Disaster Management Centre
Sri Lanka

TERMS OF REFERENCE (TOR)

Website Design, Development, Deployment, and Maintenance of the Disaster Management Centre Website

Disaster Management Centre Sri Lanka
August 2026

Contents

Contents

TERMS OF REFERENCE (TOR) 1

Contents 2

1. Introduction 4

1.1 Overview 4

1.2 About Disaster Management Centre 4

2. Background and Objectives 5

2.1 Project Objectives and Goals 5

2.1.2 Universal Accessibility 5

2.1.3 Automated Services 5

2.1.4 Facility Management 5

2.1.5 Conformance to Standards 5

2.2 Key Tasks and Related Activities 5

3. Scope of Work 6

3.1 Website Development – Disaster Management Centre 6

3.1.1. Website Content and Functional Structure 6

3.1.2. Real-Time Data and Visualization 6

3.1.3. Performance Optimization 6

3.1.4. Social Media and Content Sharing 6

3.1.5. Document Management System (DMS) 7

3.1.6. Knowledge Testing Module (Optional) 7

3.1.8. Slide Presentation Module 7

3.1.9. Surveys and Polls 7

3.1.10. Mobile Responsive Design 7

3.1.11. Email Alerts and Notifications 7

3.2 System Administration/ Access Rights and User Roles 7

3.3 Design Guidelines and Qualifications 7

3.3.1 Stakeholder Survey 7

3.3.2 Usability Testing 8

3.3.3 Design, Usability, Accessibility, and Language 8

3.3.4 User-Friendly Dashboard 8

3.3.5 Website Hosting and Infrastructure 8

3.3.6 Testing and Quality Assurance 8

3.3.7 Monitoring and Auditing 8

3.3.8 Ownership Transfer 8

3.4 Maintenance and Support 9

3.4.1 Support – 9
3.4.2 Support Materials and training – 9
3.4.3 Support Service Level Agreement – 9
3.4.3.2 Escalation Process 9
3.4.3.3 Monitoring and Reporting 9
3.4.3.4 Planned Maintenance 10
3.4.4 Ongoing Maintenance/ New Product Releases – 10
3.4.5 Software Service Level Agreement – 10
3.4.6 Modifications 10
3.4.7 Security and Data Protection 10
3.4.8 Backup and Disaster Recovery 10
3.4.9 Performance Monitoring and Reporting 10
3.4.10 Intellectual Property Rights 11
3.5 Technology/Platform Requirements 11
3.5.1. Browser Support – 11
3.5.2. DDoS Mitigation 11
3.5.3. Website security specifications for meteo.gov.lk website. 11
3.6. Disaster Recovery and Performance Requirements 12
3.7. Testing and Quality Assurance 12
4. Evaluation of Proposals 12
4.1. Evaluation Criteria (100 Marks) 13
4.2. Financial Evaluation (20 Marks) 14
5. Deliverables and Payment Schedule 14
6. Submission Requirements 15
6.1 Technical Proposal (Mandatory) 15
6.2 Financial Proposal (Mandatory) 15
6.3 Legal and Financial Documents (Mandatory Due Diligence) 15
6.4 Submission of Proposals (Mandatory Format) 15
6.4.1 Interested firms should submit: 15

1. Introduction

1.1 Overview

The purpose of this Terms of Reference (TOR) document is to outline the scope, objectives, and deliverables for the development of a modern, responsive, and user-centric website for the Disaster Management Centre (DMC), Sri Lanka. This website will serve as a comprehensive platform to ensure timely dissemination of information, public awareness, and inter-agency collaboration during emergencies.

It aims to enhance accessibility, transparency, and public engagement through intuitive design, robust backend infrastructure. DMC seeks proposals from highly experienced website development service providers with proven expertise in:

- Successful website design and development
- User experience (UX) and usability testing
- Information architecture
- Website deployment and maintenance
- Social media integration
- Search engine optimization (SEO)
- Responsive and multilingual design

Preference will be given to vendors with prior experience in government website projects and a strong understanding of industry best practices. This TOR does not commit DMC to award a contract or proceed with the project. DMC reserves the right to modify, cancel, or withdraw this solicitation at any time if deemed in its best interest.

1.2 About Disaster Management Centre

The Disaster Management Centre, Sri Lanka, located at No. 120/2, Wijerama Mawatha, Colombo 07, DMC serves as the national focal point for disaster risk reduction, preparedness, emergency response, and recovery coordination. As part of its mandate, the DMC plays a critical role in ensuring timely dissemination of information, public awareness, and inter-agency collaboration during emergencies.

The existing DMC public-facing website (**www.dmc.gov.lk**) was developed several years ago and no longer meets modern standards for accessibility, security, user experience, or real-time performance. Its current limitations hinder the Centre's ability to communicate critical information quickly and effectively to citizens, stakeholders, and partner agencies.

To address these gaps, the DMC intends to undertake a **comprehensive revamp and modernization** of its official website. The new digital platform will serve as the **secure, resilient, and high-performing national hub** for crisis communication, early warnings, and coordination tools, supporting both day-to-day operations and rapid information dissemination during emergencies.

2. Background and Objectives

2.1 Project Objectives and Goals

The primary objective of this project is to modernize and enhance the digital presence of the Disaster Management Centre, Sri Lanka, by delivering a user-friendly, mobile-optimized, and functionally robust website. The following specific objectives have been identified:

2.1.2 Universal Accessibility

Ensure full mobile responsiveness (desktops, tablets, and smartphones) and multilingual support (Sinhala, English, Tamil). Comply with WCAG 2.1 accessibility standards for users with disabilities.

2.1.3 Automated Services

Should provide automated services that improve preparedness, response, coordination, and public awareness

Early Warning and Alert Services - Real-time alert dashboard, Multi-hazard alerts (floods, landslides, cyclones, tsunamis, droughts, lightning) with colour codes

2.1.4 Facility Management

Integrate incident report facility for citizens including photos and GPS location.

2.1.5 Conformance to Standards

The new website must comply with W3C, WCAG, WAI, and ICTA government web standards, and ensure licensing and confidentiality.

2.2 Key Tasks and Related Activities

The key tasks of the project include requirement gathering, design, system architecture, admin panel development, and more, with timelines and deliverables clearly defined.

No.	Action Item	Timeline
01	Software Requirements Specification (SRS)	2 Weeks
02	UX/UI Designing & System Architecture	4 Weeks
03	Product launch	6 Weeks

3. Scope of Work

The selected bidder shall be fully responsible for the design, development, deployment, configuration, and maintenance of the Disaster Management Centre's official website. The DMC will provide the required server space from SLT, however the bidder shall assist and support the DMC preparation of specifications and recommendations for hosting.

The bidder shall also ensure compliance with industry-standard security practices, conduct all necessary testing and quality assurance prior to launch, and provide complete documentation, source code, and user/admin manuals. Adequate training must be given to Department staff on system administration and content management. The bidder shall provide five (05) years of comprehensive maintenance and support (included in the procurement cost and extendable by one year at DMC's discretion), including 24/7 support, adherence to SLA requirements, minor modifications free of charge, reasonable rates for major modifications, and zero-downtime updates. All intellectual property rights of the developed system shall remain with the Disaster Management Centre.

3.1 Website Development – Disaster Management Centre

The development of the Disaster Management Centre website must follow a modern, modular, and secure design. The key activities under this section include:

3.1.1. Website Content and Functional Structure

The website will feature comprehensive sections including National level Disaster Dashboard with data visualization , Interactive Sri Lanka Map, publications, photo galleries, and awareness materials., dynamic data visualizations, downloadable reports, The site will also include sections for Early warning dissemination, organizational information, and external links to relevant national and international agencies.

3.1.2. Real-Time Data and Visualization

- Provide **Disaster data dashboards** using **charts, graphs, and tables**, optimized for fast loading even on low bandwidth connections.
- Support **interactive visualization** of Alerts level of Disasters on Sri Lanka Map (e.g., Landslides , Flood etc).

3.1.3. Performance Optimization

- Ensure the site is **optimized for low bandwidth and mobile users**, especially in remote or rural areas of Sri Lanka.

3.1.4. Social Media and Content Sharing

- Integrate **social media functionalities** such as Facebook, X (formerly Twitter), and YouTube for real-time information dissemination.
- Allow streaming and auto-sharing of content between the website and social platforms.

3.1.5. Document Management System (DMS)

- Implement a comprehensive DMS to **upload and manage various formats** (PDF, DOC, JPG, etc.), including metadata such as uploader name, upload date, file tags, and description.
- Support internal indexing and search functionality, with **mouse-over tooltips** for better user guidance.

3.1.6. Knowledge Testing Module (Optional)

- Optionally include a **self-assessment or quiz module** for staff and General public on Disaster Management knowledge.
- Support automatic grading and question bank management by DMC administrators.

3.1.8. Slide Presentation Module

- Enable DMC to publish **educational slide presentations** (e.g., awareness) that can be customized and embedded on the website.

3.1.9. Surveys and Polls

- Include a module for **conducting online surveys and opinion polls**, to collect public or stakeholder feedback.

3.1.10. Mobile Responsive Design

- The entire website must be fully **mobile responsive** and optimized for devices including smartphones and tablets, across all OS platforms.

3.1.11. Email Alerts and Notifications

- Enable **email alert options** for users to subscribe to Early warnings

3.2 System Administration/ Access Rights and User Roles

The vendor shall implement and maintain system administration features ensuring secure and reliable operation of the website.

- Implement tiered user permission levels:
    - Read-only users
    - Read/Write users
    - Full Control (Read/Write/Delete)
    - System Administrators

3.3 Design Guidelines and Qualifications

3.3.1 Stakeholder Survey

The Disaster Management Centre will conduct a stakeholder forum to gather requirements, validate objectives, and define key tasks. Outputs will be consolidated into a Software Requirements Specification (SRS), which upon mutual agreement will be signed off and serve as the project baseline.

3.3.2 Usability Testing

Conduct usability testing in real user environments to assess navigation, layout, and user interaction. Deliver a report with recommendations and wireframe prototypes.

3.3.3 Design, Usability, Accessibility, and Language

- Ensure adherence to WCAG accessibility standards
- Provide full multilingual support (Sinhala, English, Tamil) with seamless language switching
- Design for fast loading times and cross-browser compatibility
- Ensure SEO-friendly URLs and Unicode compliance
- Align design with DMC branding and government ICT standards

3.3.4 User-Friendly Dashboard

Develop an intuitive editorial backend allowing DMC staff to easily upload and manage content aligned with operational workflows.

3.3.5 Website Hosting and Infrastructure

- The website should be hosted in adequate server space to accommodate all added features and uploads. Vendor shall provide hosting requirements detailing server specs, software environment, and security.
- Hosting must support at least 10,000 concurrent users with high availability (99.9% uptime), scalability, and secure data transmission via SSL certificates.
- Include disaster recovery solutions with RTO $\leq$ 60 minutes and RPO $\leq$ 15 minutes.
- Average page load time must be $\leq$ 1.5 seconds.

3.3.6 Testing and Quality Assurance

- Vendor shall implement comprehensive QA including functional, performance, security, and acceptance testing.
- QA methodology and documentation must be provided.

3.3.7 Monitoring and Auditing

- The website should include tool(s) (nonproprietary) that can generate statistics about users who publish, update, and delete any content of the website.
- The website should include statistic generating tool(s) which can generate statistics: Hit counter; Number of page loads; Number of hits received; Pages accessed by the user; visitors location-based information etc.

3.3.8 Ownership Transfer

- Deliver all source codes, databases, content tools, graphics (source files), documentation, and licenses to DMC.
- Intellectual property rights for all developed components shall belong to DMC.

3.4 Maintenance and Support

3.4.1 Support –

- The vendor shall provide comprehensive maintenance and support for a period of five (05) years.
- At the discretion of the Disaster Management Centre (DMC), the maintenance period may be extended by one (01) year under mutually agreed terms.
- Support must include 24/7 live assistance via e-mail and telephone.
- The vendor's support staff must have full technical knowledge of the website, mobile application, and associated modules.
- The system shall be designed for future feature expansion, with vendor support available for enhancements when required.

3.4.2 Support Materials and training –

- The vendor shall provide all relevant support documentation (user manuals, admin guides, FAQs).
- Training sessions must be conducted for designated DMC staff on content management, troubleshooting, and system administration.

3.4.3 Support Service Level Agreement –

The vendor shall adhere to the following minimum SLA levels during the 5-year maintenance period.

3.4.3.1 Incident Response and Resolution Times

Issue Severity	Description	Response Time	Resolution Time
Critical	Complete service outage, data loss, or security breach	Within **1 hour**	Within **4 hours** or provide a workaround with full resolution in **24 hours**
Major	Significant functionality impacted but system still usable	Within **2 hours**	Within **48 hours**
Minor	Small issues, cosmetic bugs, or non-urgent errors	Within **1 business day**	Within **5 business days**
Enhancement Requests	New features or major modifications	Acknowledgement within **2 business days**	Delivery timeline to be mutually agreed

3.4.3.2 Escalation Process

If an issue is not resolved within the SLA timelines:

- Escalation Level 1 – Project Manager (Vendor)
- Escalation Level 2 – Vendor's Senior Technical Lead
- Escalation Level 3 – Vendor's Management and DMC's designated officer

3.4.3.3 Monitoring and Reporting

- Vendor shall submit quarterly SLA compliance reports, including uptime, downtime logs, and resolution statistics.

- Failure to meet SLA commitments will result in penalties as specified in the contract (e.g., deductions from payments or extension of maintenance period at no extra cost).

3.4.3.4 Planned Maintenance

Any planned downtime must be scheduled outside of peak usage hours (to be defined by DMC) and prior written notification (minimum 48 hours) must be given to DMC.

3.4.4 Ongoing Maintenance/ New Product Releases –

- The vendor shall ensure seamless updates and new releases without service downtime.
- All bug fixes, patches, and security updates during the 5-year period shall be included

3.4.5 Software Service Level Agreement –

Vendors must provide an SLA detailing software upgrade guarantees, bug fixing processes, and enhancement procedures.

3.4.6 Modifications

- **Minor modifications** and adjustments (e.g., content changes, small UI refinements, bug fixes) shall be included at no additional cost during the 5-year period.
- **Major modifications** (e.g., new modules, significant feature development, third-party integrations) shall be chargeable at reasonable rates, subject to DMC approval.

3.4.7 Security and Data Protection

- The system must comply with recognized IT security standards and remain protected against cyber threats.
- Periodic security audits and vulnerability testing shall be carried out, with reports submitted to the DMC.
- All data must be hosted and stored in compliance with government regulations and data protection requirements.

3.4.8 Backup and Disaster Recovery

- The vendor shall ensure regular automated backups of applications and databases.
- A tested disaster recovery and business continuity plan must be in place to ensure restoration of services within an agreed recovery time.

3.4.9 Performance Monitoring and Reporting

- The vendor must implement performance monitoring tools to ensure availability and reliability.
- Quarterly reports on uptime, downtime, and support resolutions shall be submitted to the DMC.

3.4.10 Intellectual Property Rights

- All source code, documentation, and related deliverables shall be the property of the DMC.
- The vendor shall not reuse, resell, or disclose these without written consent from the DMC.

3.5 Technology/Platform Requirements

3.5.1. Browser Support – The DMC is looking for the new website to support mobile and desktop versions of Apple Safari, Google Chrome, Microsoft Internet Explorer and Edge, and Mozilla Firefox. The site should support all versions of the browsers that have been released within the last 5 years and the site should compatibility of future upgrades of browsers.

3.5.2. DDoS Mitigation – The hosted solution should protect the website against Distributed Denial of Service (DDoS) and other cyberattacks, and should be able to detect and mitigate malicious traffic within seconds. The solution should have smart-detection technology that can identify the source and analyze the behavior of the attack.

3.5.3. Website security specifications for meteo.gov.lk website.

Security Area	Requirements
1. General Security Standards	• Adhere to OWASP Top 10 • Follow ISO 27001/NIST Framework • Apply security patches throughout project
2. Authentication and Access Control	• Secure user authentication (bcrypt) • Role-Based Access Control (RBAC) • Admin portals: 2FA + IP whitelist/VPN
3. Data Encryption	• HTTPS with TLS 1.2+ • Encrypt sensitive data at rest • Implement HSTS
4. Web Application Firewall (WAF) Compatibility	• Compatible with WAF (e.g., Fortinet, AWS WAF) • Input sanitization and filtering
5. Input Validation and Security Controls	• Validate input client/server side • CSRF protection • Use CSP headers
6. API and Data Feed Security	• Secure APIs with HTTPS & tokens • Implement rate limiting & CORS • Secure weather APIs
7. Secure File Handling	• Allow only whitelisted file types • Scan for malware • Store files outside web root

8. Session and Cookie Management	• Secure, HTTP-only, SameSite cookies • Session timeout (e.g., 15 mins) • Destroy session on logout
9. Logging and Monitoring	• Log security events (login/admin) • Store logs securely, SIEM-ready • Include timestamp, IP, user ID
10. Backup and Recovery	• Automated, encrypted backups • Offsite storage • Test recovery procedures
11. Testing and Audit Requirements	• Independent VAPT before launch • Submit security test reports
12. Compliance and Documentation	• Complete security checklist • Document auth, access, backup, recovery
13. Deployment Security	• CI/CD with security scans • Harden deployment (disable services, firewall) • Enforce least privilege
14. Maintenance and Support	• Patch management for 5 years (Initial Agreement) • SLA for vulnerabilities (e.g., If Critical - 48 hrs) • Optional extended support
15. Optional security features	• CAPTCHA • account lockout after failed logins, • digital signatures for weather alerts/data

3.6. Disaster Recovery and Performance Requirements

Hosting solution must include backup or failover data centers to ensure uninterrupted service.

3.7. Testing and Quality Assurance

Quality Assurance should be guaranteed for the whole website in all aspects. Quality Assurance approach should be described in detail the Methodology. The web developer should implement all necessary security measures and adhere to the security measures proposed by Sri Lanka Computer Emergency Response Team (SLCERT) for ensuring the security of the website.

4. Evaluation of Proposals

Proposals will be evaluated based on the following criteria. Only bidders scoring 60 marks or above in technical evaluation will be considered for financial evaluation.

4.1. Evaluation Criteria (100 Marks)

The evaluation will employ a **Quality and Cost Based Selection (QCBS)** method, prioritizing technical quality and compliance with a **80% Technical / 20% Financial** weighting ratio.

Evaluation Category	**Sub-Criterion**	**Proposed Weighting (%)**	**Description**
I. Technical Proposal & Expertise	**80%**		
I.A. Technical Approach & Methodology (QNFRs)	30%	Soundness of architecture, API strategy, and **realism of the methodology** for delivering RTO/RPO (mins) and Peak Load capacity (50,000 CU).	
I.B. Experience in similar projects and organizational Capacity	20%	Relevance of past projects; and organizational capacity/stability (assessed via financials).	
I.C. Team Composition & Expertise	15%	Qualifications and experience of key personnel (Lead, Security Engineer, Architect);	
I.D. Security & Mandatory Compliance (MQT)	15%	Detailed plan to meet **all Sri Lanka CERT mandates** (MFA, Two-Way SSL, OWASP mitigation, PEN Testing	

		accommodation) and **WCAG 2.1 Level AA** compliance.	
II. Financial Cost (Price)	**20%**	Reasonableness and competitiveness of the budget; clarity of cost breakdown for development, and the mandatory 12-month maintenance period.	
Total	**100%**		

4.1.1. Minimum Technical Score Required:

Bidders must score a minimum of 60 marks out of 80 in the technical evaluation to qualify for financial evaluation.

4.2. Financial Evaluation (20 Marks)

The financial proposal will be scored as follows:

Score = (Lowest Price / Bidder's Price) × 20

The evaluation committee may request presentations, demonstrations, or clarifications from shortlisted vendors.

5. Deliverables and Payment Schedule

No.	Type of Work	Deliverable	Time Frame	Payment (%)
1	Requirement analysis and planning	Requirement Specification Document	Two weeks after contract signing	20%
2	Design, development, and implementation	Fully functional hosted website	Two months from contract signing	50%
3	Training for administrative users and documentation	Final report/User manual	Immediate after website launch	20%
4	Maintenance and software support 1. Quality support and maintenance report	Go-Live + 12 months	12 months	10%

No.	Type of Work	Deliverable	Time Frame	Payment (%)
	2. Final Software and Maintenance report should consist with comprehensive knowledge transfer with the documentation (including above mentioned all the updated documents.			

6. Submission Requirements

Interested firms are requested to submit the following mandatory documents:

6.1 Technical Proposal (Mandatory)

- A cover letter expressing interest.
- Detailed methodology and work plan addressing all functional, security, and integration requirements.
- Detailed plan for meeting the stringent QNFRs (RTO, RPO, Peak Load).
- Curriculum Vitae (CVs) of key personnel, highlighting relevant experience and security certifications.
- List of at least two (2) similar projects successfully completed in the last five (5) years, including client references.

6.2 Financial Proposal (Mandatory)

- A detailed breakdown of all costs associated with the assignment, including professional fees, hosting recommendations, and the full 12-month maintenance cost.

6.3 Legal and Financial Documents (Mandatory Due Diligence)

- Copy of company registration certificate and Tax registration certificates.
- **Audited financial statements for the past three (3) years** to demonstrate financial stability and capacity.

6.4 Submission of Proposals **(Mandatory Format)**

- All submissions must be made in Hard Copy.

6.4.1 Interested firms should submit:

- A detailed **technical proposal** (approach, methodology, work plan, and CVs of key experts)
- A **financial proposal**
- Evidence of past performance (with URLs and references)