall be provided to JCI officials as and when required.
- **Half-Yearly Reviews:** Comprehensive reports covering performance, security, compliance, and maintenance activities shall be submitted and reviewed with JCI on a half-yearly basis.
- **Audit Reports:** All security audit reports, functional audit reports, and payment gateway integration audit reports will be provided to JCI.

11. Communication and Contact

- **Single Point of Contact:** The Service Provider shall provide a dedicated project manager who will act as a one-point contact for JCI.
- **Communication Channels:** Defined channels for communication (e.g., email, phone, ticketing system) will be established for issue reporting, content update requests, and general queries.

- **Meeting Frequency:** The dedicated project manager shall be available for discussions and important meetings as required by JCI. Half-yearly review meetings are mandatory.

12. Penalties for Non-Compliance (Example - to be finalized by JCI)

- **Uptime SLA Breach:** If monthly uptime falls below 99.5%, a penalty of 0.5% of the monthly maintenance fee may be applied for each 0.1% decrement below the target.
- **Critical Bug Resolution Breach:** Failure to resolve a critical bug within the stipulated 4-hour resolution time may result in a penalty of 0.5% of the monthly maintenance fee per incident.
- **Security Patch Delay:** Delays in applying critical security patches beyond the stipulated timeframes may incur a penalty of 0.1% of the monthly maintenance fee per delayed patch.

(Note: Specific penalty percentages and caps should be mutually agreed upon during contract negotiation.)

13. Term This SLA shall commence upon the successful operational acceptance of the new JCI Web Portal and Integrated Systems and shall remain in effect for a period of **3 years**, unless terminated earlier in accordance with the terms of the main contract.

TECHNICAL BID FORM

(Submit separately from Financial Bid)

1. Bidder Details

Particulars	Details	Supporting Document																
Company Name																		
Year of Incorporation		Certificate of Incorporation																
PAN		Self-Certified Copy of PAN Card																
GSTIN		Self-Certified Copy of GST Certificate																
Registered Address																		
Udyam Registration No.		Self-certified copy of Certificate																
Type of Enterprise	Medium / Small / Micro Goods / Services																	
National Industry Classification Code																		
DIPP Certificate No.		Self-certified copy of Certificate																
Valid Upto																		
Contact Person		Letter of Authorisation from BoD / Propreitor																
Designation																		
Email ID																		
Contact Number																		
Financials (₹ in lakhs)	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th><th>2024-25</th><th>2023-24</th><th>2022-23</th></tr> </thead> <tbody> <tr> <td>Turnover</td><td></td><td></td><td></td></tr> <tr> <td>Profit before tax</td><td></td><td></td><td></td></tr> <tr> <td>Net worth</td><td></td><td></td><td></td></tr> </tbody> </table>		2024-25	2023-24	2022-23	Turnover				Profit before tax				Net worth				Audited balance sheet
	2024-25	2023-24	2022-23															
Turnover																		
Profit before tax																		
Net worth																		
Company has not been blacklisted/ debarred/ terminated/ banned by any Govt. Department/Public sector undertaking in last 3 Financial Years																		
Declaration on No Criminal Conviction																		
ISO 9001																		
ISO 27001		Self-attested copy of valid certificates																
CMMi3 or above																		

2. Technical Experience (Minimum 3 Projects)

Project Name & Duration	Client	Scope	Value (INR)	Functionalities implemented (tick as applicable)	Sample Documentation Provided
				<input type="checkbox"/> UIDAI/Aadhaar OTP verification. <input type="checkbox"/> State Land Records APIs for digital verification. <input type="checkbox"/> GIS platforms like ISRO Bhuvan or similar services for crop verification. <input type="checkbox"/> MS365 LDAP/Azure AD for secure access. <input type="checkbox"/> Deploying and managing systems on a MeitY Empanelled Cloud Server.	

3. Proposed Team

Role	Name	Experience (Years)	Certifications	Past Projects (Highlight projects listed under Technical Experience)
Project Manager				
UI/UX Designer				
Frontend Developer				
Backend Developer				
Mobile App Developer				
Security Specialist				
DevOps Engineer				

4. Technical Approach (Brief Methodology)

- ✓Web Portal Development: [Describe approach]
- ✓CMS Integration: [Describe approach]
- ✓Mobile Apps: [Describe approach]
- ✓Security Compliance (CERT-in, OWASP, etc.): [Describe measures]

5. Hosting Environment Proposal

A. Hosting Environment for New Systems			
Requirement	Proposed Solution	Specifications	Vendor Responsibility
MeitY- Empanelled Cloud Server	[Vendor to Specify]	- CPU/RAM/Storage	- Setup & Configuration
		- Scalability Options	- Security Hardening
		- Backup Policy	- Migration Support
B. Interim Hosting for Existing WordPress Website			
Requirement	Proposed Solution	Duration	Vendor Responsibility

Temporary Hosting Services	[Vendor to Specify]	Until New System Go-Live	- Uptime Guarantee
			- Security Patches
			- Data Migration Plan

6. Declaration

"We confirm that all information provided is accurate and complies with the RFP requirements."

Authorized Signatory: _____

Name:

Designation:

Company Stamp & Date: _____

FINANCIAL BID FORM

(To be printed on Bidder's letterhead and submit in a sealed envelope)

1. Cost Breakdown

Item			Amount (INR)	GST (%)	Total (INR)
One-Time Development Cost	Component	Sub-Component			
	Web Portal Development				
	CMS Integration				
	Mobile Appication	- Android ("Paat-mitro") Upgrade			
		- iOS Version Development			
	Farmer Slot Booking & Crop Verification				
	Employee Portal & KMS				
Annual Maintenance (Year 1)					
Annual Maintenance (Year 2)					
Annual Maintenance (Year 3)					
Grand Total					

2. Additional Costs (Reimbursable by JCI)

Item (Please mention all the items, that will require to deliver the scope)			Duration	Estimated Cost incl. of GST (INR)
Audit Requirement		Security Audit		
		Functional Audit		
		Payment Gateway Integration Audit		
MeitY Hosting	New Systems Hosting	Cloud Server Setup		
		Annual Maintenance		
	Interim WordPress Hosting	Basic Hosting		
		Migration Support		
SMS Gateway				
Active Directory License				
Grand Total				

3. Total Cost to the Corporation - _____ (Summation of 1 & 2 above)

Authorized Signatory: _____

Name: [Printed Name]

Designation: [Your Position]

Company Stamp & Date: _____

Declaration for non-blacklisting

I s/d/w/o resident of _____

Owner/ Partner/ Proprietor/ Director/ Chairman of M/s _____

having its registered office at _____

do hereby solemnly affirm and declare the following:

That our firm/ organization/ company/ society namely

M/S _____

has never been blacklisted by any department / Organization / Central Government / State Government / PSU in the preceding three years.

Place

Date

Signature

Official Stamp

Affidavit

I, s/o - resident of -----owner/ Partner/ Proprietor/ Director/
Chairman of M/s----- having its registered office at ----- do
hereby solemnly affirm and declare that neither Bidder nor the firm/ Partners/
proprietor/Director of the company has never been convicted or punished by
any Hon'ble Court of Law nor any criminal prosecution, involving moral
turpitude, in which a charge sheet is issued, is pending against any of them.

Deponent

Verification

Verified aton thedate

.....that the contents of the above

affidavit is true and correct to the best of my knowledge and belief.