

**REQUEST FOR PROPOSAL: Cyber security audit**

The College of Physiotherapists of Ontario (“College") is inviting submissions to complete a cybersecurity audit and a comprehensive analysis and review of the College’s IT infrastructure, with the goal of detecting vulnerabilities and threats, displaying weaknesses, and high-risk practices. The College aims to hire a vendor to complete an in-depth review of the organization's security measures as a part of a comprehensive risk management strategy.

Submissions must be received by **January 17, 2024.**

**The College**

The College of Physiotherapists of Ontario is the regulatory body responsible for registering and governing the 11,000+ physiotherapists in Ontario. The College’s mandate is to protect the public interest by ensuring that College registrants are qualified, competent, and ethical practitioners.

The College has approximately 40 staff who work remotely across Ontario. The College utilizes the Microsoft Platform for the CRM, Office 365 including SharePoint and Azure. The College’s online presence includes a website, database, Public Register and online PT Portal.

**Project** **Background, Description, Requirements and Deliverables**

**The College’s external IT vendor completed an internal cybersecurity audit, identifying several actions to be taken. The next step is for the College to hire an external vendor to evaluate the effectiveness of the College’s security program** by uncovering external network vulnerabilities and threats and the level of risk exposure the organization faces both continuously and in real-time.

The College seeks to learn **where remediation or improvement is needed** to lower certain risks and decrease any risks of attack. Also, the College would like to measure **security performance improvements** over time by delivering an outside-in view of its entire digital environment.

The vendor will develop an actionable cybersecurity report and plan that includes:

* An executive summary
* Long (purpose), medium (objective, priorities) and short (action plans) term components
* Actionable and measurable outcomes
* Resources and best practice recommendations
	+ The College requires the following:
* Internal/External Penetration Testing
	+ Includes testing of firewall
	+ Review of firewall rules
	+ Approximately twenty (20) external IP addresses
	+ Internal network is 10.0.0.0/16
		- May use a sampling from various DHCP pools
		- Should include both wireless and wired clients
* Internal/External Network Vulnerability Testing
	+ Wireless network
		- Option for onsite testing of wireless required
		- Approximately Fifteen (15) access points
	+ Wired network
		- Approximately three (3) switches
* Data Governance Policy Review
	+ Current policy aligned to practice
* Deliverables, Reporting and Remediation
	+ Deliverable — Provide a report of findings
	+ Deliverable — Provide recommendations to remediate any issues
		- Not utilizing vendor as a solution
		- College should be able to remediate issues based on report without utilizing vendor (unless College requests afterward)
* Cyber Security Audit – OPTIONAL ITEMS
	+ Phishing Test
		- Option for testing approximately 40 staff members
	+ Physical Security Review – ONSITE
		- Review of physical network security
	+ Internal Control Review
		- Review of the internal controls

**Proposed Timeline**

* Proposal Released: **December 19, 2023**
* Proposal Submission Deadline: **January 17, 2024**
* Interview shortlisted Vendor: **January 24, 2024**
* Contract awarded: **February 5, 2024**

**Submission Requirements**

1. All proposals will be treated in confidence.
2. Quoted prices and discounts should be guaranteed for at least 120 days from the due date.
3. Proposals should be succinct yet comprehensive and include:
* Background information on the vendor that will support the project.
* An outline of the vendors proposed approach to strategic planning.
* The defined components of the process and a timeline for completion of each part of the process.
1. Identification and qualifications of the project lead and individuals involved.
2. The costs associated with each part of the project.
3. A minimum of 3 references, including name, position, organization, phone and email contact information.
4. A sample of the vendor’s work.

**Budget Guidelines**

Proposal must include a detailed breakdown of the project components including:

* Approximate number of days proposed and cost for:

a) the background review and work

b) draft recommendation and action plan

c) the development of a final report/action plan

**Vendor Selection Criteria (criteria is subject to change)**

1. Demonstrated expertise and experience in cyber security
2. Quality of previous work
3. Thoroughness/quality of the submission
4. Reasonableness of cost
5. Ability to meet timelines as determined
6. Demonstrated understanding of the regulatory environment

**General Terms of Proposal Process**

* The project will be tendered at the discretion of the College.
* Nothing in this request for proposal mandates that the College is obliged to award a contract under this RFP.
* The College shall not be responsible for any costs involved in or associated with preparing the submission or any meeting, discussion or negotiation following submission that could lead to acceptance of the proposal.

**Deadlines**

Anticipated timeline for project completion: **September 7, 2024**

Proposals must be submitted on or before **January 17, 2024** to:

Tom Aitas, IT Manager

IT@collegept.org

All enquiries related to this RFP should be directed, by email only to Tom Aitas at IT@collegept.org.

We look forward to receiving your response.