

Terms of Reference

Design, Development, Hosting and Maintenance of a Secure Official Website for NMHD

Client / Beneficiary	National Mental Health Department (NMHD)
Document Type	Terms of Reference (TOR)
Assignment	Official bilingual website, CMS, integrations, hosting and support
Technology Baseline	Laravel, Vue, PostgreSQL, Node.js, Docker-based hosting

Background

The National Mental Health Department (NMHD) is responsible for planning, implementing, and coordinating mental health services, prevention, promotion, and awareness programmes nationwide. To strengthen public access to reliable mental health information and services, NMHD intends to hire a qualified firm or individual consultant to design, develop, host, secure, operationalize and support an official website for the Department.

The NMHD website will serve as an official dissemination, awareness, advocacy and public-service information platform. It shall provide information on NMHD's mandate, services, programmes, announcements, laws and regulations, careers, mental health resources, referral pathways, and public communications. The system shall support bilingual content in English and Dhivehi and must be designed to accommodate future expansion, integrations and digital service workflows.

The website will cater to government institutions, service providers, health-sector stakeholders, media organizations, NGOs, development partners and the general public. Considering the subject matter and public trust implications, the solution must be professional, highly secure, accessible, resilient, high-performing and maintainable by authorized NMHD staff.

1. Objectives of the Assignment

- Design, develop and deploy a bilingual English and Dhivehi official website for NMHD that is accessible, user-friendly, secure and responsive across desktop, tablet and mobile devices.

- Provide a robust content management platform enabling authorized NMHD staff to manage pages, announcements, news, publications, awareness materials, media galleries and service information without code-level changes.
- Establish a modern application architecture using Laravel, Vue, PostgreSQL and Node.js, hosted through a Docker-based setup suitable for controlled deployment, versioning, portability and future scaling.
- Implement website security controls, auditability, role-based access, secure authentication, hardened hosting, backup, disaster recovery, monitoring, logging and handover documentation appropriate for a high-requirement government system.
- Integrate authentication and communication services including OAuth-based login, email notifications and a separate SMS microservice for SMS queueing, provider integration, message templates, delivery tracking and administration.
- Improve public access to accurate mental health information, NMHD services, programmes, referral pathways, awareness campaigns and official announcements.

2. Scope of Work

Under the overall guidance of NMHD, the Consultant shall undertake end-to-end discovery, design, development, testing, deployment, hosting setup, documentation, training, handover and post-launch support. The scope shall include all activities required to deliver a production-ready, secure and maintainable system.

2.1 Planning, Discovery and Creative Design

- Conduct inception discussions with NMHD to confirm stakeholders, user groups, content structures, workflows, approval processes and functional priorities.
- Prepare an information architecture, sitemap, navigation model, wireframes and page templates for NMHD review and approval.
- Propose an overall look and feel aligned with NMHD's mandate, public communications needs and target audiences.
- Apply modern UI/UX practices to ensure usability, readability, accessibility, mobile responsiveness and visual consistency.
- Provide structured design iterations based on NMHD feedback, including at least three key page mock-ups before development begins.
- Design the platform as a high-visibility public service system, with clear content hierarchy, fast access to urgent information, trust-building presentation and simple navigation for the public.

The website design shall:

- Be responsive and fully compatible with current mobile, tablet and desktop browsers.
- Have a clean, professional, accessible and user-friendly interface.
- Support English and Dhivehi versions with easy language switching and properly configured fonts that render without user device installation.

- Include accessibility and inclusivity features such as keyboard navigation, screen-reader compatible markup, alternative text, captions, contrast-compliant design and accessible form labels.
- Ensure consistent visual identity across fonts, colors, icons, layouts, buttons, cards, forms, alert banners and downloadable resources.
- Display NMHD organizational information, contact details, geographical location and public communication channels.
- Comply with applicable government website, data protection and information governance requirements communicated by NMHD.
- Include privacy-aware analytics functionality for website usage, content performance and system health reporting.

2.2 Website Development and CMS

- Develop the system in accordance with approved design, architecture and functional specifications.
- Implement a CMS/admin portal allowing content and components to be managed without direct code editing.
- Support content workflows with configurable roles such as Super Administrator, Administrator, Editor, Publisher, Media Manager, Report Viewer and Read-only Viewer.
- Provide role-based permission controls for pages, content types, media uploads, publication approval, user administration and configuration management.
- Provide role customization using permissions. Custom role creation by selecting required permissions.
- Support draft, review, publish, unpublish, archive and scheduled publishing workflows where applicable.
- Ensure compatibility with current versions of major browsers and optimize performance, security and maintainability.
- Avoid dependency on uncontrolled plugin-heavy themes; where reusable components are required, they must be documented, maintained and compatible with the selected technology stack.

2.3 Functional Requirements

The website shall include, but not be limited to, the following functional areas.

Functional Area	Minimum Requirement
Core Public Pages	Home; About NMHD; Services; Department Structure; News and Publications; Awareness Messages and Articles; Laws and Regulations; Careers; Contact and Location; Frequently Asked Questions; Referral Pathways.
Page Editors	Dynamic page editors with core features such as text formatting, picture inserting and formatting, alignments, inserting links, inserting code snippets, column management, inserting buttons and links
Content and Media Management	Add, edit, delete, archive and schedule pages and sections; upload and manage images, videos, documents and

	downloadable resources; manage news and events with galleries and attachments; automatic image optimization; high-resolution downloads where required.
Downloads and Announcements	Upload publications, job vacancies, newsletters, circulars, annual reports and other materials in HTML, PDF, Word or other approved formats; mark items as New, Expired or time-bound; maintain date stamps and metadata.
Search and Data	Site-wide search across pages, posts, publications and resources; searchable categories, tags and filters; ability to publish statistical data related to NMHD mandate and programmes.
Interactive Features	Complaint and feedback forms for different NMHD sections; configurable home page banner; rotating announcements; awareness campaign modules; countdown timers used only when required; social media feed integration.
Administration	User management, role permissions, audit logs, content approval, media library management, system settings and reporting dashboards.
Accessibility and Bilingual Content	Full English and Dhivehi content management with language-specific fields, RTL-aware presentation where required, accessible forms, alt-text governance and browser/device testing.
Data Ingestion & State Management	Reactive Data Binding: The component must accept datasets via properties (props) and automatically re-render the visualization when the underlying data changes. Asynchronous Loading States: It must display a visual loading indicator (like a skeleton loader or spinner) while fetching data from the API endpoint. Error & Empty States: If the API returns a 404, a 500 error, or simply an empty array, the component must gracefully display a fallback message (e.g., "No data available for this period") rather than rendering a broken canvas.
Rendering & Configuration	Dynamic Chart Types: The component must support switching between fundamental chart types (Line, Bar, Pie, Scatter) based on a configuration prop.

	Responsive Scaling: The canvas or SVG container must be fluid, automatically resizing its width and height to fit the parent container, whether on a desktop monitor or a mobile device. Theming & Styling: It must accept configuration objects for colors, axis labels, and grid lines to ensure the charts match the application's global design system.
Registries and API	Published registries based on NMHD requirement and custom API configuration setup to allow issuing API access to these registries for third parties where required. User managing the website should be able to create new custom registries with custom data columns. Further configure API access and issue tokens to access individual registries from admin panel.
Department / Service registry	Searchable service registry allows users to search through services provided by the office. Allow profiling major programs under office with basic details and attached photo galleries.
API Endpoint	API endpoint for registries is integrated into the website with the API key management admin interface. Include view and manage scopes for each collection which can be exposed through the endpoint.
Chat Bot	Website must have a chat bot available. A knowledge base must be available on the website CMS, allowing staff to update information on FAQs. Further chatting with agents must be available.

2.4 Homepage Requirements

- Clear navigation menu with priority access to services, referral information, announcements and resources.
- Prominent banner area for major public notices and campaigns.
- NMHD contact details, location information and official channels.
- Mental health awareness messages and emergency or referral pathway notices where approved by NMHD.
- Recent news, publications, announcements and campaign highlights.
- Key statistics, programme highlights and important public information cards.
- Social media feed integration where approved and privacy compliant.
- Performance-optimized homepage assets to support fast loading on desktop and mobile networks.
- Homepage customization through web admin portal. Custom configuration options for each sections such as visibility and content depth.

2.5 Technology and Architecture Requirements

The proposed system shall be implemented as a modern application platform with clear separation between presentation, backend services, database, jobs, integrations and hosting environment. The solution shall be suitable for a large-scale, high-requirement public sector system.

Component	Requirement
Backend framework	Laravel / node.js shall be used for backend application logic, APIs, CMS/admin services, authentication integration, authorization, queues, notifications and configuration management.
Frontend framework	Vue / react shall be used for interactive frontend components, admin interface components and responsive user-facing interfaces where required.
Database	PostgreSQL shall be used as the primary relational database for content, users, configurations, forms, logs and structured records.
Runtime and tooling	Node.js shall be used for frontend build tooling, package management, asset compilation and any approved supporting services.
Containerization	Docker shall be used to package application services, database-related support components, queues, workers and supporting infrastructure configuration for repeatable deployment.
API design	The platform shall expose internal APIs using secure, documented and version-aware practices for frontend, admin and integration use cases.
Queues and jobs	Background workers shall be used for email, SMS, image processing, scheduled publishing, search indexing, analytics processing and other long-running tasks.
Search and indexing	The Consultant shall propose a scalable search approach suitable for website content, publications, tags, categories and bilingual content.

Architecture Expectation

- The solution shall not be treated as a simple static website. It shall be architected as a maintainable government digital platform with CMS, integrations, auditability, deployment automation and expansion capacity.
- The Consultant shall submit a technical architecture diagram, environment diagram, deployment flow, data flow and security control matrix before implementation.

2.6 Hosting, Deployment and Docker Setup Requirements

- Provide a Docker-based deployment setup with documented Dockerfiles, docker-compose or equivalent orchestration configuration, environment variable templates and deployment instructions.
- Separate application services for web server/reverse proxy, Laravel application, queue workers, scheduler, frontend build process, PostgreSQL database connectivity, cache/session services and SMS microservice integration.
- Implement HTTPS/TLS configuration, secure reverse proxy setup, security headers and controlled exposure of only required public ports.
- Support environment separation for development, staging/UAT and production, with environment-specific configuration and secrets management guidance.
- Implement automated database migration and rollback procedure, controlled seed data approach and release tagging.
- Provide backup and restoration procedure for database, uploaded media, configuration files and logs.
- Provide monitoring and operational checklists for container health, disk usage, service availability, SSL certificate status, queue status, scheduled jobs and backup completion.
- Ensure deployment documentation is specific enough for NMHD or Ministry technical staff to redeploy the system from source-controlled code and configuration.
- CI / CD setup available in the source-controlled folder

2.7 Security Requirements

Given the public-sector and health-related context, security shall be a core requirement throughout design, development, testing, deployment and support. The Consultant shall provide documented evidence of security controls and testing before go-live.

Security Area	Minimum Requirement
Secure Development	Secure coding practices; input validation; output encoding; CSRF protection; XSS prevention; SQL injection prevention; server-side validation; dependency review; secure error handling; no secrets in source code; peer review before release.

Authentication and Authorization	OAuth integration where approved by NMHD; role-based access control; least privilege; secure password policy for local administrative accounts if any; MFA readiness; account lockout and session timeout; configurable access permissions.
Data Protection	Encryption in transit through HTTPS/TLS; secure storage of credentials and secrets; protection of personally identifiable information submitted through forms; privacy-by-design for analytics and logs; retention and deletion procedures.
Infrastructure Hardening	Minimal exposed services; hardened Docker images; regular patching approach; non-root containers where feasible; secure file permissions; disabled debug mode in production; production configuration review.
Application Security Testing	Vulnerability assessment, dependency scan, configuration review, authentication and authorization testing, form and file upload security testing, API testing and remediation of critical/high findings before launch.
Logging and Auditability	Administrative audit logs for user changes, content publishing, configuration changes, login attempts and integration actions; logs shall avoid storing sensitive data unnecessarily.
File and Media Security	Allowed file types, file size limits, virus/malware scanning approach where available, secure storage of uploads, protection against executable uploads and safe handling of public downloads.
Availability and Recovery	Backup and restore testing, disaster recovery procedures, uptime monitoring, rate limiting, cache strategy, queue monitoring and documented incident escalation process.

2.8 Integration Requirements

- OAuth: Integrate OAuth-based authentication for authorized administrative users where approved by NMHD, including secure redirect URI handling, role mapping and fallback administrative access procedures.
- Email: Implement email notification capability for approved workflows such as feedback submissions, administrative alerts, account actions, publication approvals, system warnings and support communications.

- SMS: Implement SMS functionality through a separate SMS microservice responsible for message templates, queue management, provider API integration, delivery status tracking, retry handling, throttling and administrative monitoring.
- Microservice boundary: The SMS microservice shall be independent from the main CMS application and communicate through secure API calls or message queues with authentication, logging and error handling.
- Configuration: All integration credentials, provider URLs, sender IDs, templates and environment values shall be configurable without code changes and shall not be committed to source control.
- Audit and reporting: Email and SMS dispatch events shall be logged with status, timestamp, triggering module, recipient reference where appropriate and failure reason, while avoiding unnecessary exposure of sensitive message content.
- Future integrations: The system architecture shall allow future integration with government identity, data exchange or service platforms if instructed by NMHD.

2.9 Performance, Scalability and Reliability

- The website must be optimized for fast page loading, efficient asset delivery, caching, compressed images and performance on mobile networks.
- The application shall support traffic spikes during public campaigns, announcements and mental health awareness events through caching, queueing and scalable deployment practices.
- Database queries shall be optimized and indexed appropriately for content listing, search, filtering and reporting functions.
- The Consultant shall provide performance testing results, including baseline response time observations and remediation actions for bottlenecks discovered during testing.
- The platform shall include monitoring guidance for uptime, container health, queue workers, scheduled jobs, backup checks, disk usage and application errors.

2.10 Governance, Compliance and Content Management

- Support structured content ownership, review and approval workflows aligned to NMHD's internal governance needs.
- Maintain revision history or audit logs for critical content and configuration changes.
- Comply with applicable government website standards, accessibility requirements, information governance instructions and data protection requirements communicated by NMHD.
- Include privacy notice, accessibility statement, terms of use and contact/feedback channels as approved by NMHD.
- Ensure all content, designs, code, documentation and configurations are handed over to NMHD without vendor lock-in.

3. Testing, UAT and Knowledge Transfer

- Conduct functional testing across public pages, CMS workflows, content publishing, search, forms, media uploads, bilingual content, admin permissions and integrations.

- Conduct compatibility testing across current major browsers and common device sizes.
- Conduct performance testing, security testing and infrastructure configuration review prior to launch.
- Facilitate User Acceptance Testing (UAT) with NMHD and obtain written sign-off before production go-live.
- Provide training sessions for authorized NMHD staff covering content management, media management, user administration, security practices, reporting and basic troubleshooting.
- Develop and hand over user manuals, administrator manuals, technical documentation, deployment procedure, backup procedure, security checklist and support escalation procedure.
- Hand over full administrative, management, customization and source-control rights to NMHD.
- Handover of full source code. The code must be pushed to a provided source control repository provided by the Ministry of Health, Family and Welfare.

4. Deliverables

Deliverable	Details
Inception and Requirements	Inception report, confirmed scope, stakeholder inputs, content inventory template, detailed requirements matrix and implementation work plan.
Functional requirements detailed document	Detailed functional requirements implemented in the website with data flow diagrams and design charts as per Government software development standard.
Design Package	Approved design concept within 20 calendar days of contract signing, information architecture, sitemap, wireframes and mock-up designs for minimum three key pages.
Architecture Package	Technical architecture document, deployment diagram, database design, data flow diagram, integration design, security controls matrix and hosting setup plan.
Functional Website	Fully developed and functional bilingual NMHD website with CMS/admin portal and initial NMHD-provided content uploaded.
Source-controlled Source Code	Complete source-controlled source code repository handover, including Laravel backend, Vue frontend, Node.js build/configuration files, SMS microservice, database migrations, Dockerfiles, deployment configuration, environment templates and release tags.

Hosting and Deployment Assets	Docker setup files, deployment guide, reverse proxy/HTTPS guidance, environment setup instructions, backup/restore scripts or documented procedures, monitoring checklist and operational runbook.
Integrations	OAuth authentication integration, email notification setup and separate SMS microservice implementation with templates, queueing, provider configuration and delivery tracking.
Testing Evidence	Functional/UAT test results, browser/device test results, performance test observations, vulnerability/security test report and remediation evidence for agreed findings.
Documentation and Training	User manual, CMS administrator manual, technical documentation, process flows, sitemap, training materials and completed orientation sessions.
Go-live and Handover	Tested and live website ready for public use, administrative credentials, source-control access, deployment credentials or sealed handover package as approved by NMHD and support transition checklist.

5. Terms and Conditions

- Development shall commence immediately upon approval of the design concept and agreed implementation plan.
- The Consultant shall provide regular progress updates to NMHD, including weekly progress summaries, risks, dependencies and decisions required.
- Iterations and revisions shall be provided as required during the design phase and within agreed change-control boundaries during development.
- A support period of six (6) months shall be provided for bug fixing, UI adjustments, deployment support, configuration support, security fixes and minor operational adjustments after handover.
- The contract period shall cover development, deployment, handover and the full support period.
- All production access, credentials, source-control repositories, documentation and licenses shall be handed over to NMHD before final acceptance.
- The Consultant shall not retain unauthorized access to production systems after handover except where explicitly approved for support purposes.

6. Required Experience and Team Capability

- Be a firm or individual consultant with experience in website design and development, preferably including public-sector, health-sector, bilingual or high-visibility web platforms.

- Demonstrate strong expertise in Laravel, Vue, PostgreSQL, Node.js, Docker-based deployment, CMS development, UI/UX design, security hardening and system documentation.
- Demonstrate experience implementing OAuth or comparable authentication integrations, email notifications and SMS gateway integrations or messaging services.
- Provide evidence of secure coding practices, version control usage, deployment procedures and maintenance/support capability.
- Provide portfolio of similar assignments with references and identify key team members responsible for project management, backend, frontend, DevOps/hosting, QA/security and documentation/training.

7. Proposal Evaluation

Proposals should be submitted as separate Technical and Financial Proposals.

Evaluation Component	Requirement
Mandatory Technical Considerations	Security approach, architecture quality, CMS usability, bilingual capability, Docker hosting setup, source-control handover, integration capability, testing methodology and support plan shall be considered during technical evaluation. Details of how to achieve these and system architecture must be included in the proposal.

8. Documents to be Submitted. All this information must be available in the proposal for the proposal to be accepted.

- Portfolio of relevant previous work, including links or screenshots, where available.
- Reference letters, minimum five.
- Sample mock-up designs or wireframes for minimum three key pages.
- Technical proposal with methodology, architecture, security approach, technology stack, Docker hosting approach, integration approach, testing plan, risk management plan and support plan.
- Financial proposal with full cost breakdown inclusive of all taxes, licenses, resources, hosting setup, deployment, documentation, training and support.

9. Duration of Assignment

- Website development: should not take more than six (6) calendar months, including discovery, design, development, testing, UAT and go-live preparation.
- Technical support and maintenance: six (6) calendar months after go-live/handover.
- Total maximum assignment duration: twelve (12) calendar months.

10. Intellectual Property and Source Control

All outputs, source files, designs, themes, components, modules, licenses, documentation, configurations, source-controlled source code, Docker setup files, database schemas, migrations, scripts, microservices and related materials produced under this assignment shall be the sole property of NMHD.

The Consultant warrants that all work is original or properly licensed and free from intellectual property infringement. NMHD shall not bear responsibility for any misuse of copyrighted material by the Consultant. Any third-party libraries, packages, templates, icons, fonts or assets shall be clearly listed with license terms and usage rights.

The Consultant shall hand over the complete source-controlled repository or repositories to NMHD. The repository shall include clear commit history, release tags, README files, deployment instructions, environment templates, database migrations and documentation sufficient for NMHD or Ministry technical staff to maintain and redeploy the system.

11. Acceptance Criteria

- Approved design and information architecture are implemented consistently across public and CMS pages.
- English and Dhivehi content workflows are functional and tested.
- Core pages, CMS roles, content publishing, forms, search, media management, analytics and integrations operate correctly during UAT.
- Docker-based deployment setup is documented, reproducible and tested in the agreed environment.
- OAuth, email and SMS microservice requirements are implemented or configured as approved by NMHD.
- Security testing has been completed and critical/high findings have been remediated or formally accepted by NMHD with mitigation plan.
- Backup, restore, monitoring, support, training and handover requirements are completed.
- Complete source-controlled source code and technical documentation have been handed over to NMHD.

12. Risk and Quality Requirements

- The Consultant shall maintain a project risk register covering scope, schedule, content availability, security, hosting, integration, data protection and handover risks.
- The Consultant shall apply quality assurance throughout the project and shall not defer testing or documentation to the end of the assignment.
- The Consultant shall provide traceability between TOR requirements, implemented features, test cases and acceptance evidence.
- Any deviation from the approved technology stack, architecture, security controls or handover obligations shall require written approval from NMHD.