Terms of Reference

For

"Hiring a firm for enhancement, implement, support & maintenance of National Portal Framework (NPF) Platform"

Aspire to Innovate (a2i)

Government of the People's Republic of Bangladesh

ICT Division

Agargaon, Dhaka

1. Background

The Government of Bangladesh, through the Aspire to Innovate (a2i) Programme under the ICT Division, has undertaken extensive initiatives to improve public service delivery using digital platforms. One of the major achievements of this transformation effort is the establishment and continuous expansion of the National Portal Framework (NPF), a unified digital gateway that hosts more than 35,000 government websites. The portal ecosystem serves as a critical public interface where ministries, divisions, departments, directorates, district and upazila offices publish essential information, services, forms, notices, circulars, and citizen-facing content.

A significant volume of work was completed under the previous development contract, which included architectural improvements, module enhancements, integration upgrades, theme development, capacity building, mobile app improvements, and large-scale operational support. The current system now functions as a mission-critical national digital asset, receiving millions of pages views every month and supporting tens of thousands of government officials in content management roles.

This Terms of Reference (TOR) outlines the specific responsibilities, functional requirements, service expectations, development methodology, team composition, and deliverables required from the selected firm to maintain and continuously enhance the National Portal Framework during the contract period.

2. Review of the Existing System

The National Portal Framework (NPF) is the core technology platform used to operate Bangladesh's unified e-Government web ecosystem. It provides a standard, centralized framework for building, hosting, managing, and maintaining government websites.

NPF is built on cloud infrastructure and follows microservices-based architecture, which ensures scalability, reliability, and easier maintenance. It includes an in-house Content Management System (CMS) that enables government offices to independently manage their website content. The CMS supports around 100 predefined content types, such as notices, news, service information, employee profiles, and office details.

The framework manages a hierarchical sub-domain structure for government offices. For example, an Upazila website operates as a sub-domain of its district (e.g., savar.dhaka.gov.bd), and an office under that Upazila operates as a further sub-domain (e.g., dae.savar.dhaka.gov.bd). This structure enables centralized control, easier monitoring, and consistent navigation for citizens.

NPF includes a theme library where multiple website themes are centrally managed. Site administrators can customize these themes using a block-based configuration, without changing the core system.

The platform allows government offices to publish news, notices, and progress updates in a standardized manner. To support high traffic, NPF uses automatic scaling, load balancing, caching, and real-time content delivery, allowing it to serve millions of users efficiently.

NPF exposes secure and high-performance APIs with built-in authentication, authorization, and Single Sign-On (SSO) for controlled access across services. Media and content are stored using S3-compatible object storage (Oracle S3), enabling efficient storage, search, and retrieval.

The framework also includes real-time monitoring, analytics, and data synchronization, ensuring operational stability and visibility across all government portals.

- National Portal is a single platform for the citizen to access all information about 35,250+ Government websites, 700,000 + Govt. Officers information, 10 million+ Contents, 1800 + Govt. forms, 800+ government services, 1500 + Master Trainers and so on. Average 70000+ people are engaged per 30 minutes & 15 million visitors in each month
- Existing Technology Stack
  Lang: Node JS, PHP Framework: Next JS, Nest JS, Express, Laravel, October,Falcon, Drupal
  Database: Postgre SQL, MongoDB, Mysql,
- Existing Independent Modules:
  - Job Portal
  - Portal Management system
  - Report Portal/ Monitoring Dashboard
  - Citizen Participation
  - Social media framework for national portal
- Existing Mobile App
  - e-directory
- NPF ensures that all government organizations have online presence, and the existing officers and staffs of the organizations are able to update the sites without depending on technical personnel.
- ln order to thrive in the mobile-first world, we must have to craft a mobile-first government in formation access plat form and service delivery strategy to ensure and strengthen better services. Thus, National Portal will be a mobile- first approach in Bangladesh.

2.1 About the Organization

Aspire to Innovate (a2i), is a whole-of-government programme of the ICT Division, supported by the Cabinet Division and UNDP that catalyzes citizen-friendly public service innovations, simplifying government and bringing it closer to people. It supports the government to be at the

forefront of integrating new, whole-of-society approaches to achieve the society. The objective of the project is to increase transparency, improve governance, and reduce the time, difficulty, and costs of obtaining government services for under-served communities of Bangladesh. This is to be achieved by the following 3 major components of the project:

Component 1: Institutionalizing Public Service Innovation and Improving Accountability

Component 2: Catalyzing Digital Financial Services and Fintech Innovations

Component 3: Incubating Private Sector-enabled Public Service Innovation

2.2 Existing Service, Resources, Infrastructure, Connectivity and Data Status (if any)

National Portal is a single platform for the citizen to access all information about 35,250+ Government websites, 800,000 + Govt. Officers information, 10 million+ Contents, 1800 + Govt. forms,800+ government services, 1500 + Master Trainers and so on. Average 70000+ people engaged per 30 minutes & 15 million visitors in each month. Around 200 virtual machine is used to manage this national portal framework.

2.3 Problems and Challenges

Despite the successful operation of the existing system, several technical, operational, and functional challenges have emerged over time that necessitate a structured maintenance and enhancement contract. These challenges impact system stability, performance, user experience, and long-term sustainability. The following issues have been identified as key areas requiring ongoing attention:

A. Technical Challenges

1. **Performance Bottlenecks**
   As traffic and data volume have grown, certain modules experience delays, slow response times, or inefficiencies in database queries. Search indexing, caching, and content rendering may require optimization to maintain expected service performance.

2. **Integration Instability**
   The system depends on multiple external services (APIs, authentication systems, content gateways, SMS/e-mail services, etc.). In some cases, integration points become unstable due to external changes, resulting in disruptions or inconsistent data flow

B. Operational Challenges

1. **Frequent Content Updates & Limited Editorial Tools**
   Regular content updates across multiple organizational units require improved editorial workflow tools. In some cases, editors face difficulties when large-scale content revisions or structural updates are necessary.

C. Security and Compliance Challenges

1. **Emerging Cybersecurity Threats**
   With increasing digital threats, the system must continuously adapt to new security risks. Outdated packages, inconsistent sanitization, or missing patch updates could expose vulnerabilities.

D. User Experience Challenges

1. **Inconsistent UI/UX Elements**
   Over time, incremental updates have resulted in visual inconsistencies across different modules. Some pages or components may not fully align with modern UI/UX guidelines or accessibility standards (e.g., WCAG).

2. **Mobile Responsiveness Issues**
   While the system is accessible on mobile devices, certain views, components, or forms may require additional refinement to ensure seamless responsiveness across all screen sizes and device types.

E. Hosting & Infrastructure Challenges

1. **Resource Scalability and Environment Constraints**
   Traffic growth and increased data load may strain existing hosting resources. Without proper scaling, catching improvements, or infrastructure optimization, performance may degrade over time.

2. **Dependency on Third-Party Hosting Procedures**
   Deployments, server-level adjustments, and certain security configurations depend on the

hosting authority's approval and support, occasionally delaying urgent fixes or enhancements.

F. Maintenance & Support Challenges

1. **Limited Automated Testing**
   Absence of systematic unit tests and regression automation increases the risk of unexpected side effects during updates.

2. **High Volume of User Support Requests**
   Continuous operational support is required for editors, administrators, and users reporting technical issues or seeking assistance.

2.4 Sign-Off & Operation Review Committee, IT Audit & Maintenance Monitoring Personnel for this Project

The sign off & operation review committee will be enacting by a2i authority time to time in the interest of the project whichever needed.

2.5 Data, Environment and Facilities to be Provided by Client

Existing system data will be available to firm. Staging, Production & UAT environment application will be provided by client.

Client will be providing Hosting & infrastructure facility. Service provider will ensure rendering services using this infrastructure.

3. Proposed System/ services

3.1 Objective

The objective of this assignment is to ensure the smooth, uninterrupted operation, maintenance, and improvement of the existing portal system. The Consulting Firm will provide technical support, bug fixing, code refactoring, and performance optimization, along with developing minor enhancements as required by the Client. The assignment also includes design improvements, theme updates, security reinforcement, and ensuring system compliance with government standards.

In addition, the Consulting Firm will provide technical and operational support for National Portal implementation activities, including deployment assistance, configuration support, troubleshooting, and coordination with relevant stakeholders.

The overall objective is to maintain system stability, improve usability, strengthen security, and support ongoing national portal initiatives.

3.2 Scope

The scope of services includes the following key activities:

1. Total duration of this project will be 7 (seven) months.
2. Provide regular technical support, issue resolution, troubleshooting, and stability improvements to ensure uninterrupted operation.
3. Upgrade outdated technical & architectural components, optimize database/API performance, improve code quality, and address technical debt.
4. Enhancement functionalities based on Client requirements, ensuring compatibility with the existing structure.
5. Update layout, fix UI issues, dynamic themes, improve accessibility, and refine design elements as needed.
6. Apply necessary security patches, address vulnerabilities, and maintain compliance with government ICT guidelines.
7. Assist in deployment, configuration, integration, issue resolution, and content or template support for National Portal initiatives.
8. Maintain updated technical and user documentation and support knowledge transfer to Client personnel.

3.3 Functional Requirements

The Functional Requirements outlined in this section specify, in detail, the activities, responsibilities, and outcomes expected from the selected service provider for ensuring the sustainable maintenance, enhancement, optimization, and continued improvement of the National Portal Framework (NPF) and all associated modules, mobile applications, and backend services. These requirements ensure that the system remains functional, resilient, secure, user-friendly, and compliant with government standards while supporting future growth and evolving operational needs.

The Consulting Firm will be responsible for delivering all functionalities described in the subsections below. Any omission of specific functionality does not exempt the Consulting Firm from delivering it if the requirement is reasonably implied or necessary for the stability, performance, or continuity of the system.

3.3.1 Functions and Features

This subsection describes the complete functional responsibilities the vendor must perform, categorized under three primary service areas:

A. Code Refactoring

B. Enhancement of NPF V2.0 (NodeJS- React Based)

C. Security & Compliance Enhancements

D. National Portal Implementation Support

E. Support & Service Delivery

A. Refactoring Responsibilities

The selected vendor will undertake comprehensive maintenance, code-level improvements, and refactoring activities to ensure that the system remains technically sound, optimized, and scalable.

A.1 Code Refactoring

The NPF platform consists of legacy, mid-generation, and modern components developed over multiple years. As a result, structured refactoring is required to improve long-term sustainability.

The Consulting Firm shall:

- Continuously identify technical debt across backend services, frontend layers, CMS logic, APIs, and integrations
- Refactor legacy code to improve:
  - Readability and maintainability
  - Modularization and separation of concerns
  - Reusability and testability
- Replace deprecated or unsupported libraries and functions with supported alternatives
- Eliminate duplicated logic and unused code blocks
- Externalize hard-coded values into configuration files or environment variables
- Align refactored code with standardized design patterns and coding conventions

- Ensure zero functional regression and full backward compatibility during refactoring

Please note that:

- Refactoring is **continuous**, not a one-time activity
- Monthly refactoring plans and progress reporting are mandatory
- Refactoring effort will be prioritized based on system risk, performance impact, and Client direction

A.2 Stability Maintenance & Corrective Actions

The Consulting Firm shall provide proactive and reactive maintenance to ensure uninterrupted operation of all system components.

This includes:

- Diagnosing and fixing:
  - Functional bugs
  - Performance degradation
  - Rendering or UI inconsistencies
  - API failures or integration errors
- Resolving content publishing, caching, indexing, or workflow issues
- Ensuring uniform theme behavior across thousands of portals
- Supporting mobile app stability, crash resolution, and OS compatibility

Please note that:

- Issue resolution volume is expected to be low and continuous
- All fixes must be tracked through an issue management system
- RCA documentation is mandatory for recurring or critical issues

A.3 Library, Package & Framework Updates

The Consulting Firm must keep all system components secure and supported by updating core libraries and frameworks.

This includes, but is not limited to:

Legacy Stack (NPF v1):

- Drupal 6.x
- Falcon Framework
- October CMS
- Lumen 6
- MySQL 5.6

Modern Stack (NPF v2):

- Next.js
- React
- NestJS
- Kafka
- MongoDB

The Consulting Firm shall:

- Assess impact before upgrades
- Ensure compatibility with existing modules
- Test thoroughly before deployment
- Document all version changes
- Framework upgrades may involve code adjustments and regression fixes
- Security-driven updates take priority over feature work

A.4 Database Optimization & Index Maintenance

The Consulting Firm is responsible for ensuring optimal database performance across PostgreSQL, MySQL, and MongoDB.

Key activities include:

- Query optimization and slow-query analysis
- Index creation, rebuilding, and tuning
- Managing large datasets and historical data growth
- Preventing deadlocks and data inconsistencies
- Ensuring referential integrity across modules

Scope clarification:

- Database tuning is expected to be **ongoing**
- Monthly performance metrics and improvements must be reported

A.5 Search Engine Optimization

Security maintenance is continuous and mandatory.

The Consulting Firm shall:

- Apply security patches across applications, databases, and dependency layers
- Conduct vulnerability scanning and remediation
- Address OWASP Top 10 risks
- Secure authentication, RBAC, APIs, sessions, and cookies
- Monitor logs for anomalies and suspicious activities

A.6 Security Hardening & Patching

Security maintenance is continuous and mandatory.

The Consulting Firm shall:

- Apply security patches across application, databases, and dependency layers
- Conduct vulnerability scanning and remediation
- Address OWASP Top-10 risks
- Secure authentication, RBAC, APIs, sessions, and cookies
- Monitor logs for anomalies and suspicious activities

B. Enhancement of new versions

During the implementation and operational phases, new requirements, gaps, or system inconsistencies may be identified. The Consulting Firm shall analyze these findings and develop necessary improvements, fixes, or feature adjustments to ensure smooth rollout and stable operation of the system. While this is a maintenance contract, the system will evolve with policy requirements and user demands within existing architecture. The vendor must deliver enhancements as directed by the Client.

B.1 CMS Extensions & Dynamic Content Workflow Enhancements

The Consulting Firm shall improve editorial productivity without disrupting existing workflows.

Enhancements may include:

- Improved CKEditor configuration
- Rich text and media improvements
- Bulk content operations
- Approval workflows and staging
- Versioning and rollback mechanisms

B.2 Enhancement Based on Findings During Implementation

During onboarding or live usage, new gaps may emerge.

The Consulting Firm shall:

- Analyze operational issues
- Design and implement small to medium enhancements
- Adjust workflows, templates, or configurations
- Support policy-driven functional changes

B.3 Dynamic Themes & UX Modernization

The vendor will develop:

- New themes (10) and templates aligned with interactive layouts
- Responsive and WCAG 2.1 compliant UI
- Improved navigation and component libraries
- Theme customization options for offices

Minor thematic changes must be deployable without downtime.

B.4 API Integrations

The Consulting Firm shall:

- Support mobile apps, dashboards, and cross-portal data exchange
- Implement authentication, rate limiting, and standardized responses
- Support approved storage migration initiatives (e.g., S3 → MinIO)

APIs must follow REST principles and include authentication, rate limits, and standardized responses.

B.5 Search Feature Enhancements

Search enhancements may include:

- Auto-suggestions
- Synonym dictionaries
- Fuzzy search
- Ranking and relevance tuning

B.6 Enhancement of independent Modules

The vendor will need to enhance the following independent modules:

- Portal Management system
- Report Portal/ Monitoring Dashboard Visualization
- People's Participation

C. Security & Compliance Enhancements

C.1 Continuous Security Enhancement

The Consulting Firm shall improve the platform's security posture through:

- Strengthening authentication mechanisms
- Implementing secure cookies and session policies
- Reinforcing API security and request validation
- Hardening configuration parameters

C.2 SOC Monitoring & Log Analysis

The Consulting Firm shall implement SOC-driven enhancements including:

- Enhanced log formats with contextual metadata
- Centralized log consolidation across layers
- Generation of actionable event logs for SOC review
- Real-time alert generation for suspicious activities
- Configuration enhancement & monitor WAZUH or similar SIEM tool.

C.3 Threat Detection & Incident Response Support

The Consulting Firm shall:

- Support SOC team investigations
- Assist in forensic log review
- Produce RCA for security incidents
- Implement mitigation steps and prevention controls

C.4 Vulnerability Management

Includes:

- Periodic vulnerability scans
- Resolving critical findings promptly
- Updating dependencies and patching components

- Hardening file uploads, APIs, input fields, and access paths

C.5 Access Control & Identity Security

The Consulting Firm shall:

- Improve RBAC permission structures
- Reduce over-privileged roles
- Strengthen editor/admin authentication flows
- Support optional 2FA or IP-based restrictions if requested

D. National Portal Implementation

The existing system is a core component of the broader National Portal ecosystem, which consists of thousands of government offices operating under a unified digital framework. Due to the rapid expansion of the system over the years, multiple government offices currently operate portals built on different codebase versions, theme structures, and module configurations. This creates inconsistencies in functionality, user experience, security posture, and upgrade-readiness.

Accordingly, the Consulting Firm shall play an active and continuous role in assisting a2i and the Client in the following key areas:

D.1 Technical Support for National Portal Implementation

The Consulting Firm must work directly with a2i and relevant government teams to ensure that new and existing offices are implemented smoothly into the National Portal ecosystem. This includes:

- Supporting deployment of standardized portal releases
- Assisting with installation, configuration, and environment setup
- Troubleshooting issues during onboarding or migration
- Providing technical guidance to ensure compliance with national standards
- Ensuring pages, menus, structures, and content templates match national guidelines

This support is continuous and applies both to new offices and offices requiring version updates.

E. Support & Service Delivery

E.1 Technical Support

The vendor shall provide:

- Issue diagnosis
- Technical debugging
- Backend analysis
- Code-level fixes
- User-office support

Support must follow SLA timelines and use structured reporting.

E.2 Incident Management & RCA

The vendor must:

- Maintain incident registers
- Perform root cause analysis
- Implement corrective & preventive actions
- Ensure no recurrence of major incidents

E.3 Deployment & Release Management

The vendor will:

- Manage staging & production deployments
- Maintain a2i Git repositories
- Follow versioning standards
- Create release notes for every deployment
- Prepare rollback plans

Reimbursement Cost:

SMS, SMTP Server, Security tools, Google captcha this tool can be paid from here.

3.3.2 User and User Roles

The National Portal Framework serves a wide and diverse set of users who interact with the system in different capacities. The vendor must ensure that all maintenance, enhancements, refactoring, and support activities respect the existing user hierarchy, preserve the role-based access control (RBAC) model, and maintain the operational integrity of the workflow.

Users of the system can be broadly classified into the following categories:

A. Super Administrator

The Super Administrator role represents the highest level of authority within the system. This role is typically exercised by a2i's central digital service team. Key responsibilities include:

- Managing system-wide configuration
- Overseeing portal hierarchy
- Creating or modifying ministry/division-level administrator accounts
- Approving large-scale updates or structural changes
- Monitoring activity logs for compliance
- Managing global settings, themes, and workflow parameters

The vendor must ensure exclusive and secure access to this role, with strict audit trails for all actions performed.

B. Ministry / Division / Directorate Administrators

These users are responsible for managing portal operations for their respective ministry or department. Their responsibilities include:

- Approving content submitted by office-level administrators
- Conflict resolution among subordinate offices
- Managing office-level account creation (within their authority)
- Overseeing portal theme and template usage

- Monitoring content quality & compliance with government standards

The vendor must ensure continuity of their workflows and approval chains during enhancements.

C. Office Administrators

These users manage an individual office-level portal. Their tasks include:

- Publishing content
- Managing pages, menus, media, and notices
- Coordinating with the parent ministry/division
- Assigning editorial responsibilities to subordinate editors
- Ensuring content accuracy and timely updates

The system must support high usability for these users, given the large number of office-level administrators across Bangladesh.

D. Editor / Publisher / Content Contributor

These users perform day-to-day content operations including:

- Drafting and editing content
- Uploading images, videos, documents
- Updating notices, forms, or service information
- Submitting content for approval

Any changes in UI/UX must be validated to ensure minimal disruption to this role.

E. Field ICT Officers

This technical role exists across various offices. They support:

- Misconfigurations
- Portal data consistency
- Minor troubleshooting
- User account support

The vendor must ensure availability of documentation and help resources for them.

F. General Citizens / Public Users

Citizens access the public-facing portal for:

- Viewing information
- Navigating menus
- Downloading forms, notices
- Using integrated services
- Submitting queries or feedback

The vendor must maintain accessibility, stability, search accuracy, and uptime for this role.

User Name	Roles	No. Of Users
Site Admin	Add, Update, Delete of portal	70000
Ministry /Division	Monitoring & Coordination	200
NPF Admin	NPF management & admin	100
Master Trainer	Training of NPF	300
Assistant Programmer	Overall management offices of Upazila/District	1000

3.3.3 Security and Privacy Policy

The Consulting Firm must ensure that the system complies with the national cybersecurity standards, Government Rules & regulation with alignment of global ethics & best practices. Security is of highest priority given the large-scale usage and sensitivity of government information.

The vendor shall be responsible for:

A. Application-Level Security

- Full adherence to **OWASP Top 10**

- Protection against XSS, CSRF, SQL Injection, SSRF, directory traversal, code injection
- Implementation of secure authentication and authorization
- Preventing unauthorized access to admin functions
- Validating all inputs at both client and server levels

B. Data Security & Privacy

- Securing personal data and sensitive content
- Ensuring encryption in transit (HTTPS)
- Ensuring encryption at rest where applicable
- Enforcing secure password policies
- Preventing data leakage through logs or API misconfigurations
- Maintaining strict session management

C. Server & Infrastructure Security

Vendor must coordinate with the National Data Center (or designated hosting agency) to ensure:

- Proper firewall rules
- Regular OS-level patching
- Access control at server and network layers
- Secure deployment processes
- Backup validation and recovery readiness

D. Log Management & Monitoring

A structured log review and alert mechanism must be maintained. Logs include:

- Access logs
- Error logs
- Security logs

- Admin activity logs
- API consumption logs

Vendor must perform periodic (every 3 months) security audits and mitigate findings immediately.

E. Adherence to National Policies

The system must comply with:

- Govt. CERT & CIRT guidelines
- Personal data protection ordinance, 2025
- ICT Division security circulars
- Data localization requirements
- All applicable legal and regulatory frameworks

3.3.4 Integration and External Dependencies

The NPF interacts with multiple external systems, national platforms, government repositories, and third-party services. The vendor must ensure uninterrupted functioning of all such integrations.

Responsibilities include:

1. API Monitoring & Issue Resolution

- Monitor API endpoints for failures
- Handle token expiry, header issues, rate limits
- Implement standardized error-handling mechanisms
- Maintain integration logs and dashboards

2. New Integrations (As Requested)

Vendor must be prepared to:

- Develop new REST APIs
- Implement new adapters
- Extend data schemas
- Participate in joint testing with partner systems

Sl	External connectivity	Stakeholder name
1.	SMS Gateway	Telecom Operators
2.	Payment Gateway/ ekPay/binimoy	a2i / Third Party Organization
3.	333	a2i
4.	iBAS++	Finance Division
5.	Mygov	a2i
6.	AI Chatbot	a2i
7.	CDAP	a2i
8.	Bangla Spell Checker	Bangla Project, BCC
9.	Bangla Speech to text	Bangla Project, BCC
10.	Nothi/Doptor	A2i
12.	ekShop	A2i
13.	Google Analytics	Google
14.	Heatmap Tools	Open Source/Open Platform
15.	Social Media Framework for NPF	A2i

3.3.5 Hosting Requirement and Plan

The system is hosted in the government's designated data center environment. Therefore:

A. Hosting Environment

The vendor must:

- Maintain compatibility with the existing hosting infrastructure
- Coordinate environmental changes with the data center team
- Maintain staging, UAT, and production environments
- Schedule & maintain periodic backup of Database, Source Code & environment configuration
- Ensure all hosted components meet availability & security requirements

B. Deployment Coordination

Vendor will:

- Preparing deployment packages
- Conduct staging environment validations
- Coordinate change requests with Data Center
- Ensure proper rollback mechanisms

C. Environment Documentation

Vendor must maintain:

- Environment configuration guide
- Port lists, firewall rules, DB connection parameters
- Server-level dependencies
- Cron jobs and scheduled tasks
- Monitoring configuration

D. Data Center Compliance

Vendor must comply with:

- Access protocols
- Deployment windows

- Security guidelines
- Documentation requirements

3.4 Non-Functional Requirements

The Non-Functional Requirements define the essential quality attributes, performance benchmarks, compliance obligations, documentation expectations, and operational standards that the Consulting Firm must ensure throughout the duration of the maintenance and enhancement contract. These requirements apply across all modules, components, APIs, mobile applications, user interfaces, and backend services.

The Consulting Firm must ensure full compliance with these standards for both existing functionalities and new enhancements delivered under this contract. The non-functional requirements are binding and will serve as a benchmark for monitoring vendor performance, system health, and overall service quality.

3.4.1 Sizing, Performance and Scalability Requirements

The National Portal Framework serves millions of users across the country and supports thousands of content administrators. Therefore, system performance must be continuously optimized to ensure a smooth and uninterrupted experience.

A. Performance Requirements

The Consulting Firm must ensure:

- Fast page load times (below 4 Second) across all government portals
- Optimized backend response times
- Efficient database queries
- Reduced latency in API calls
- Minimal rendering delays in frontend components
- Optimized mobile app performance across diverse devices

Performance tuning must be done proactively, not only reactively after issues appear.

B. Scalability Requirements

The system must scale horizontally and vertically as per national needs. The vendor must ensure:

- Backend architecture supports increased traffic
- Search indexing scales with content growth
- Database is optimized for large datasets
- Cache layers are used efficiently
- New components are designed to be scalable by default

Scalability planning must be documented in the monthly technical report.

C. Capacity Monitoring

The Consulting Firm must continuously monitor:

- CPU, RAM, I/O usage
- DB storage and growth trends
- File storage and media volume
- Search index size
- API throughput

Thresholds must be defined, and alerts must be tracked and resolved.

3.4.2 Coding Convention

The Consulting Firm must maintain rigorous coding standards to ensure long-term sustainability, readability, and maintainability of the system.

A. Coding Standards

All new code and refactored code must follow:

- PSR standards
- Standardized JavaScript/TypeScript conventions

- Modular component design
- Clean architecture principles
- Avoidance of tightly coupled logic
- Descriptive naming conventions and commenting

B. Source Code Quality

Vendor must ensure:

- No hardcoded credentials
- No deprecated functions
- Minimal duplication
- Proper exception handling
- Unit-level logical clarity

C. Version Control Discipline

The vendor must:

- Maintain Git repositories properly
- Use feature branches
- Follow merge request conventions
- Ensure tagged and documented releases
- Keep commit history clean and meaningful

D. Refactoring Practices

Code refactoring must be:

- Planned
- Documented
- Tested

- Non-breaking
- Continuously incremental

3.4.3 Business Continuity Plan

The Consulting Firm must ensure the system's uninterrupted operation even in the event of operational disruptions, hardware failures, unexpected traffic spikes, or security incidents.

A. Continuity Assurance

Vendor must:

- Ensure 24/7 system availability
- Maintain alternative access to tools
- Following deployment fallback procedures
- Maintain backups of code, DB, and configurations

B. Disaster Recovery Readiness

Vendor shall:

- Ensure backup integrity
- Support restoration procedures
- Maintain DB snapshot rotation
- Test rollback mechanisms regularly

C. Zero-Disruption Change Management

Vendor must deploy enhancements in a way that:

- Does not disrupt live services
- Ensures rollback availability
- Minimizes downtime windows

3.4.4 Accessibility

Firm should follow & comply Digital Service and Web Designing Guideline for Inclusive Accessibility 2022. Also follow below check list for understanding.

Sl.	**Items To check**	**Details**
1.	For anything on a web page that is not text, is there any text equivalent for that item?	• Anything that does not text on a web page usually includes, but is not limited to, an image, graphic, audio clip, applets (small application running within a web browser, i.e. text chat window, etc.), tickers, or other feature that conveys meaning through a picture or sound. Examples include buttons, check boxes, pictures and embedded or streaming audio or video. • Providing a text equivalent means that words are being used to describe what an item (that does not physically consist of text) actually is, why it is there, and any information being communicated by the use of that item or the item itself. • Check that all images have accurate and meaningful text equivalents. Images mostly use an "alt-tag" or "longdesc" attribute as part of the object. To check, mouse users can roll their cursor over an image. If a text label or window pops up, then it has a text equivalent. Screen reader users can listen to see if an image is identified and described. It is also acceptable to simply include a text description above or below the image. For example, "The picture below shows…" • Ascertain that images of text, graphical text (pictures of text), or text that is part of an image have a text equivalent. Be sure that the text equivalent correctly describes the image or communicates any information as part of the image. For example, if the image itself contains words, be sure the exact wording from the image is used within the text equivalent. • Ensure any audio has a text equivalent, such as a text transcript.
	Is captioning, audio descriptions, or other	• Determine that all audios have been captioned for the deaf and hard of hearing, and all videos have audio descriptions for blind and visually impaired.

	equivalent provided for presentations that utilize both audio and video at the same time? Is captioning, descriptions, or other alternatives synchronized with the presentation?	• Ascertain that captions and audio descriptions are synchronized correctly with the audio and video. For example, synchronized captions allow someone to read captions and also watch the speaker's relevant body language. • Remember that this only applies to multimedia presentations, i.e., those presentations utilizing both audio and video at the same time. For example, the audio and video web cast of a program would need to be synchronized. An audio web cast would require a text transcript. A silent (no audio) web slide show would require a text equivalent for any images.
	If color was removed, would it inhibit use of the web site?	To check, view the page using a monochrome monitor (ex. black and white monitor, etc.) or by printing a page to a black and white printer.
	Is color being used to emphasize text or indicate an action?	If so, an alternate method needs to be included so users can identify what is being emphasized by the use of the colored text or action. For example, if all links on a web page are blue, than underlining the links is an acceptable method for identifying blue colored links. Another example, if users are prompted to press a green start button, than a text label above the green button saying "press green start button" is an acceptable method.
	Do web pages ignore user defined style sheets?	Style sheets are formatting instructions on how a page should be displayed (can also include how it is printed and presented). For example, a user specifies that they want their browser to view pages with extra-large font with white characters on a black background. These preferences are set up for all pages viewed.
	Does a web page override or ignore user settings?	To check, disable style sheets within the browser (Check browser's help menu for instructions) or try changing the font size or background colors through the browser's settings.

	If a link is embedded in an image, is there an equivalent text link?	• Frequently, a web designer will use an image map which contains a link or set of links. • Check to see if the image has any text links or labels. In some cases, you may have to move the mouse around the image to see if different text labels appear over different portions of the image. Screen readers will announce "image map link…" when a link is detected. These text labels alert users that by clicking or selecting the link in this particular region of the image, it will retrieve a specific web page. This is an example of a client-side image map which can be quite accommodating to people with disabilities and those using assistive technology. • On the other hand, there are image maps that do not indicate to the user which specific web page will be retrieved when a particular region of the image is selected. These are called server-side image maps, because the computer or server hosting the web page determines which page is sent based on portion of the image selected. These are not accessible image maps, requiring a redundant text link on the same page retrieving the same pages as those links used in the image map.
	If information is displayed using a table(s), can columns and rows be identified by screen readers?	Using a screen reader, listen to how the table is read aloud.
	If frames are used, are they accurately text labeled?	Frames are used to visually separate information on a web page.
	Does anything on the page blink or flicker?	Ask if the web designers can prove whether any blinking or flashing elements have a frequency greater than 2 Hz and lower than 55 Hz. This requirement is necessary because some individuals with photosensitive epilepsy can have a seizure triggered by displays that

		flicker or flash, particularly if the flash has a high intensity and is within certain frequency ranges.
	Do web sites not conforming to acceptable and approved accessibility standards offer a text only equivalent of their web site?	4 The World Wide Web Consortium's (W3C) Web Accessibility Initiative Guidelines and Section 508 are the two widely accepted authorities on Web accessibility and design. 5 Web sites that cannot adhere to the accessibility guidelines set forth by W3C and Section 508 can offer a text only equivalent for all the information displayed and all functions available.
	If scripting is used, such as JAVA, etc., is there a text equivalent so assistive technology, like screen readers, can read the information?	An example of scripting could be a stock ticker on a web page that is animated, refreshing, and displaying information. Another example is using an image, that when a mouse cursor rolls over the image, additional information pops open on the screen, and then disappears when the mouse cursor rolls off.
	If online forms are used, can people using adaptive technology fill in and submit all the required information?	4 Can a keyboard be used to access all the form fields? 5 Are text labels used either inside or near form fields to identify what information users should be entering? 6 Can a screen reader identify the form(s)? 7 Do the forms follow a logical order? For example, if a user hears "Last Name" is the corresponding form the area where they would enter their last name?
	Is there a way for users, especially those using screen readers	Navigational links are a set of routine navigation links frequently used to move users to pages within a web site,, usually located on the top or side of each web page. For example, "Help," "Contact Us," etc. links

	to skip repetitive navigational links?	that all appear on the same page within a web site in exactly the same way and location.
	If users are given a certain amount of time for an action or response, is there any indication how much time they have left or an option to request more time?	Some web pages may expire or time out after a certain amount of time, and refresh the entire page, for example those requesting personal information.
	Unicode character set for Bangla	Use of Unicode character set for Bangla - Interspersing Bangla and English in the same page should be avoided until such time that there is a screen reader which can handle multiple languages.
	Accessible documents on web pages	Where it is not possible to make a document accessible, then an alternative, accessible format should be downloadable along with the original image file.
	Navigation mark-up	Use of heading level 1-6, in addition to navigation links like 'skip to main content'.
	HTML validation	HTML is the simplest programming language used for website development and is accessible on all browsers — desktop browser or a mobile browser. All web pages should have HTML validation.
	CSS validation	Content presented with CSS errors may lead to serious problems such as overlapping of content, making it almost impossible to read. CSS errors may also prevent some users from successfully carrying out custom CSS processing to set the preference of color and size of text and object to suit their vision requirement.

	Color adjustment option	High contrast and font customization options should be available
	Labeling of Links	Labeling links correctly rather than just 'click here'- i.e., descriptions should be accurate. 1. The web page has a descriptive and informative page title. 2. A sign language video is provided for all media content that contains audio. 3. The page is readable and functional when the text size is doubled. 4. All page functionality is available using the keyboard
	Accessibility plugin	Some accessibility features such as Monochrome, Invert Colors, Big Cursor, Highlight Link, Show Headings, Reading Guide, Reset Button, Keyboard Shortcut etc. Commonly these items are named Accessibility Plugin.
	Accessibility Guideline	Have to follow the WCAG 2.1 Guideline.

3.4.6 Standard, Tools and Technologies to be Used

All development, maintenance, and enhancement activities must follow modern and widely accepted standards.

A. Development Tools

Vendor must use:

- Version control (Git)
- Issue tracking (Jira, Redmine, or equivalent)
- Code quality tools
- CI/CD pipelines

- Automated testing tools

B. Technology Stack Compatibility

Enhancements must be compatible with:

- Existing framework versions
- Server OS
- Database engine
- Search engine (Solr/Elastic)
- Mobile platforms (Android, iOS)

C. Compliance with Government Guidelines

All tools used must adhere to:

- ICT Division guidelines
- a2i technical directives
- Personal Data Protection Ordinance, 2025
- Data hosting policies

3.4.7 Data Ownership

All data generated, stored, processed, or transferred through the system shall remain the exclusive property of the Government of Bangladesh and the Client organization. The Consulting Firm shall have no ownership, usage, reproduction, resale, or distribution rights over system data under any circumstances.
The Consulting Firm must ensure that:

1. All source code, databases, configuration files, log files, media, and content will be plagiarism free & belong solely to the Client.
2. No data may be stored in external, third-party, or cloud repositories without explicit written approval.
3. Data shall not be used for any analytical, commercial, or testing purposes outside this project.

4. Upon contract completion, all system data, credentials, and associated artifacts must be handed over to the Client without delay.

5. No data shall be retained by the Consulting Firm after contract closes out.

The Consulting Firm shall sign necessary confidentiality and data-protection declarations as required by the Client.

3.4.8 Data Security

To ensure the confidentiality, integrity, and availability of government data, the Consulting Firm shall uphold strict data security standards across all environments (development, staging, UAT, and production). Responsibilities include:

1. Adhering to the Government of Bangladesh ICT Security Guidelines.

2. Implementing strong access control, secure authentication, and encrypted communication methodologies.

3. Ensuring secure coding standards to prevent OWASP Top-10 vulnerabilities (XSS, CSRF, SQL Injection, insecure deserialization, etc.).

4. Protecting data at rest and in transit using industry-standard encryption mechanisms, and ensuring file upload security and data sanitization.

5. Maintaining secure backup procedures with strict access control to backup environments.

6. Ensuring no sensitive credential (DB passwords, API keys, admin rights) is exposed, logged, or shared.

7. Supporting SOC and security audit activities, implementing mitigation measures, and responding to identified vulnerabilities within the stipulated timeframe.

Any security breach, attempted intrusion, or data anomaly must be reported to the Client within 1 hour of detection.

3.4.9 Technology Handover

The project requires full and transparent handover of all technology artifacts to the Client. The Consulting Firm must ensure:

1. Delivery of full source code, configuration files, APIs, scripts, deployment scripts, documentation, templates, and all related technical assets.

2. Handover of all credentials including admin logins, database access, SSL, hosting access (where applicable), monitoring dashboards, repo access, and deployment tools.
3. Ensuring the system can be operated independently by a2i personnel after handover.
4. Providing final knowledge-transfer sessions for a2i technical teams.
5. Ensuring that the Client receives the final "Build & Deployment Package" suitable for re-deployment without vendor involvement.
6. Ensuring no proprietary or vendor-locked components prevent the Client from operating or modifying the system.

The Consulting Firm shall ensure that the entire technology stack is fully documented and capable of being managed without dependency on the vendor.

3.4.10 IT Compliance

The Consulting Firm shall ensure that all activities, implementations, configurations, and maintenance works strictly comply with applicable national ICT policies, standards, and regulations. These include but are not limited to:

1. National ICT Policy, National Data Center Hosting Guidelines, Digital Security Act considerations, and applicable e-Government standards.
2. Compliance with government data privacy requirements and audit recommendations.
3. Following all directives from a2i, ICT Division, NDC, and other authorized entities relating to security, hosting, or portal management.
4. Ensuring accessibility compliance (WCAG 2.1), interoperability standards, and platform usability guidelines.
5. Adhering to version control and configuration management practices recommended by government IT governance frameworks.
6. Supporting third-party IT audits and addressing findings within the prescribed timeline.
7. Ensuring compliance with software license policies (open-source, proprietary, third-party libraries) and maintaining documentation of all components used.

Non-compliance may result in penalties, mandatory rework, or contract termination based on the severity and nature of the issue.

3.4.7 Quality Assurance and IT Audit Requirements

Approved VAPT certification from Software & Hardware Quality, Testing and Certification (SHQTC) Center & Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT) Or any Certification from any international organization agreed upon a2i & responsible firm.

System testing at every delivery phase (according to delivery schedule) of the project ranging from 1-3 months by the firm. Also, Domain team and technical team of a2i will conduct test by themselves or using 3rd party organization. Following testing has to be done-

- Accessibility testing
- Black box testing.
- End to end testing.
- Functional testing.
- Interactive testing.
- Integration testing.
- Load testing.

The following vulnerabilities must be checked and ensured security from the beginning:

- Cross Site Request Forgery (CRSF)
- Cross Site Scripting (XSS)
- Session hi-jacking
- Session Fixation
- SQL Injection
- Input Validation/Filtering
- Output Escaping
- Secure File Access

Submit quarter-wise report on security testing and fix the necessary security holes found in security testing. Contracted firm will take necessary steps to fix the security holes.

3.5 Critical Components in Delivering the Services

The successful execution of this contract depends on several critical components that collectively ensure the stability, modernization, and long-term sustainability of the National Portal Framework (NPF). These components represent the essential conditions, technical foundations, operational practices, and vendor responsibilities required to maintain the system at national scale. The Consulting Firm must therefore ensure full preparedness, capability, and procedural rigor to deliver all services described in this TOR.

The following elements are considered critical components for delivering the required services:

A. Deep Understanding of the Existing Codebase

Given that this contract is focused on the maintenance and continuous enhancement of a large, multi-layered, legacy-plus-modern blended system, one of the most critical components is the vendor's ability to:

- Rapidly understand the existing architecture
- Navigate legacy components, refactored modules, and updated code blocks
- Interpret historical development decisions
- Identify technical debt and potential failure points
- Ensure backward compatibility in all changes

The vendor's development team must allocate time and expertise to study the existing system thoroughly before making any modification, ensuring the stability of ongoing operations.

B. Capability in Code Refactoring and Optimization

A significant part of this assignment involves improving system performance, maintainability, and long-term efficiency through structured code refactoring. Refactoring must be continuous and systematic.

Critical components include:

- Expertise in modern coding practices
- Ability to restructure complex and lengthy legacy functions
- Skill in improving modularity and reducing duplication
- Experience in optimizing database-heavy and API-driven systems
- Adherence to coding standards and architectural discipline

Refactoring must be carried out without breaking live services, and must strictly follow versioning and testing protocols.

C. High Availability and Incident Response Readiness

The NPF ecosystem supports a nationwide user base. Any downtime directly impacts citizen service delivery and government communication.

Critical operational components include:

- 24/7 monitoring
- Rapid incident detection and escalation
- SLA-driven issue resolution
- Root cause analysis (RCA) and preventive actions
- Ability to coordinate with data center teams during emergencies
- Alternate deployment pathways in case of critical failures

The vendor must maintain sufficient technical staff and tools to ensure uninterrupted service continuity.

D. Expertise in Managing Large-Scale CMS and Search Platforms

The portal framework hosts thousands of websites and hundreds of thousands of content items.

Critical components include:

- Understanding of large hierarchical CMS structures
- Expertise in search indexing (Solr/Elastic)
- Ability to maintain and optimize back-office workflows
- Competence in handling mass content operations without performance loss
- Experience with caching strategies for large-scale content delivery

The vendor must ensure the system remains responsive and efficient despite scale.

E. Secure Development and Deployment Practices

The vendor must follow strict security-first principles across all development and maintenance activities.

Critical elements include:

- Secure coding
- Vulnerability assessments
- CSRF/XSS/SQLi prevention
- Session and token security
- Strict RBAC adherence
- Compliance with national cybersecurity guidelines
- Secured deployment pipelines

Failure to implement secure practices may jeopardize national-level data.

F. Strong Coordination with Stakeholders

The system relies on inputs and usage from:

- Ministries and divisions
- District and upazila offices
- External government agencies
- Data center teams
- a2i technical and program teams

Critical components include:

- Clear communication channels
- Regular review meetings
- Responsiveness to instructions
- Transparent reporting

- Proper documentation of enhancements, issues, and deployments

Coordination must be professional, timely, and well-documented.

G. Continuous Performance Monitoring

System performance must be proactively managed.

Critical monitoring components include:

- Resource utilization dashboards
- Log monitoring
- Slow query detection
- API latency analysis
- Real-time search index health checks
- Background job/queue monitoring
- Automatic alerting mechanisms

Performance monitoring must be part of daily operations, not reactive measures.

H. Adherence to Structured Development & Testing Practices

Every change — whether minor maintenance or major enhancement — must go through defined processes:

- Requirement analysis
- Impact assessment
- Development and peer review
- Functional and regression testing
- UAT validation based on user instructions
- Staged deployment

This structure is essential for preventing unintended disruptions.

I. Capacity to Manage Mobile App Updates

Critical components include:

- Timely OS compatibility updates
- Maintaining app performance and stability
- Ensuring API compatibility
- Managing release cycles via Play Store and App Store
- Providing updated builds for UAT

Given the national use of the app, proper mobile management is essential.

J. Robust Documentation and Knowledge Retention

Critical elements include:

- Maintaining a living documentation repository
- Keeping technical references updated
- Preparing change logs and release notes
- Ensuring new team members can quickly onboard
- Maintaining operational continuity even if individual personnel change

Well-maintained documentation protects long-term system integrity.

3.6 Development & Approach Methodology

3.6.1 Development & Implementation Methodology

The Consulting Firm must follow a structured, predictable, and quality-driven development methodology throughout the duration of this contract. Because this is a continuation and maintenance-focused engagement, the methodology must prioritize stability, backward

compatibility, controlled releases, and minimal service interruption. The approach must support both incremental improvements and strategic enhancements, ensuring that all changes are implemented in a controlled and technically sound manner.

The development & implementation methodology shall consist of the following key components:

A. Agile-Inspired Iterative Approach Adapted for Maintenance

The Consulting Firm shall adopt an agile-influenced iterative methodology suitable for continuous maintenance and enhancement work. This includes:

- Short development cycles
- Incremental feature delivery
- Continuous feedback incorporation
- Flexible adaptation to new requirements
- Prioritization based on urgency and impact

However, given platform criticality and stability requirements, the Consulting Firm must maintain a **hybrid model** that combines agile flexibility with traditional government-grade approval processes.

B. Requirement Analysis

For every maintenance issue, enhancement request, or new feature, the vendor must:

1. Perform requirement analysis
2. Conduct impact assessment
3. Document feasibility, constraints, and dependencies
4. Review with the Client for approval
5. Prepare a technical solution proposal

This ensures that all changes are fully understood before development begins, reducing risk to the live system.

C. Controlled Development Environment

The vendor must maintain separate environments for:

- Development
- Staging / UAT
- Production

All development work must be isolated from production until review and approval are completed.

The Consulting Firm must ensure:

- Code isolation
- Proper environment synchronization
- Controlled access rights
- Secure and validated deployment pipelines

D. Incremental Development and Feature Branching

The Consulting Firm must rely on feature branching and version-controlled development to ensure:

- Cleaner merges
- Isolation of parallel work
- Clear traceability
- Preservation of stable code in main branches

No development task may bypass version control under any circumstances.

E. Mandatory Code Review

All code changes must undergo:

- Peer review
- Static code analysis
- Function-level validation

This ensures removal of:

- Logic errors
- Unoptimized structures
- Security vulnerabilities
- Redundant code

Peer review must be documented through the issue tracking system.

F. Backward Compatibility & Non-Disruptive Enhancement

Since the system is already live and used nationwide, all development must:

- Avoid breaking existing features
- Ensure legacy compatibility
- Maintain database schema stability unless approved
- Include migration scripts if needed
- Ensure performance neutrality or improvement

Every enhancement must pass **regression testing** before deployment.

G. Documentation-Driven Development (DDD)

For every development or maintenance task, the vendor must update:

- Technical design notes
- API documentation

- Database schema changes
- Sequence diagrams (if applicable)
- Operational instructions
- User guides (for admin-facing improvements)

This ensures long-term readability and maintainability of the system.

H. Continuous Integration & Planned Releases

The Consulting Firm must maintain a structured release cycle that includes:

- Scheduled deployments
- Unscheduled hotfix deployments as required
- Release notes for every version
- Proper version tagging
- Pre-deployment checklist
- Post-deployment verification

High-risk deployments must be scheduled during low-traffic periods in coordination with the Client and hosting authority.

I. Emphasis on Refactoring and Code Health

The methodology must include a continuous and proactive approach to improving existing code:

- Removal of duplicate logic
- Breaking large blocks into smaller modules
- Improving object and function boundaries
- Updating outdated libraries
- Enhancing readability and maintainability

- Cleaning unused variables, functions, or data
- Reducing technical debt progressively

Refactoring must never introduce new bugs or break existing features.

J. Collaboration and Review with Client

Throughout the development cycle, the Consulting Firm must maintain:

- Weekly or bi-weekly review meetings
- Requirements validation sessions
- Demonstrations of completed features
- Transparent communication about risks or dependencies
- Documentation of all decisions

Client approval is mandatory for:

- Feature acceptance
- Release promotions
- Inter-agency integrations
- Major UI/UX changes
- Database-level structural updates

K. Quality Assurance as an Integrated Methodology Component

Testing must be embedded into each development cycle (details in 4.4.3). Every deliverable must be validated thoroughly before UAT.

L. Compliance with National Standards

Development methodology must comply with:

- ICT Division guidelines
- a2i digital service standards
- CIRT security advisories
- Government data hosting and privacy requirements

M. Transparent Change Management

The Consulting Firm must follow a structured change management process:

- Change Request (CR) documentation
- Impact analysis
- Client approval
- Development
- Testing
- Deployment
- Closure documentation

All changes must be logged and auditable.

3.6.2 System Design & Development Plan

The System Design & Development Plan outlines how the Consulting Firm will plan, design, structure, and deliver all maintenance, enhancement, and optimization activities throughout the contract period. Unlike a new system development project, this continuation contract focuses on maintaining the integrity of the existing architecture while gradually modernizing components, improving code quality, and delivering enhancements in a controlled and sustainable manner.

The Consulting Firm must follow a systematic, structured, and risk-aware approach to system design and development that ensures continuity of service and adheres to national standards.

A. Understanding and Preserving the Existing Architecture

Before any new development or enhancement begins, the Consulting Firm must conduct an in-depth analysis of:

- The current system architecture (frontend, backend, CMS, APIs, databases, search engines, caching layers)
- Dependencies and third-party libraries
- Data structures and schema relationships
- Workflow and RBAC logic
- Existing theme and template mechanics
- Connectivity and integration points

The objective is not to redesign the system but to preserve architectural stability while making improvements that enhance maintainability, performance, and future scalability.

B. Modular Enhancement Approach

All new enhancements, updates, and maintenance corrections must be designed in a **modular** manner. This ensures:

- Clear separation of responsibilities
- Minimization of cross-module impact
- Easier debugging and testing
- Improved readability and maintainability
- Simplified versioning and deployment

New modules must be loosely coupled and adhere to clean code principles.

C. Design Principles to Follow

The Consulting Firm must apply the following design principles:

1. Clean Architecture

- Separation of business logic and presentation layers
- Encapsulation of reusable functions
- Consistent naming standards
- Dependency inversion where beneficial

2. SOLID Principles

All enhancements must follow:

- Single Responsibility
- Open/Closed
- Liskov Substitution
- Interface Segregation
- Dependency Inversion

3. DRY (Don't Repeat Yourself)

Repeated logic or code blocks must be consolidated into shared components or utility functions.

4. API-First Approach

For any new feature requiring interaction between frontend, backend, and mobile apps, API contracts must be defined before implementation.

5. Backward Compatibility

No change may break existing workflows unless explicitly approved by the Client.

D. Development Planning and Task Breakdown

For each enhancement, fix, or improvement, the vendor must prepare:

1. A task breakdown
2. Time estimation
3. Risk and dependency identification

4. Data impact analysis
5. API impact or UI flow modifications
6. A micro-design or technical note

These documents must be submitted to the Client upon request.

E. Versioned Feature Development

Development must follow a **versioned release strategy**, such as:

- vX.X.M (Maintenance Release)
- vX.X.E (Enhancement Release)
- vX.X.H (Hotfix Release)

This ensures clear traceability between:

- Issues
- Enhancements
- Deployments
- Rollbacks

Release notes must be produced for every version.

F. UI/UX Design Consistency

All UI/UX updates must:

- Reflect modern design principles
- Follow national branding guidelines
- Be responsive across all devices
- Align with WCAG 2.1 accessibility standards

- Use consistent color palettes, typography, and interaction patterns

Any major UI change must be approved by the Client before development.

G. Database Design Considerations

Any modification involving database changes must:

- Maintain referential integrity
- Avoid downtime
- Maintain backward compatibility
- Follow a version-controlled migration script
- Include rollback procedures
- Be tested in staging with real data samples

Database optimization must be continuous and measurable.

H. Integration Design & API Management

For new or modified integrations:

- API request/response structures must be documented
- Authentication methods must be secure and standardized
- Rate limits, error handling, and fallback methods must be defined
- Integration logs must be tracked and analyzed

Vendor must participate in joint testing with external platform teams.

I. Search Engine Enhancement Planning

For Solr/Elastic enhancements:

- Indexing logic must be clearly designed
- Schema changes must be tested thoroughly
- Ranking algorithms must be evaluated for relevance
- Performance and latency benchmarks must be documented
- Load testing scenarios must be created where applicable

J. Mobile App Design Planning

Enhancements to Android or iOS apps must:

- Maintain compatibility with backend APIs
- Consider OS-level changes
- Follow standard design guidelines
- Be optimized for performance and memory usage
- Include updated push notification logic where applicable

Mobile app releases must be planned with the Client, including store approval timelines.

K. Zero-Disruption Deployment Planning

The development plan must ensure:

- Zero or minimal downtime
- Blue-green or rolling deployment where feasible
- Prior deployment validation in staging
- A rollback plan for every release
- Careful sequencing when multiple modules are updated

L. Documentation as Part of the Design Plan

Every enhancement must result in:

- Updated architectural diagrams (if impacted)
- Revised API documentation
- Updated user/admin manuals
- Release notes and deployment notes
- Technical design notes

4.4 Development & Approach Methodology (Continued)

3.6.3 Testing Plan

The Testing Plan outlines the systematic approach for validating all maintenance fixes, enhancements, new features, refactoring updates, and integrations. Given the mission-critical nature of the National Portal Framework, the Consulting Firm must adopt a rigorous and multi-layered testing methodology to ensure system integrity, accuracy, stability, and backward compatibility. Provide proper documentation during these phase is necessary.

A. Types of Testing

The Consulting Firm must perform the following:

1. **Unit Testing**
    - Mandatory for all refactored and newly developed components
    - Ensures logical correctness at component level
2. **Functional Testing**
    - Validates new features, existing functionality after maintenance
    - Ensures functional correctness against requirements
3. **Regression Testing**
    - Essential after every release and code change

- Prevents reappearance of previously resolved issues
- Must cover all critical paths and workflows

4. **Integration Testing**
    - Verifies smooth interaction between modules and APIs
    - Ensures stable communication with external systems such as MyGov, Doptor, SMS gateway, etc.
5. **Performance Testing**
    - Ensures system responsiveness and resource optimization
    - Must include load, stress, and endurance testing when required
6. **Security Testing**
    - Ensures compliance with OWASP Top-10
    - Identifies vulnerabilities in authentication, sessions, APIs, and inputs
    - Addresses issues raised by CIRT or external auditors
7. **UI/UX & Accessibility Testing**
    - Ensures WCAG 2.1 compliance
    - Validates responsive behavior across devices and browsers
8. **Mobile App Testing**
    - Device compatibility testing
    - API alignment testing
    - App performance, crash, and memory usage testing

B. Testing Environment

The Consulting Firm must maintain:

- A dedicated **Staging/UAT environment** for testing

- A **sandbox environment** for integration tests
- Clear separation between development, staging, and production environments
- Proper access control for testers and Client representatives

C. Test Cases, Scripts, and Reporting

The vendor must maintain:

- Test case documents
- Test scripts for repetitive tests
- Testing checklists
- Screenshot or video proof for critical tests
- A centralized test report for every release
- Bug lifecycle documentation (open → assigned → resolved → verified → closed)

3.6.4 User Acceptance Test (UAT)

User Acceptance Testing is an essential step in validating all deliverables before production release. UAT ensures that the system meets the Client's functional expectations and does not introduce any operational risks. a2i will bear related official procedure & expenses - i.e., venue, logistics, travel, accommodation, food, TA/DA, Honorarium of participants etc.

A. UAT Execution

- All features and fixes must be deployed to UAT environment
- Consulting Firm must provide a demonstration of changes/fixes
- Client will conduct functional approval testing
- Consulting Firm must support debugging during UAT

B. UAT Documentation

Vendor must submit:

- UAT test results summary
- Known issues list
- Final approval request
- Release readiness confirmation

No release may proceed to production without explicit UAT sign-off.

3.6.5 Migration of Legacy Data (If any)

Although this contract primarily concerns maintenance and enhancement, occasional data migration tasks may arise (e.g., schema updates, module upgrades, integration restructuring).

Vendor Responsibilities

- Analyze data mapping requirements
- Write migration scripts with rollback capability
- Ensure no data loss, corruption, or inconsistency
- Conduct dry runs in staging
- Obtain Client approval before executing on production

All migration activities must be logged and documented.

3.6.6 Risk Management Plan

The Consulting Firm must maintain an active risk management process to identify, categorize, mitigate, and track risks associated with maintenance and enhancement activities.

A. Risk Categories

1. **Technical Risks**

- Code vulnerabilities
- Integration failures
- Refactoring side effects
- Database inconsistencies

2. **Operational Risks**
    - Downtime during deployment
    - Performance degradation
    - Server/environment issues
3. **Security Risks**
    - Unauthorized access
    - Data breach
    - Misconfigured APIs
4. **Project Management Risks**
    - Delayed delivery
    - Resource shortages
    - Communication gaps

B. Mitigation Strategies

Vendor must:

- Maintain detailed risk logs
- Assign severity and priority levels
- Conduct RCA for major incidents
- Prepare fallback plans for deployments

- Escalate high-impact risks immediately to Client

3.6.7 Deployment & Implementation Plan

Deployment must be performed carefully to ensure uninterrupted service. Vendor must maintain a disciplined deployment process.

A. Deployment Process

1. Code delivery to staging
2. Cross-team validation
3. UAT sign-off
4. Approval for production
5. Scheduled deployment during low-traffic hours
6. Post-deployment verification
7. Rollback (if necessary)

B. Deployment Controls

- Version tagging
- Change logs
- Automated or semi-automated deployment scripts
- Zero-downtime deployment methods when possible (blue-green, rolling, etc.)

C. Coordination with Hosting Authority

Vendor must coordinate with:

- NDC/hosting personnel
- a2i system administrators
- Network and security teams

3.6.8 Training and Knowledge Transfer Plan

The vendor must provide training and capacity support throughout the contract. a2i will bear related official procedure & expenses - i.e., venue, logistics, travel, accommodation, food, TA/DA, Honorarium of participants etc.

A. Types of Training

1. **Technical Training**
    - For developers, technical officers, programmers
2. **Operational Training**
    - For editors, administrators, and content managers
3. **Hands-on Demonstration Sessions**
    - Conducted as needed for new features

B. Knowledge Transfer Documents

- Updated user manuals
- Technical manuals
- Change logs
- Training slide decks
- Video guides (if applicable)

C. Institutionalizing Knowledge

At the end of the contract, the vendor must:

- Conduct knowledge transfer workshops
- Provide final documentation packages
- Ensure Client team can sustain operations

3.6.9 Support & Maintenance Plan

This contract requires ongoing technical support and structured maintenance.

A. Support Services

1. **Incident Management**
    - Logging, categorization, escalation, and resolution
    - SLA adherence
2. **Problem Management**
    - RCA preparation
    - Permanent fixes for recurring issues
3. **Change Management**
    - Controlled introduction of new features
    - Impact analysis and documentation
4. **Release Management**
    - Planned monthly releases
    - Emergency hotfix releases

B. Maintenance Activities

- Code refactoring
- Library and framework updates
- Database optimization
- Search index tuning
- Security patching
- Performance monitoring
- Log analysis

- API health monitoring
- Mobile app upkeep

C. Monitoring & Reporting

Monthly reports must include:

- Issues resolved
- Enhancements delivered
- SLA compliance
- Performance metrics
- Security observations

Minimum Service Level Agreement (SLA)

SLA compliance is a mandatory condition of this contract. Failure to meet SLA requirements may lead to penalties, warnings, or termination as per Government rules.

Support Response & Resolution Times

A. Critical Issues (System Down / Major Function Broken)

- Response time: Within 10 minutes
- Work starts: Immediately
- Resolution time: Within 2 hours

B. High Severity Issues (Service Impacting but not Down)

- Response time: Within 30 minutes
- Work starts: Within 1 hours
- Resolution time: Within 6 hours

C. Medium Severity Issues

- Response time: Within 2 hours
- Resolution time: Within 1 working day

D. Low Severity / Minor Fixes

- Response time: Within 8 hours
- Resolution time: Within 3 working days

Enhancement Delivery SLA

Enhancements, new features, or thematic improvements shall be delivered within a mutually agreed timeline based on complexity:

- Small enhancement: 5–7 working days
- Medium enhancement: 7–15 working days
- Large enhancement: timeline to be mutually determined

No enhancement may be delayed without written justification.

Uptime Requirement

The vendor must ensure:

- 99.9% system uptime (excluding scheduled maintenance)

Any deviation must be reported with justification and RCA.

Reporting Requirements

The vendor must submit monthly SLA compliance reports including:

- Issue logs
- Resolution times
- Performance metrics
- Downtime statistics
- Support and operational activities

3.6.10 Work Distribution & Team Composition

The Consulting Firm must deploy a qualified, dedicated team with the expertise needed to maintain and enhance a nationwide digital system.

Sl.	Key Position	No.	Job Description	Required Minimum Qualification
1	Project Manager (K1)	01	• Discussing potential projects and their parameters with clients, executives, and software developers. • Planning out the blueprints for software projects, including defining the scope, allocating resources, setting deadlines, laying out communication strategies, and indicating tests and maintenance. • Assembling and leading the project team. • Participating in and supervising each stage of the project. • Ensuring each project stays on schedule and adheres to the deadlines. • Tracking milestones, deliverables, and change requests. • Serving as a liaison to communicate information regarding changes, milestones reached, and other pertinent information. • Delivering completed software products to clients and performing regular checks on the products' performance.	• Minimum academic requirement is graduation in Computer Science and Engineering/ICT. • Minimum 5 years of experience in managing large scale IT projects with a total of 10 years of experience in ICT industry.

2	Business Analyst (K2)	01	• Incorporate new technology into the current system. • Advise on system upgrades and oversee software audits. • Diagnose and repair inventory errors. • Respond to end-user needs. • Design and maintain data processing systems. • Modify scripting and evaluate coding. • Implement timelines for IT staff. • Create and draft technical requirements, specifications, and policies. • Stay up to date on the latest technological innovations and trends.	• Minimum graduate degree in any relevant discipline from a reputed university. • Minimum 3 years of experience in business system analysis & relevant experience in the corporate field.
3	System Architect (K3)	01	• Building and integrating information systems to meet the project's needs. • Assessing the systems architecture currently in place and working with technical staff to recommend solutions to improve it. • Resolving technical problems arise. • Providing supervision and guidance to development teams. • Continually researching current and emerging technologies and proposing changes where needed.	• Minimum graduate degree in any relevant discipline from a reputed university. • Minimum 3 years of experience in Solution Architect & relevant experience in the corporate field.

			• Informing various stakeholders about any problems with the current technical solutions being implemented. • Assessing the business impact that certain technical choices have.	
4	Sr. Software Engineer (K4)	02	• Serve as a Technical Lead contributing to and directing the efforts of development teams, including internal and external team members. • Contribute to the ongoing evolution of the existing content supply portfolio of applications and services. • Design, develop, modify, implement, and support software components anywhere in the Software stack. • Determine root cause for the most complex software issues and develop practical, efficient, and permanent technical solutions. • Remain current on new technologies and available firm packages; evaluate and make recommendations as necessary. • Assist in task planning, estimation, scheduling, and staffing. • Mentor Software Engineers to allow for skill/knowledge development through advice, coaching, and training opportunities. • Determine process improvements, best practices, and develop new processes.	• Minimum graduate in Computer Science and Engineering / relevant subjects • Minimum 5 years of experience in the field of IT solution development. • Must have experience in web and mobile application development in government domain.

5	Software Engineer (K5)	04	• Developing and directing software system validation and testing methods. • Directing our software programming initiatives • Overseeing the development of documentation. • Analysing data to effectively coordinate the installation of new systems or the modification of existing systems. • Managing the software development lifecycle. • Monitoring system performance. • Communicating key project data to team members and building cohesion among teams. • Developing and executing project plans. • Applying mathematics and statistics to problem-solving initiatives. • Applying best practices and standard operating procedures. • Creating innovative solutions to meet our company's technical needs. • Testing new software and fixing bugs. • Shaping the future of our systems.	Minimum graduate in Computer Science and Engineering / relevant subjects • Minimum 3 years of experience in the field of IT solution development.
6	Data Base Administrator (K6)	01	• Monitoring system performance and identifying problems that arise. • Responding in a timely manner to user-reported errors.	• Minimum graduate in Computer Science and Engineering/ICT or any relevant field.

			• Protecting the database against threats or unauthorized access. • Ensuring that the database is adequately backed up and able to be recovered in the event of memory loss. • Reporting on metrics regarding usage and performance. • Suggesting changes and improvements for maintenance or protection. • Regularly liaising with IT project managers and database programmers. • Designing databases with both front-end and back-end users in mind.	• Minimum 5 years' experience in Database design, development and administration using multiple Database including MySql/ Mongodb/ SQL Server and NoSql.
7	Security Expert (K7)	01	• Implement, manage, and monitor security measures to protect the hosting infrastructure and all e-Government applications. • Conduct regular security assessments, vulnerability scans, and penetration tests to identify and address security gaps. • Configure and maintain firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and other security devices. • Develop and enforce security policies, standards, and guidelines to ensure compliance with ICT security frameworks and best practices. • Investigate security incidents, analyse breaches, and implement corrective measures to prevent recurrence.	• Bachelor's degree in Computer Science, Information Technology, or a related discipline. • Minimum 5 years of hands-on experience in IT security, network security, or information security roles. • Relevant professional certifications such as CEH, CISSP, CISM, CompTIA Security+, or equivalent will be an added advantage.

			• Perform regular patching and updates of operating systems, network devices, and security tools to address emerging threats. • Implement strong authentication and access control mechanisms to protect data and ensure proper user authorization. • Implement log visualization tools, monitor security logs, generate reports, and provide actionable insights to improve the security posture of the hosting environment. • Coordinate with other technical teams to embed security into the entire IT lifecycle, including design, deployment, and operations. • Prepare security-related documentation and participate in audits, reviews, and capacity-building exercises for continuous improvement.	
8	Mobile Application Developer – Android (K8)	01	• Create and maintain mobile applications (Android Platform). • Keep abreast of the latest technology for mobile applications. • Work with computer engineers to brainstorm new applications. • Create UI tests to source analytics.	• Minimum graduate in Computer Science and Engineering/ICT or any relevant field. • Must have 5 years of experience in Mobile application development - Android.
9	Mobile Application Developer – IOS	01	• Create and maintain mobile applications (IOS Platform).	• Minimum graduate in Computer Science and Engineering/ICT or any relevant field.

	(K9)		• Keep abreast of the latest technology for mobile applications. • Work with computer engineers to brainstorm new applications. • Create UI tests to source analytics.	• Must have 5 years of experience in Mobile application development – IOS
10	Infrastructure Expert (K10)	01	• Design the deployment architecture • Installing and maintaining operating environments. • Monitoring these operating environments. • Responding effectively and speedily to any problems. • Maintaining a professional demeanour with clients and colleagues. • Providing training and support. • Ensuring operating environments stay safe and secure. • Updating any software and hardware where necessary. • Documenting all reported malfunctions and actions taken in response.	• Minimum graduate in Computer Science and Engineering or relevant subjects. • Minimum 5 years of progressive experience Develop and maintain infrastructure in cloud environments to power different standard networks ensuring the highest security standards and best-practices.
11	Infrastructure Engineer (K11)	01	• Installing and maintaining operating environments. • Monitoring these operating environments. • Responding effectively and speedily to any problems.	• Minimum graduate in Computer Science and Engineering or relevant subjects. • Minimum 3 years of progressive experience Develop and maintain infrastructure in cloud

			• Maintaining a professional demeanour with clients and colleagues. • Providing training and support. • Ensuring operating environments stay safe and secure. • Updating any software and hardware where necessary. • Documenting all reported malfunctions and actions taken in response.	environments to power different standard networks ensuring the highest security standards and best-practices.
12	Security Engineer (K12)	02	• Monitor SIEM (Security Information and Event Management) systems, IDS/IPS, firewalls, antivirus logs, and cloud security alerts. • Perform root cause analysis of critical incidents and prepare post-incident reports with actionable recommendations. • Regularly analyze threat intelligence feeds and apply threat-hunting techniques to detect advanced persistent threats (APTs). • Document all security alerts, findings, and actions taken in the incident management system in compliance with SOPs. • Assist in maintaining and updating security monitoring tools, dashboards, and threat detection rules. • Follow incident response procedures and support containment, eradication, and recovery efforts under guidance.	• Minimum graduate in Computer Science and Engineering or relevant subjects. • Minimum 3 years of progressive experience in analysing complex business problems to be solved with automated systems

			• Conduct daily health checks on security tools, log collection status, and threat feeds. • Participate in continuous learning on threat landscapes, security operations, and emerging attack techniques	
13	DevOps Expert (K13)	01	• building and setting up new development tools and infrastructure • understanding the needs of stakeholders and conveying this to developers • working on ways to automate and improve development and release processes • testing and examining code written by others and analysing results • ensuring that systems are safe and secure against cybersecurity threats • identifying technical problems and developing software updates and 'fixes' • working with software developers and software engineers to ensure that development follows established processes and works as intended	• Minimum graduate in Computer Science and Engineering or relevant subjects. • Minimum 5 years of experience Dev-ops. • Must have experience of working with tools like Git, Jenkins, Selenium, Docker, Kubernetes, Puppet, Chef, Ansible, Nagios etc
14	QA Engineer (K14)	02	• Meeting with the product design team to determine product testing parameters. • Writing test plans and creating test cases for the product. • Conducting quality assurance and designing performance tests using the new testing procedures.	• Minimum graduate in Computer Science and Engineering or relevant subjects. • Minimum 3 years of progressive experience in the sector of software

			• Troubleshooting any errors and streamlining the testing procedures. • Writing up the final QA and test procedures for the quality technicians. • Preparing test reports	testing and quality assurance
15	Technical Documentation Expert (K15)	01	• Organizing an archiving system. • Labelling, sorting and categorizing documents for ease of use. • Retrieving documents upon request. • Outlining a long-term storage strategy. • Adhering to regulatory requirements. • Ensuring documentation integrity. • Controlling access to documents. • Removing documents that are obsolete. • Utilizing storage software and applications for electronic filing. • Performing transcription and conversion work. • Proofreading documents upon request.	• Minimum graduate in Computer Science and Engineering/ICT or any relevant field. • Minimum 3 years' experience of working with enterprise software development team with the role of documenting requirements, SRS, DFD, ERD etc.
16	Support Executive (K16)	03	• Responding to support requests. • Meeting with team to diagnose software, networking, or hardware issues. • Providing technical support on-site or via remote-access systems.	• Minimum graduate in Computer Science and Engineering/ICT or any relevant field. • Minimum 3 years' experience in relevant field

			• Offering solutions that meet the needs of the client. • Repairing hardware malfunctions, software issues, and networking problems. • Maintaining good client relations. • Tracking and managing work records. • Compiling job reports.	
17	UI Designer (K17)	01	• Improve the look and feel of interactive computers and product software • Create overall concepts for the user experience within a business webpage or product, ensuring all interactions are intuitive and easy for customers • Analyse customer responses and website data to determine high traffic web pages and why some perform better than others • Design the aesthetics to be implemented within a website or product, from the layout menus and drop-down options to colors and fonts • Build storyboards to conceptualize designs and convey project plans to clients and management • Account for and track the human-computer interaction (HCI) element of a design • Create surveys for research through various social media platforms to gather feedback on user's ease of use	• B.Sc. in computer engineering/science/ mathematics /statistics or any relevant field. • Must have 5 years' experience in designing web and mobile applications.

			• Conduct testing of completed applications, websites and software to Assess user experience	
18	UX Expert (K18)	01	• Do Research from Users (Research) • Build User Persona (Analysis) • Create User Stories/Scenario Map/Sitemap (Analysis) • Start creating Wireframes and Interaction Prototypes (Design) • UI - visual design • Metrics Analysis (Validate designs)	• B.Sc. in computer engineering/science/ mathematics /statistics or any relevant field. • Must have 3 years' experience in User Experience design (Please provide project details worked, roles and Journey process). •
19	Project Coordinator (K 19)		• This role will make collaboration act as bridge among Team leader of Digital Service-1, Domain Team & Firm. • Liaise between the development team and the domain team to ensure effective communication and collaboration. • Facilitate meetings between the development team and the domain team to review project progress, identify challenges, and develop solutions. • Ensure that project requirements are clearly defined and communicated to the development team. • Ensure that project timelines are met and that progress is reported to the domain team.	• Minimum graduate in any subject • At least 3 years of experience in the field of business requirement study, analysis and Implementation for ICT based or Software projects.

3.6.11 Expected Deliverables

Sl.	Deliverable	Timeline	Payment
1	Project Inception Report	1st Month	2%
	System Maintenance and Support of all systems (all Offices) with maintenance support service approved report		4%
2	Technical Overview Report on National portal	2nd Month	2%
	System Maintenance and Support of all systems (all Offices) with maintenance support service approved report		4%
3	Approved NPF Optimization & Enhancement Plan	3rd Month	5%
	Updated Software Requirements Specification (SRS) & System Design Documents (SDD)		5%
	System Maintenance and Support of all systems (all Offices) with maintenance support service approved report		4%
4	Quarterly Testing Report	4th Month	2%
	Approved five (5) theme delivery		6%
	System Maintenance and Support of all systems (all Offices) with maintenance support service approved report		4%
5	Enhanced & optimized version of NPF	6th Month	15%
	Quarterly Testing report		5%
	Approved five (5) theme delivery		6%
	System Maintenance and Support of all systems (all Offices) with maintenance support service approved report		8%
6	Approved VAPT Report from authorized organization	7th Month	4%
	Quarterly Testing report		2%
	Approved Knowledge Transfer Completion Report		3%
	Technology Handover completion report		4%

	Technical Document Transfer report		3%
	Source Code Handover with latest build		3%
	Project Closing Report		5%
	System Maintenance and Support of all systems (all Offices) with maintenance support service approved report		4%

The vendor must deliver the following documents throughout the contract in accordance with the above-mentioned deliverables:

A. Periodic Deliverables

- Maintenance support service approved report
    - Monthly maintenance report
    - Monthly technical performance report
    - Monthly SLA compliance report
    - Issue logs and resolutions
- Updated documentation
- Release notes for each deployment

B. Technical Deliverables

- New features/enhancements as assigned
- Code refactoring outputs
- Updated API documentation
- Updated architecture diagrams
- Testing Report
- Security Report
- Deployment Guideline

C. Training & Knowledge Materials

- User manuals
- Technical manuals
- Training session materials
- Final knowledge transfer package

D. Final Project Completion Deliverables

At the conclusion of the contract:

- Comprehensive documentation bundle
- Fully updated code repositories
- Final technical audit response set
- Knowledge transfer handover documents