

Vendor Invitation: Web Hosting and IT Service Engagement

1. Project Overview

The Financial Dispute Resolution Centre (FDRC) is seeking to engage a qualified web hosting service provider to support the migration and ongoing security of its public-facing website. The current hosting platform does not offer sufficient flexibility for timely security maintenance or operational oversight. This engagement is not limited to hosting services alone. The selected vendor will be expected to deliver a complete solution that includes the migration of the existing website, initial hardening and configuration of the hosting platform, and ongoing security updates throughout the duration of the engagement.

The project is short-term in nature and focused on delivering a secure, stable, and supportable production environment. The solution must be capable of passing a formal security risk assessment arranged by FDRC prior to go-live. Vendors submitting proposals should demonstrate solid experience with similar projects, preferably involving government or public sector clients.

2. Technical Scope

The vendor is required to propose a technically sound solution that supports the seamless migration and secure operation of the FDRC website. The hosting environment must be configured to comply with the HKSAR Government's Baseline IT Security Policy (S17) and the practices recommended in the G3 IT Security Guidelines.

Additionally, the vendor will be responsible for reviewing and remediating any security findings that have been identified in a formal Security Risk Assessment and Audit (SRAA) Report commissioned by FDRC. This report cannot be shared publicly due to its sensitive nature, but will be made available to the selected vendor upon appointment, under confidentiality.

3. Security and Support Requirements

FDRC expects the hosting solution to be protected by industry-standard security measures. Vendors must be able to demonstrate that their infrastructure supports

security patching, vulnerability management, encrypted communication, and access controls appropriate to the project's requirements.

In addition to implementing technical safeguards, vendors should maintain a clear process for identifying and responding to service incidents. While 24/7 support is not required, there should be a defined escalation procedure for handling time-sensitive issues.

4. Compliance and Contractual Terms

The successful vendor will be required to enter into a short-term service agreement that clearly defines deliverables, responsibilities, and expectations. The contract must also address compliance with applicable data protection and security regulations, including the PDPO, as well as local government standards where applicable. Any reliance on subcontractors or third-party service providers must be disclosed.

5. Proposal Submission

Interested vendors are invited to submit a brief company profile and relevant team background, a technical proposal outlining the migration and hosting approach, and any documentation supporting their security capabilities, such as certifications or audit reports. A service level or support matrix should also be included.

For all proposal submissions or enquiries regarding this invitation, please contact Joe Lee at joe.lee@fdrc.org.hk. The deadline for submitting proposals is October 31st, 2025.
