GEO NOVA SCOTIA
getting everyone online

Request for Proposal (RFP)

IT Support Services

GEO Nova Scotia is seeking proposals from qualified experienced service providers to provide IT Support, Cybersecurity, and Compliance services.

GEO Nova Scotia
Dartmouth, Nova Scotia
January 22, 2026

PART 1: OVERVIEW

1.1 Introduction

A. About GEO Nova Scotia

Getting Everyone Online (GEO) Nova Scotia is a province-wide non-profit that works toward the goal of digital equity for all Nova Scotians. This means supporting those who cannot afford to connect on their own so they can benefit from opportunities that internet connectivity provides.

> *The digital divide is the issue.*
> *Digital equity is the goal.*
> *And digital inclusion is the work.*

Digital Inclusion means being part of digital society. It means having internet access, a decent device, and the basic skills to use them confidently and safely. GEO works closely with funders and private-sector suppliers to serve thousands of households through a network of over 130 community partner organizations across the province.

GEO Nova Scotia has **16 full-time staff** with approximately **30 unique user accounts** operating in a **fully remote Google Workspace** work environment. In our search for IT Support, cost efficiency, flexibility, and right-sizing services are critical considerations. Vendors are encouraged to propose creative, value-driven IT Service approaches that eliminate unnecessary costs. An overview of our current IT Support Service is in Appendix A.

B. About Vendors

The Vendor must be Canadian and a single legal entity that, if selected, intends to negotiate and enter into a contract with GEO Nova Scotia. If the proposal is being submitted jointly by two or more separate entities, the proposal must identify only one of those entities as the “Vendor”. The Vendor will be accountable for all Deliverables. While not a requirement, preference may be given to BBB certified IT service providers.

C. Scope of Services

The vendor shall provide managed IT support, security monitoring, endpoint protection, vulnerability monitoring, and compliance advisory services suitable for a cloud-first, Canadian non-profit using Google Workspace, and be designed for a fully remote user base.

The scope of services includes:

- Assessment of current IT/Cybersecurity infrastructure
- Transition to vendor-proposed IT Service
- Ongoing IT support and maintenance
- Data backup and disaster recovery solutions
- Network security enhancements
- Occasional employee training in new technologies

1.2 GEO IT Overview

A. Current GEO Nova Scotia IT Support Overview

An overview of our current IT Support Service is in **Appendix A.**

GEO's Core Platforms

- Primary identity, email, and collaboration platform: Google Workspace Enterprise
- CRM platform: Salesforce
- Productivity application: Google Workspace
- Environment: Fully remote users; cloud-first operations

1.3 Submission Guidelines

Key Dates

Due Date	Time Due	Item
Friday, **January 30**, 2026	11:59 AM	Expression of Interest (EOI)
Wednesday, **February 4,** 2026	11:59 AM	Questions
Friday, **February 13**, 2026	11:59 AM	Complete Proposal

All items must be submitted electronically to info@geonovascotia.ca

A. Expression of Interest (EOI)

Due: Friday, January 30, 2026

Vendors must submit an **Expression of Interest (EOI)** to info@geonovascotia.ca by 11:59 AM on Friday, January 30, 2026.

The Expression of Interest email must contain:

- Company Name and website
- Confirmation that you intend to submit a complete proposal for the GEO Nova Scotia Request for Proposal (RFP) for IT Services by the submission deadline.
- Full Name of One Main Contact person with their position, cellular number and email.
- An email response will be sent confirming receipt of the EOI. GEO's email confirmation is what will enable vendors to proceed to the next steps. IF you do not receive an email confirmation from GEO please contact info@geonovascotia.ca to request one.

B. Questions

Due: Wednesday, February 4, 2026

Questions must be submitted to info@geonovascotia.ca by 11:59 AM on Wednesday, February 4, 2026.

- A MAXIMUM of three (3) questions per vendor.
- All three (3) questions must be in one (1) email. Your questions will be shared with all confirmed vendors competing for this RFP.
- Questions must be written succinctly in plain language.
- GEO Nova Scotia will send the questions submitted from all vendors and the answers to those questions to all confirmed vendors by end-of-day Friday, February 6, 2026.

C. Proposal Submission

Due: Friday, February 13, 2026

- Vendor Proposals must be submitted electronically as a **PDF only** to this email: info@geonovascotia.ca by 11:59 AM on Friday, February 13, 2026.
- Emailed submission subject lines must read: **GEO NS 2026 IT Submission**
- Submissions will receive email confirmation of submission receipt. Respondents who do not receive this notification should check junk/spam folder, if not found, Vendors should request verification of receipt of submission in an email to info@geonovascotia.ca
- No amendments will be accepted once the notification of receipt has been sent.
- Proposals submitted after the Submission Deadline will be rejected. This determination shall be based on the electronic time/date stamp generated by GEO's email server.

E. Assessment

Proposals will be evaluated on the following criteria:

Demonstration of Relevant Experience & Qualifications	25 points
Service Delivery Model	10 points
Client references and past performance	15 points
Value-added Services	10 points
Pricing and Cost Breakdown	40 points
Total Points	**100 points**

PART 2: SUBMISSION CONTENT

2.1 Vendor Experience and Qualifications

A. Vendor Background, Experience and References

Vendors must be an established IT services company with over 5 years of experience. They have successfully implemented IT solutions for comparable organizations. The Vendor must be Canadian and a single legal entity that, if selected, intends to negotiate and enter into a contract with GEO Nova Scotia. If the proposal is being submitted jointly by two or more separate entities, the proposal must identify only one of those entities as the “Vendor”. The Vendor will be accountable for all Deliverables.

While not a requirement, preference may be given to BBB certified IT service providers. Preference may also be given, when all other factors and measures are equal, to vendors from equity deserving groups represented by their staff or company. This includes women, queer community, African Nova Scotian, Black, newcomers, Indigenous peoples, and people with disabilities.

Vendor background should include:

- Brief overview/history of the company.
- Vendor qualifications
- Areas of expertise

Transition plan: Please provide any details on how you will support a smooth transition from our current provider to your company.

B. Technical Expertise and Certifications

Describe the vendor team and areas of expertise.

- Names and resumes of specific staff that will be assigned to GEO Nova Scotia.
- List of certifications and qualifications of technical staff.
- **Subcontractor Details**: Details about any subcontractors. If subcontractors have a significant role, please provide a substantive description of their work and background. Additional information on subcontractors may be requested depending on their role.

C. Past Performance and Client References

Outline client groups (corporate, non-profit, government etc.) and briefly describe types of services provided. Provide examples of comparable organizations for which your company has provided IT support services.

- **References**: Provide three references from clients provided with similar IT support.

2.2 Service Delivery Model

A. Managed Monitoring and Security Maintenance

The vendor shall provide continuous monitoring and proactive security maintenance for all users, endpoints, and supported cloud services. Services should prevent, detect, and respond to security threats while maintaining system health and minimizing disruption.

- Describe whether it is a per-ticket, per-hour basis, block hour approach etc. and how it will be managed. Please include a statement confirming willingness to work with GEO to establish system thresholds. For example, if it is a ticket system - a threshold of $500 may be established whereby senior staff approval must be provided (to prevent excessive amounts being spent for small or low-benefit tasks).
- Outline remote and on-site support processes.

Support & Delivery Requirements:

- Continuous monitoring of user identities and endpoints
- Proactive alerting and remediation where appropriate
- Incident triage and escalation procedures
- Reporting suitable for leadership review
- Support for fully remote users

Licensing & Provisioning Requirements:

- Per-user licensing preferred
- Vendor to manage license assignment, configuration, and lifecycle
- Ability to scale up/down without undue penalty
- Non-profit pricing or cost-reduction measures must be clearly identified

B. Identity and Cloud Security (Google Workspace)

The vendor shall provide identity and cloud security services centered on Google Workspace Enterprise to protect user accounts, data, and access to cloud services including Salesforce and other SaaS platforms.

Support & Delivery Requirements:

- Monitoring and protection of Google identities
- Management of authentication policies (e.g., MFA, context-aware access)
- Detection and response to suspicious sign-in activity
- Configuration and ongoing tuning of Google Workspace security controls
- Support for secure access to third-party SaaS applications

Licensing & Provisioning Requirements:

- No requirement to migrate identity platforms
- Preference for leveraging native Google security features before adding paid tools
- Any third-party tooling must be justified and itemized
- Licenses must be scalable and cost-conscious

C. Network and Security Requirements

Outline network security measures, including cybersecurity, firewalls, intrusion detection systems, and antivirus software.

D. Data Backup and Recovery Plans

Provide an overview of your approach to creating a comprehensive data backup and disaster recovery plan to ensure business continuity.

E. Response Time and Issue Resolution

Provide a detailed description of the response and resolution times for critical and non-critical; and the hours of support service availability (hours and days of operation).

F. Maintenance and Support Services

Briefly describe the approach to the provision of ongoing maintenance and support services during regular business hours.

2.3 Pricing and Cost Breakdown

A. Detailed Cost Proposal

The vendor is requested to provide a detailed line-item cost breakdown that describes how much GEO would be charged for each aspect of the proposed IT Support Services.

Details on pricing per-ticket or per-hour. Describe any additional costs (e.g., after-hours support).

B. Additional Costs or Fees

Any additional costs, such as travel expenses or licensing fees, should be clearly specified.

Outline any volume discounts or package pricing options.
Describe any value added options, non-profit pricing or cost-reduction measures.

C. Payment Terms

Payment terms should be outlined in the proposal, including preferred billing timelines.

Appendix A

GEO Nova Scotia Current IT Support Service Description

Note: This is the organization's current environment. Vendors may propose equivalent or alternative solutions.

A1. Monitoring and Security Maintenance (Per User)

Continuous monitoring and proactive maintenance of users, endpoints, and supported cloud services to detect and respond to security threats and operational issues.
Includes: user/device health monitoring, security alert triage and response, configuration oversight, and preventative maintenance.
Current tooling examples: Ninja RMM, Atera RMM

A2. Identity and Cloud Security Monitoring

- Monitoring and protection of cloud identities and access policies to prevent unauthorized access and account compromise.
- Includes: policy drift monitoring, suspicious login alerting, and secure access enforcement.
  Current tooling examples: Google Workspace native controls; Augmentt (policy monitoring); Microsoft 365 monitoring (productivity-related monitoring only, where applicable).

A3. Endpoint Remote Monitoring and Maintenance

Remote monitoring and management of user endpoints.
Includes: patching, automated remediation, device compliance monitoring.
Current tooling examples: Ninja RMM, Atera RMM; BitLocker for disk encryption.

A4. Corporate Anti-Virus and Endpoint Protection

Centrally managed endpoint protection against malware and ransomware.
Includes: malware detection/remediation, policy management, alerting, reporting.
Current tooling example: Webroot Corporate AV.

A5. Endpoint Detection and Response (EDR)

Advanced endpoint threat detection with investigation and response.
Includes: behavioral detection, containment, incident investigation support.
Current tooling example: Blackpoint Cyber.

A6. Email Security and Phishing Protection

Layered email security to protect users from phishing and malicious content.
Includes: link/attachment scanning, advanced detection, policy enforcement, reporting.
Current tooling example: AvePoint Email Security (secondary layer).

A7. Security Awareness Training and Phishing Simulations

Ongoing security awareness training and simulated phishing campaigns.
Includes: training modules, phishing exercises, user risk metrics, executive reporting.
Current tooling examples: Webroot Security Awareness Training or KnowBe4.

A8. Cyber Warranty / Financial Protection (Optional)

Financial protection or warranty coverage related to cyber incidents.
Current tooling example: Cork.

A9. Backup and Data Protection
Backup and recovery services for cloud data.
Includes: automated backups, retention management, restore support/testing.
Current tooling example: DropSuite (Google Workspace backup).

A10. Compliance and Regulatory Management
Ongoing compliance monitoring, advisory services, and reporting aligned to Canadian regulations.
Includes: control mapping, dashboards, executive reporting, audit support.
Current tooling example: Cork (compliance management).

A11. Microsoft 365 Desktop Application Support
Support for Microsoft 365 desktop applications used occasionally by staff (e.g., Word, Excel, Outlook) in a Google-centric environment.
Includes: installation/support, troubleshooting, and compatibility guidance without migrating identity/security platforms.

A12. Salesforce Support
Support for Salesforce access and common operational issues.
Includes: user access assistance (as it relates to identity/access workflows), troubleshooting, and coordination with internal Salesforce administration where applicable.

Current Tooling Reference (Not Mandatory)

RMM: Ninja, Atera
EDR: Blackpoint Cyber
Corporate AV: Webroot
Email Security: AvePoint
Training/Phishing: Webroot campaigns or KnowBe4
Cyber Warranty & Compliance Management: Cork
M365 Policy/Monitoring Tooling: Augmentt
Google Workspace Backup: DropSuite
Disk Encryption: BitLocker