Peguis First Nation
Surrender
Claim Trust

# REQUEST FOR PROPOSAL

## REQUEST FOR PROPOSAL (RFP)
## Cybersecurity Audit


**PEGUIS SURRENDER CLAIM TRUST**
**BOX 942**
**PEGUIS, MB, R0C 3J0**


**MAY 14TH, 2025**

Peguis First Nation
Surrender
Claim Trust

## Table of Contents

## 1. Summary and Background

The Peguis Surrender Claim Trust represents one of the largest settlements of its kind in the history of Canada. Established in 2010 to receive, invest, manage, and administer the assets of the Trust for the benefit of the beneficiaries, Peguis First Nation, and its members.

Peguis Surrender Claim Trust is migrating its local file server network to use Microsoft 365 cloud services for shared Trust files, email services, user device back-backups and collaboration services. It is currently accepting proposals to conduct a third-party cybersecurity audit of the new cloud configuration.

## 2. Proposal Guidelines

This Request for Proposal represents the requirements for an open and competitive process. Proposals will be accepted until 5pm CST May 28th, 2025. Any proposals received after this date and time will be returned to the sender. All proposals must be signed by an official agent or representative of the company submitting the proposal.

All costs must be itemized to include an explanation of all fees and costs.

Contract terms and conditions will be negotiated upon selection of the winning bidder for this RFP.

## 3. Project Scope

The Project is currently on cloud services provided by MS365 due to migrating the current information systems of the Trust from a local file server.

| | ***In scope:*** *Cybersecurity Audit* | ***Out of Scope:*** *Information Security Audit* |
|---|---|---|
| *Focus* | Evaluate effectiveness of cybersecurity, including security controls, vulnerabilities, and cyber risk mitigation. | All aspects of information security, including physical security, administrative controls, and technical measures. |
| *Scope* | Network security, data protection, access controls, and incident response. | Entire IT environment, including hardware, software, data |

| | | |
|---|---|---|
| | | management, and overall governance |
| *Objective* | Ensure that cybersecurity measures are robust enough to protect against potential threats and comply with relevant laws and regulations | Evaluate overall effectiveness of information security controls and compliance with regulatory requirements. Improve information asset protection. |

***Audit Requirements***

The Audit should provide the following required results for stakeholders of Trust digital operations including:

- Trust system users (e.g., Trustees and staff)
- Trust beneficiaries (e.g., band members) whose personal data may be stored on Trust systems.

| | |
|---|---|
| *Assessment of Security Configurations* | The Audit will evaluate the Trust's security settings and configuration of the M365 user and cloud services environment, ensuring they align with cybersecurity best practices and industry standards. |
| *Identification of Vulnerabilities* | The Audit will pinpoint weaknesses in Trust systems and processes that could be exploited by cyber threats. |
| *Compliance Verification* | The Audit will verify whether the new cloud configuration and Trust processes comply with relevant laws, industry regulations, and standards. In particular, the audit should verify Trust compliance with, but not limited to, the following Manitoba laws:<br>1. The Personal Information Protection and Identity Theft Prevention Act<br>2. The Personal Health Information Protection Act (PHIA). |
| *Data Sovereignty* | The Audit will verify whether the Trust's data is stored on cloud servers located in Canada to ensure that storage and protection of Trust data is subject to the laws and regulations of Canada. |
| *Actionable Insights* | The Audit will provide insights into, and recommendations for improving, the digital security capabilities of the Trust, including stronger security controls, updated policies, and enhanced incident detection and response. |

| | |
|---|---|
| *Risk Assessment* | The Audit will evaluate the potential cybersecurity risks to the Trust and prioritize them based on their potential likelihood and impact. |
| *Cybersecurity Incident Response* | The Audit will review the incident response plan and procedures for actual or suspected cybersecurity breaches to ensure they are robust and effective. |
| *Improved Security Awareness* | The Audit will assess the effectiveness of current security awareness training and highlight areas for improvement. |
| *Findings and roadmap* | The Audit will document all findings and recommendations and provide a clear roadmap for addressing issues and deficiencies. |

## 4. Request for Proposal and Project Timeline

| | |
|---|---|
| Proposal Due | 5:00 pm May 28th, 2025 |
| Proposal Evaluation Completed | June 4th, 2025 |
| Select Bidder | June 13th, 2025 |
| Contract Negotiations Completed | June 16th, 2025 |
| Project Completion | July 16th, 2025 |

## 5. Budget

All proposals must include proposed costs to complete the tasks described in the project scope. Pricing should be listed for each of the following items in accordance with the format below:

## 6. Bidder Qualifications

Bidders should provide the following items as part of their proposal for consideration:

- Description of experience in overall project scope
- Examples of 3 or more Cybersecurity Audits performed by your organization or testimonials from past clients

- Anticipated resources you will assign to this project (role, title, experience and cybersecurity audit accreditations)
- Cybersecurity audit plan including expectations of Trust staff and Trustees
- Timeframe for completion of the project

## 7. Proposal Evaluation Criteria

Peguis Surrender Claim Trust will evaluate all proposals based on the following criteria. To ensure consideration for this Request for Proposal, your proposal should be complete and include all of the following criteria:

- Overall proposal suitability: proposed solution(s) must meet the scope and needs included herein and be presented in a clear and organized manner
- Organizational Experience: Bidders will be evaluated on their experience as it pertains to the scope of this project
- Previous work: Bidders will be evaluated on examples of their work client testimonials and references
- Value and cost: Bidders will be evaluated on the cost of their solution(s) based on the work to be performed in accordance with the scope of this project
- Cybersecurity audit expertise and experience: Bidders must provide descriptions and documentation of staff cybersecurity audit expertise and experience.

Each bidder must submit copies of their proposal to the address below by May 28th, 2025 at 5pm CST:

**Peguis Surrender Claim Trust**
**Box 942**
**Peguis, MB R0C 3J0**
trustmanager@peguissurrendertrust.com