Request for Proposals (RFP)
Corporate Website Design, Build, & Launch
ADDENDUM 1

RFP No.: 2026-10-027

Addendum Issue Date: Tuesday, October 27th, 2026

Addendum Summary

This addendum prevails where it conflicts with the original RFP. The Access and APIs clause replaces the existing API-security bullet. Data residency and processing replaces the existing Canadian-hosting bullet. Administrative access and pre-launch security acceptance replace the existing non-public administrative-login and vulnerability-scanning bullets, respectively. Other security requirements remain unchanged and are supplemented by the clauses below.

Submission Requirements

- Send all questions and proposals to a.harlap@ictc-ctic.ca
- Include three relevant client references with contact details.

Section Terms & Conditions

- The contract ends November 30, 2027, including 90 days of support beginning on ICTC's written confirmation of production launch. Any launch delay affecting this period requires an agreed schedule adjustment.

Section Budget

- The total maximum budget for this project is $200,000 CAD + applicable taxes, inclusive of all work described within this RFP.

Section Scope of Work: Ongoing Cost Estimates

- Provide estimates for ongoing costs of the proposed third-party plugins, services, and/or any subscriptions.

Section Scope of Work: Security Considerations

- **Scope and handover:** These requirements apply to components, configurations, services, and integrations delivered by the vendor. The vendor must identify dependencies relevant to its implementation and report any limitations or security concerns encountered during delivery. Auditing or remediating existing ICTC-managed or independently supplied systems is excluded unless expressly included. This exclusion does not remove responsibility for the vendor's selection, configuration, or integration of third-party services. Before launch, the vendor must document operational responsibilities, support hours, escalation contacts, and outstanding limitations. Ongoing maintenance, monitoring, and emergency support are excluded, except for the security-correction obligations below.
- **Access and APIs:** Require MFA for administrative and privileged accounts within the vendor's solution. APIs accessing non-public data or privileged functions must enforce authentication and authorization. Public APIs may permit anonymous access. All exposed APIs must use appropriate validation, rate limiting, and abuse protection.
- **Administrative access:** Protect administrative access using MFA, login-abuse protection, and appropriate access restrictions.
- **Pre-launch security acceptance:** The solution must undergo ICTC's vulnerability scanning before launch. Remediate Critical and High findings or obtain ICTC's written approval of compensating controls. Agree on a remediation plan for remaining findings.
- **Logging and recovery:** Configure logs for administrative sign-ins, account and permission changes, and significant security or configuration changes, with 90-day retention unless ICTC approves a documented platform limitation. Protect logs, exclude credentials and sensitive form/chat contents, and provide ICTC access and instructions. Verify hosting backup capabilities, demonstrate restoration before launch, and document backup coverage, retention, recovery capabilities, and gaps requiring ICTC approval.
- **Security correction and warranty:** At no additional cost, correct vendor-attributable vulnerabilities, misconfigurations, and control deficiencies discovered by the vendor or reported to it during implementation or the 90-day post-launch support period, including findings from ICTC-directed testing. Obligations for

findings discovered by the vendor or reported to it within that period continue until resolved, including after contract expiry. These timelines do not override ICTC's pre-launch security acceptance requirements.

Mitigate Critical or actively exploited findings within 24 elapsed hours; permanently remediate within seven calendar days where a fix is available. Remediate High findings within 14 calendar days and Medium findings within 60 calendar days. Where a fix is unavailable, implement compensating controls. Extensions require ICTC's written approval. These timelines begin when the vendor discovers or receives credible notice of a finding and apply only to vendor-attributable findings. Required response coverage must be included in the project price. Newly disclosed third-party vulnerabilities after launch fall under ongoing maintenance unless attributable to the vendor's failure to meet the agreed requirements.

- **Providers and AI:** Disclose subcontractors, sub-processors, and AI providers handling ICTC data as required under Data residency and processing. Obtain ICTC approval before granting access or making material changes to approved providers or their data-handling arrangements, and apply equivalent security and confidentiality obligations. The vendor remains accountable for its subcontractors. ICTC data must not train or improve public or shared AI models; ICTC-specific training and transmission of personal or confidential data to AI services require prior written approval.

Clarifications

Scheduling of invoicing vs work performed

- All project work must be invoiced by March 31, 2027. Delivery milestones remain unchanged, including training before launch and 90 days of post-launch support. Payment timing is governed by the contract.

Data residency and processing

- Private learner/program records remain in the separate ClientPortal. Work on the ClientPortal is limited to the integrations required by this RFP; redevelopment and migration of its private records are excluded. Corporate website personal information, including emails and identifiable tracking data, must be stored and processed in Canada unless ICTC approves a legally and contractually permitted exception. This includes backups and logs containing personal information. Public

content and appropriately anonymized data may be processed internationally; stricter funding or licensing restrictions prevail.

- Vendors must disclose providers, data involved, storage and processing countries, international access, retention, and safeguards. Identify proposed exceptions and Canadian alternatives, including cost differences, in the proposal. Services named in the RFP are not automatically exempt from these requirements. Exceptions require ICTC's written approval and completion of applicable assessments before transfer. Use synthetic or appropriately de-identified data for development and testing wherever possible.

Risk Mitigation including Security and Privacy Scoring

- Security and privacy controls, including security governance, secure development practices, incident response capabilities, and compliance with the RFP security requirements, will be considered as part of the evaluation of this category. Kindly provide concise evidence of relevant security practices; SOC 2 or ISO 27001 certification is not mandatory. Identify proposed exceptions and alternatives for ICTC's approval. Include mandatory implementation and warranty costs in the project price; separately price optional ongoing services.

Inventory of sites

This is an approximate inventory of current pages and reports. Not all will be expected to be migrated.

ICTC - 1,301 Total

- Basic Page - 8
- Biography (Our Team) - 42
- Event (News & Events Search) - 165
- Landing Page (ICTC Homepage) - 83
- News (News Search) - 731
- Report (Reports, Policy Briefs) - 271
- Webform (Webform Test) - 1

eTalentCanada - 278 Total

- Basic Page (Homepage) - 69
- Event (Events) - 1
- Job Market Information (Job Market Information) - 62
- Location (Locations) - 20

- News (News) - 65
- Program (Programs) - 61