Request for Proposal (RFP)
Website Redesign and Hosting Services

1. Introduction

Multi-Service Center (MSC) is seeking proposals from qualified vendors to redesign our existing website and provide reliable hosting services. The goal is to create an engaging, accessible, and modern online presence that reflects our brand and serves our audience effectively.

2. Company Overview

MSC is a non-profit organization that primarily serves South King County (near Seattle) in Washington State. Our mission is to uplift communities by increasing equitable access to advocacy, opportunities and well-being. We provide direct services such as energy assistance, housing support, rental assistance, affordable housing, resource navigation, and employment support. We also operate a food bank and the Washington State Long-Term Care Ombudsman Program which provides support for residents in long-term care facilities across the state.

Our target audience for our website includes both clients seeking our services as well as individuals and businesses seeking to support our work through financial gifts or volunteerism.

Our current website at mschelps.org was originally designed over ten years ago with a refresh in 2018. We are currently using WordPress and are comfortable with this environment but open to other options. We prefer an open-source, non-proprietary design tool.

3. Project Objectives

- Deliver a modern, responsive, and accessible website that reflects MSC's brand identity, incorporates current web technologies, and offers a refreshed user experience across devices Use an open-source, widely supported CMS — such as WordPress — that remains fully portable and under MSC's administrative control. The CMS should allow internal content updates without ongoing developer dependency. Ensure WCAG accessibility compliance and optimize for performance and SEO

- Migrate existing content and streamline navigation to better serve core audiences

- Integrate seamlessly with third-party systems (e.g., forms, CRMs, analytics, donation platforms)

- Establish secure, scalable, and high-availability hosting.

- Implement baseline security controls appropriate to a public-facing nonprofit site

- Provide clear documentation and training for internal staff on managing the CMS and content

4. Scope of Work

If your company does not provide both these services, please reference your ability to provide referrals or recommendations to businesses that you have experience partnering with that can meet the qualification of that service listed below.

Redesign Services:

- Provide multiple UX/UI design concepts based on MSC's brand identity and audience needs, including mobile-first and responsive layouts Facilitate early discovery conversations with MSC to understand user needs, content priorities, and key visitor actions before finalizing site structure and design
- Develop a content migration and cleanup plan to transfer existing materials to the new site while removing outdated or redundant content. Conduct SEO and performance audits on the existing site and implement on-page SEO best practices (meta tags, semantic markup, alt text, URL structure, etc.) in the redesign Integrate third-party tools such as contact forms, analytics (e.g., Google Analytics 4), CRM connectors, donation platforms, and social media embeds

- Improve site navigation and content structure to help users quickly find key information and better engage with MSC’s programs and services. Proposals should include

strategies for guiding user flow, such as user journey mapping, and for measuring engagement success beyond simple bounce rates.
- Include built-in accessibility features to meet or exceed WCAG 2.1 AA standards, with a clear path to WCAG 2.2 compliance as it becomes more widely adopted
- Coordinate user acceptance testing (UAT) and a pre-launch review process with MSC stakeholders

Hosting Services:

- Vendors must implement strong logical access controls, including role-based provisioning, least privilege enforcement, and routine access reviews. Administrative privileges must be clearly scoped and regularly validated.
- Vendors must maintain and test a disaster recovery (DR) plan appropriate to the hosted environment, including clearly defined recovery time objectives (RTO) and recovery point objectives (RPO). MSC may request a summary of this plan and test results annually.
- Cloud-based hosting with a documented uptime SLA of 99.9% or better. Vendors should provide redundancy and failover measures appropriate to a public-facing nonprofit website, and disclose any use of CDN or caching layers that support performance and resilience
- Implement strong security controls aligned with OWASP best practices for web application security, including TLS encryption, regular vulnerability patching, and tenant isolation where applicable. Daily full-site backups (including content, database, and platform configuration) must be automated, encrypted at rest, and retained for a minimum of 30 days. The hosting provider must support on-demand restoration via administrative interface or vendor-supported request
- The hosting solution must support scalable storage and bandwidth to accommodate changes in traffic volume, content growth, and seasonal surges. Vendors should describe how they manage autoscaling, caching, or load balancing to ensure consistent performance without service interruptions
- Vendors must provide ongoing technical support and maintenance for the hosted environment, including CMS uptime monitoring, troubleshooting, and post-launch assistance. Proposals should outline support channels (e.g., email, ticketing, phone), response time expectations, and availability (e.g., business hours vs. 24/7). Maintenance must include routine platform upkeep, updates, and coordination of renewals or changes related to hosting infrastructure
- Vendors must maintain documented incident response and breach notification procedures that align with industry best practices. Procedures must include defined

timelines for MSC notification following any security incident involving the website or its data, a description of internal containment and remediation steps, and a commitment to transparent communication throughout the investigation and recovery process.

- Vendors must implement regular patching and vulnerability management processes that address both application-level and infrastructure-level risks. Security updates must be applied in a timely manner based on severity, with critical patches prioritized for immediate remediation. Vendors must also monitor for emerging threats and have a documented plan for handling zero-day vulnerabilities.
- Vendors must ensure that all website-related data — including content, configurations, backups, and administrative records — remains the property of MSC. Upon contract termination, vendors must return all MSC-owned data in a usable format and provide written certification of secure deletion from their systems within 30 days, unless otherwise required by law. Any applicable export or transfer fees must be disclosed in the proposal.
- Donation processing is a core function of the MSC website. All payment workflows must be isolated to PCI DSS-compliant third-party platforms. MSC's website must not directly store, process, or transmit any payment card data.

5. Deliverables

- Vendors must provide initial wireframes to illustrate page structure and layout, followed by high-fidelity mockups reflecting MSC's brand and visual style. These should cover all major page templates and be submitted for review and approval prior to development. Final design files (e.g., Figma, Adobe XD, or equivalent) must be included in project deliverables for internal reference and developer handoff.
- Vendors must deploy both a functional staging site for MSC review and testing, and a fully configured live production site for launch. The staging environment must mirror the live environment as closely as possible and remain available post-launch for testing future updates, plugins, or changes.
- Vendors must provide user-friendly documentation covering CMS administration, content updates, and common tasks relevant to MSC staff. At least one live training session must be delivered (remote or in-person), with a recording and supplemental reference materials made available for future use.
- Vendors must fully provision and configure the hosting environment, including all CMS and database components, SSL certificates, DNS configuration, and administrative access for MSC staff. Login credentials and configuration documentation must be provided at project handoff.
- Vendors must provide a high-level summary of the system architecture and hosting environment, including major components, third-party services, and third-party verification of security controls that are in place (e.g. SOC2, ISO27001/2 SoA)

Documentation should also describe how access control, data backups, and incident response are managed.

6. Timeline:

- RFP submissions due by: September 17, 2025
- Vendor selection and project kick-off anticipated to be fourth quarter 2025

7. Budget

We would request that vendors provide their best value estimate that meets the above objectives for consideration. Please include any non-profit discounts or trade/marketing discounts that may be available.

8. Proposal Evaluation Criteria

- **Relevant experience and portfolio**
    - Demonstrated experience designing and hosting websites for nonprofit, mission-driven, or public service organizations. Examples of past work should reflect diverse audiences and use cases.
- **Project management and communication**
    - Clarity of proposed process and timeline. Quality of communication practices and responsiveness. Ability to work collaboratively with non-technical stakeholders.
- **Support and maintenance options**
    - Clarity and quality of the vendor's proposed post launch support, including issue response process, availability, escalation procedures, and any included maintenance or update services.
- **CMS usability and content ownership**
    - Ease of use for internal staff managing content day-to-day. Proposals should demonstrate how the CMS will support non-technical users and preserve MSC's administrative control post launch.
- **Training and Documentation**
    - Quality and relevance of end-user documentation and training materials. Proposals should include how the vendor plans to support knowledge transfer to MSC staff.
- **Technical capabilities**

- Strength and flexibility of the proposed CMS, hosting environment, and third-party integrations. Proposals should show how the solution meets MSC's current and future needs without introducing unnecessary complexity.

- **Accessibility and Inclusion**
  - Clear commitment to building a site that complies with WCAG 2.1 AA standards and considers the needs of individuals with disabilities. Accessibility practices should be integrated into both design and development.
- **Pricing and value**
  - Overall cost-effectiveness of the proposal relative to the scope of work, quality of deliverables, and long-term sustainability. Vendors should clearly outline all fees and identify any available non-profit discounts or in-kind contributions.
- **Security and Compliance Posture**
  - Quality of proposed security controls, backup and recovery processes, compliance with industry standards (e.g. SOC2, PCI) and ability to support MSC's data protection requirements.

9. Submission Instructions and Questions

Send submissions by September 17, 2025, to:

Erin Trivelas, Associate Director, Community Engagement
erint@mschelps.org

For questions related to this RFP, please email info@mschelps.org.