ITAUKEI LANDS TRUST BOARD
(iTaukei Lands, Our Heritage, Our Future)

TENDER SPECIFICATIONS

SUPPLY, IMPLEMENTATION AND SUPPORT OF ENTERPRISE ENDPOINT PROTECTION PLATFORM

1.0 General Terms & Conditions

The following general terms and conditions will apply:

1.1 Submission of Tenders

a. Tenders must be received no later than **4:00pm Friday** 8th **May 2026**.

b. Tenderers must submit two signed copies of the proposal with one copy marked as "Original." The original version will prevail if there are any inconsistencies between the original and the copy.

c. All Tenders submissions are to be in sealed envelopes, clearly marked: "**Tender for Supply, Implementation and Support for Enterprise Endpoint Protection Platform**" and to be placed in the Tender Box located at first floor, TLTB Building, 431 Victoria Parade, Suva.

d. Submissions can also be emailed to tendersecretariat@tltb.com.fj

e. All Tenders to be submitted prior to the tender closing time.

f. The Tender response must be in the English language.

g. Should the Tenderer become aware of any discrepancy, error or omission in the Tender document submitted, and the Tenderer wishes to lodge a correction or provide additional information that material must be in writing and lodged prior to the Tender closing time.

1.2 Format of Tender Response

Each Tenderer must provide a formal letter of transmittal that must:

a. Be signed by an authorized representative of the organization and must state that the signing official is authorized to legally bind the organization.

b. Include the names, titles, office addresses and office telephone numbers of the persons authorized by the organization to conduct negotiations on the Proposal, including their expected roles in negotiations and in performance of any resulting

Agreement; and

c. Provide a contact name, address, facsimile number, and email address which TLTB will use in serving notices to the Tenderer.

d. Submit a clause-by-clause response indicating compliance with the requirements as documented in sections 6-10.

1.3 Late Tenders

Any Tender lodged after the closing time will be deemed to be late and will not be considered.

1.4 Amendment of RFT

TLTB may, at its discretion, vary, add to, or amend the terms of this RFT, including: the nature and/or scope of the services required under this RFT; and any other subject matter to which this RFT relates.

1.5 Termination of RFT

TLTB may, in their sole and absolute discretion, suspend, terminate, or abandon this RFT at any time prior to the execution of a formal written agreement acceptable to TLTB, by an authorized officer of TLTB and by the Successful Tenderer/s, by giving written notice of such a decision to each of the registered Tenderers.

1.6 Tenderers to Inform Themselves

a. Each Tenderer should:

   i. Examine this RFT, and documents referred to in the RFT and any other information made available by TLTB to Tenderers.

   ii. Obtain any further information about the facts, risks, and other circumstances relevant to its Tender by making all lawful inquiries; and

   iii. Satisfy itself that its Tender, and all information on which its Tender is based, is true, accurate, and complete.

b. By submitting their Tenders, Tenderers will be deemed to have:

   i. examined the RFT and any other information made available in writing by TLTB to Tenderers for the purpose of tendering.

   ii. examined all information relevant to the risks, contingencies, and other circumstances influencing their Tender and which is obtainable by the making of reasonable inquiries; and

   iii. satisfied themselves as to the correctness and sufficiency of their Tenders and that their prices cover the cost of complying with the RFT requirements and of all matters and things necessary for the due and proper performance and completion of the work described in the RFT.

1.7 Tenderer's Risk

The Tenderer's participation in any stage of the Tender process is at the tenderer's sole risk, cost and expense, in particular, all costs incurred by or on behalf of the

Tenderers in relation to this RFT, including preparing and lodging the Tender and providing TLTB with any further information are wholly the responsibility of the Tenderer.

TLTB accepts no responsibility, liability, or obligation whatsoever for costs incurred by or on behalf of any Tenderer in connection with any Tender or any participation in the Tender process.

1.8 Clarification and Variation of Tenders

TLTB may, at their absolute discretion, seek clarification or request further information from Tenderers after the closing date for the submission of Tenders.

Each Tenderer must nominate a person to provide additional information or answer specific questions that may arise during the selection process as required by TLTB.

Tenderers whose Tenders have been shortlisted may be required to engage in formal discussions with TLTB or make presentations to TLTB on their Tenders. In such an event TLTB will make the necessary arrangements with Tenderers.

1.9 Selection of Preferred Tenderer

Neither the lowest priced Tenders, nor any Tenders, will necessarily be selected by TLTB as the Preferred Tender/s. TLTB IT Steering Committee may decide not to accept any Tender or reject all Tenders at any time. TLTB reserves the right to cancel this RFT and pursue an alternative course of action at any time.

A Tenderer will not be deemed to have been selected as one of the Preferred Tenderer/s unless and until notice in writing for and on behalf of TLTB of such selection is:

- Handed to the Tenderer; or
- Is sent by prepaid post to or is left at the address stated in the Tender for service of notices; or
- Sent by facsimile to the number provided by the Tenderer, followed by an original by post.

Selection of Preferred Tenderer/s shall not be treated as acceptance of the Tender and no binding relationship will exist between the Preferred Tenderer/s and TLTB until a written agreement acceptable by TLTB is executed by an authorized officer of TLTB and the Successful Tenderer/s.

1.10 Conduct of Tenderers

The conduct of Tenderers or any of their consortium members, may affect the outcome of their Tender responses, including non-consideration of the Tender.

Tenderers warrant TLTB that they (and their consortium members) have not and will not engage in any of the following activities in relation to this RFT Process:

- Lobbying of or discussions with any politician or political groups during this RFT process.
- Attempts to contact or discuss the RFT process with officers, any member,

staff, or contractor currently working in TLTB or any agent of this Department; Exception to members stated in Proposal for tender.

- Provision of gifts or future promise of gifts of any sort to the previously mentioned personnel.

- Accepting or providing secret commissions.

- Submitting an inflated Tender to the advantage of another Tenderer; Entering any improper commercial arrangement with any other party.

- Seeking to influence any decisions of TLTB by an improper means; or otherwise acting in bad faith, fraudulently or improperly.

1.11 Unlawful Inducements and Collusive Tendering

Tenderer and its officers, employees, agents, and advisers must not:

- Offer unlawful inducements in connection with the Tender process; or

- Engage in any collusive tendering, anti-competitive conduct or any other similar conduct with any other Tenderer or any other person in relation to the preparation or lodgment of Tenders.

1.12 Contact with Tenderers

During the Tender process, neither TLTB nor their representatives are required to answer questions or otherwise discuss the contents of this RFT with potential Tenderers or their representatives, except in accordance with this RFT. Tenderers must not attempt to make any contact with that nature. Any unauthorized contact may disqualify the Tenderer from further consideration.

1.13 Costs

Tenderers must provide a detailed and itemized cost breakdown for all proposed services and deliverables. Lump-sum pricing without sufficient breakdown will not be considered compliant.

At a minimum, pricing must be broken down by:

- Per-endpoint and per-server licensing costs (one and three-year)
- Email security addon (one and three-year)
- Professional services – deployment, configuration, and migration (one-time)
- Optional MDR / managed service fees (if applicable – recurring)
- Optional XDR addon (1 year / 3 years)
- Training and knowledge transfer costs
- Any optional or add-on components are priced separately

The cost breakdown must clearly distinguish between one-time professional service costs and any recurring or ongoing costs (if applicable).

All pricing must be quoted in Fiji Dollars (FJD), be VAT inclusive, and represent the full cost of delivery for the proposed scope.

Prices must remain valid for a minimum period of ninety (90) days from the tender closing date.

Where estimates are provided, vendors must clearly state the assumptions used. TLTB reserves the right to seek clarification or reject proposals that present pricing as a single aggregated total without adequate detail.

1.14 Non-Delivery of Service(s)

TLTB reserves the right to hold full or partial payment until such time that the product has been delivered to the quality and expectation of TLTB.

TLTB has the right to withhold (as penalties) a percentage of the payment for vendor non-performance. Non-performance may be classed as:

- Failure to deliver on time.
- Failure to respond to queries within a reasonable amount of time.
- Introduction of unauthorized "new" clauses

1.15 Validity of Submissions

All proposals and prices shall remain valid for a period of 90 days from the closing date of the submission of the proposal. However, the responding organization is encouraged to state a longer period of validity for the proposal.

1.16 Currency

All currency in the proposal shall be quoted in Fiji Dollars and VAT inclusive and include all duties and taxes. Pricing must incorporate all Professional Services costs associated with TLTB receiving a fully configured and operational solution and must include Delivery, Installation, Configuration, Commissioning, Testing, Project Management, Documentation and Training costs.

1.17 Mergers Acquisition or Sale of Tenderer

Where such information is publicly accessible, the Tenderer must indicate whether any mergers, acquisitions or sales are planned presently or during the year following the submission of the Tender.

2.0 Project Objective & Strategic Context

The purpose of this tender is to seek proposals for the renewal or replacement of TLTB's enterprise endpoint protection platform (EPP/NGAV with EDR capability), including licensing, support, and implementation services. The tender is issued to ensure value for money, assess alternative solutions, and maintain or improve protection coverage across endpoints and servers. Optional add-ons such as XDR and MDR may be proposed as separate priced options.

TLTB currently operates an enterprise endpoint security platform with EDR and XDR capabilities. This tender is being issued to assess the market for renewal or replacement of the incumbent solution, driven by a need to ensure best value for money, capability alignment, and continued protection of TLTB's digital assets.

The outcomes of this engagement support the following strategic objectives:

- Maintain and enhance TLTB's cybersecurity posture through proactive threat detection and response.
- Ensure continuous protection of endpoints, servers, email, and identity infrastructure.
- Align endpoint security capabilities with MITRE ATT&CK and industry best practices.
- Reduce operational risk through automated detection, response, and centralized visibility.

- Achieve cost-effective, scalable security coverage across the organization

The Request for Tender document contains statements derived from information that is believed to be relevant on the date of issue but does not provide all the information that may be necessary or desirable to enable an intending contracting party to determine whether to enter a contract or arrange an agreement with TLTB. Neither TLTB nor any of its employees, agents, contractors, or advisers give any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document.

The selection of the successful vendor will be based on, but not limited to, the following five criteria:

1. Company credibility – market presence and experience with similar projects
2. Ability to meet the documented requirements
3. Technical Methodology and Approach
4. Relevant Experience, Qualifications and Capability
5. Total Cost and Deliverables

2.1 Current Environment Overview

- VMware hypervisor
- Windows 11 Pro workstations
- Windows Server 2019, 2022 and 2025 Servers
- Office 365
- Veeam backup and replication
- Linux Ubuntu Servers

2.2 Current Security Platform

a. TLTB currently operates an enterprise endpoint security platform providing antivirus, endpoint detection and response (EDR), and extended detection and response (XDR) capabilities across the organization.

b. The current deployment covers approximately:

Asset Type	Estimated Quantity
User Endpoints	350
Servers	40
Email Security Integration	360 mailboxes

Tenderers must base pricing on the above quantities and provide unit pricing for additional endpoints, servers, and mailboxes to support growth or scope changes.

3.0 Project Timelines

For renewal-only proposals (no platform change), TLTB expects licensing activation and validation to be completed within 5–10 business days. For replacement proposals (platform change), TLTB expects implementation to be completed within 6–10 weeks, subject to agreed rollout schedule and change windows.

The following high-level phasing is expected for platform change:

- Phase 1 – Project kick off, environment discovery, deployment planning, rollout strategy
- Phase 2 – Pilot deployment, tuning of policies.

- Phase 3 – Full production rollout
- Phase 4 – Handover, administrator training, documentation and project sign off.

Vendors may propose an alternate phasing approach and timelines, provided it is well-justified.

4.0 Scope of Works

TLTB is seeking proposals from suitably qualified vendors for the renewal of the incumbent enterprise endpoint protection platform and/or the supply, implementation, and support of an alternative platform that delivers equal or improved capability and value for money. The proposed solution must provide enterprise-grade next-generation antivirus (NGAV) and endpoint protection platform (EPP) capability with endpoint detection and response (EDR) as the minimum baseline, with extended detection and response (XDR) and managed detection and response (MDR) available as optional, separately priced enhancements.

Email integration may be satisfied via API-based telemetry/alert visibility and investigation linkage with Microsoft 365/Exchange Online. Full email gateway replacement is not required unless proposed as an optional add-on with separate pricing.

Base Scope (Mandatory/Minimum Requirements):

- Licensing and support for NGAV/EPP + EDR for all endpoints and servers
- Centralized management console with RBAC and reporting
- Policy deployment, tuning, and security baseline
- Alerting, investigation workflow, and containment actions (e.g., isolate device)
- Implementation support only if changing from incumbent (transition/migration plan)

Optional Scope (Must be priced separately):

- Option 1: XDR (email/identity/cloud correlation and unified incidents).
- Option 2: MDR / 24x7 SOC monitoring (service + SLA + escalation)

The selected solution (renewal or replacement) must provide continuous protection and monitoring across endpoints and servers, with strong capability for detection, investigation, containment, and remediation, and centralized visibility and reporting. The engagement must include administrator training, knowledge transfer, and comprehensive documentation. Where MDR is proposed, it must align with the MDR service requirements outlined elsewhere in the TOR and remain optional unless explicitly stated as mandatory by TLTB.

5.0 Solution Overview Requirements

The proposed solution must be an enterprise-grade, commercially supported platform that is scalable to accommodate organizational growth. It should support hybrid and cloud-first environments, including Microsoft 365 and Azure, and align with the MITRE ATT&CK framework to enable effective threat detection and reporting.

The solution should be supported by independent validation (e.g., Gartner/Forrester, AV-TEST, MITRE Engenuity evaluations, or equivalent). Vendors not listed in Gartner/Forrester must provide alternative independent evidence and comparable customer references.

6.0 Endpoint Detection & Response Requirements

(Mandatory (Base Scope)

No	Requirements	Compliance
1	The proposed solution must be an enterprise-grade Endpoint	

	Protection Platform (EPP) with integrated Endpoint Detection and Response (EDR) capabilities.	
2	The vendor's endpoint security platform should be recognized in independent industry analyst reports such as the Gartner Magic Quadrant for Endpoint Protection Platforms, Forrester Wave, or equivalent.	
3	The solution must provide next-generation antivirus (NGAV) capabilities using behavioral detection, machine learning, or AI-based threat detection techniques.	
4	The platform must provide protection against ransomware, zero-day malware, fileless attacks, and exploit-based threats.	
5	The endpoint agent must provide real-time monitoring of endpoint activity, including process execution, registry changes, file modifications, and network connections.	
6	The solution must support advanced threat detection using behavioral analysis and anomaly detection techniques.	
7	The platform must support attack timeline visualization and allow administrators to investigate the sequence of events associated with a detected threat.	
8	The platform must provide threat hunting capabilities, allowing security administrators to proactively search endpoints for indicators of compromise (IOC).	
9	The platform must provide automated response capabilities, such as isolating compromised endpoints, terminating malicious processes, and removing malicious files.	
10	The solution must support remote endpoint isolation to contain threats without requiring physical access to the device.	
11	The solution must provide centralized cloud-based management console accessible through secure authentication.	
12	The platform must support multi-layered endpoint protection, including anti-malware, exploit prevention, web protection, and device control.	
13	The endpoint security platform must support integration with threat intelligence feeds to enhance detection accuracy.	
14	The solution must align with the MITRE ATT&CK framework and provide visibility into detected tactics, techniques, and procedures (TTPs).	
15	The platform must support automated security policy enforcement across all endpoints.	
16	The solution must provide detailed security alerts and incident notifications to administrators.	
17	The solution must provide security dashboards and reporting capabilities for operational and executive-level reporting.	
18	The platform must support role-based access control (RBAC) for administrative users.	
19	The endpoint security agent must be lightweight and optimized to minimize system performance impact on endpoints.	
20	The platform must support automatic signature updates and threat intelligence updates without manual intervention.	
21	The solution must provide tamper protection mechanisms to prevent unauthorized disabling or modification of endpoint protection agents.	

7.0 Extended Detection & Response Requirements

Optional (Option 1 — must be priced separately)

No	Requirements	Compliance
1	The proposed solution must support Extended Detection and Response (XDR) capabilities across multiple security telemetry sources including endpoints, email, identity, network, and cloud environments.	
2	The solution must correlate security events from multiple sources to identify multi-stage attacks and advanced persistent threats (APTs).	
3	The platform must provide centralized visibility of security events across all protected assets within a unified dashboard.	
4	The solution must support automated threat correlation and incident prioritization to reduce alert fatigue.	
5	The platform must provide attack chain visualization, allowing security administrators to view the sequence of events involved in a security incident.	
6	The solution must support integration with email security platforms to detect phishing, malware attachments, and malicious links.	
7	The solution must support integration with identity platforms such as Microsoft Entra ID / Active Directory to detect suspicious authentication activities.	
8	The platform must support network telemetry ingestion to assist with detecting lateral movement and command-and-control communication.	
9	The solution must provide advanced threat detection using behavioral analytics, machine learning, or AI-driven detection techniques.	
10	The platform must support threat intelligence integration, including global threat feeds and indicators of compromise (IOC).	
11	The solution must provide incident investigation tools allowing analysts to perform root cause analysis.	
12	The platform must provide automated response capabilities, such as isolating endpoints, blocking malicious IPs/domains, and disabling compromised accounts.	
13	The solution must support MITRE ATT&CK framework mapping to identify tactics, techniques, and procedures associated with detected threats.	
14	The platform must provide security dashboards and incident reporting suitable for both operational security teams and executive management.	
15	The platform must support cross-product threat correlation across endpoint, email, identity, and network telemetry to identify coordinated attacks.	
16	The platform must support integration with existing network security infrastructures such as firewalls, email gateways, and identity providers where applicable.	
17	The platform must support automated security playbooks or response workflows to accelerate incident response.	
18	The solution must provide long-term event retention and search capabilities for security investigations.	

8.0 Managed Detection & Response Requirements

Optional (Option 2 — must be priced separately)

Tenderers may propose optional Managed Detection and Response (MDR) services to provide continuous security monitoring, threat detection, investigation, and response support.

Where MDR services are proposed, vendors must clearly describe their service model, SOC capabilities, escalation processes, and response procedures.

TLTB expects MDR services to augment internal ICT capabilities by providing 24/7 monitoring and rapid response to security incidents.

8.1 SOC Operations

No	Requirement	Compliance
1	The vendor must provide access to a 24/7 Security Operations Centre (SOC) responsible for monitoring and analyzing security alerts.	
2	The SOC must continuously monitor security telemetry generated by the proposed endpoint protection and XDR platform.	
3	The SOC must provide real-time threat detection and analysis of security events.	
4	The SOC must be staffed by qualified security analysts with relevant cybersecurity certifications (e.g., CISSP, GIAC, CEH, or equivalent).	
5	The SOC must leverage threat intelligence feeds and global threat research to enhance detection accuracy.	
6	The SOC must perform threat triage and validation to reduce false positives before escalating incidents to TLTB.	
7	The vendor must provide continuous threat hunting activities to proactively identify hidden threats.	
8	The SOC must maintain visibility across all integrated telemetry sources including endpoints, email, identity, and network events where available.	
9	The SOC must maintain security event logs and investigation records for audit and reporting purposes.	
10	The vendor must provide regular reporting on detected threats, security incidents, and SOC activities.	

8.2 Incident Handling

No	Requirement	Compliance
1	The MDR service must include incident detection, investigation, and response support.	
2	The SOC must provide validated incident alerts including details of the detected threat, affected systems, and recommended remediation steps.	
3	The vendor must provide incident investigation capabilities, including root cause analysis.	

4	The MDR service must support automated or analyst-initiated containment actions, such as endpoint isolation or process termination.	
5	The SOC must provide clear escalation procedures for critical incidents affecting TLTB systems.	
6	The MDR service must support remote remediation assistance where possible.	
7	The vendor must provide post-incident reports summarizing the attack, response actions taken, and recommended improvements.	
8	The vendor must maintain a defined incident response playbook aligned with industry best practices.	
9	The MDR service must support coordination with TLTB ICT staff during active incidents.	
10	The vendor must provide guidance on containment, eradication, and recovery steps following a security incident.	

8.3 Service Level Agreements

No	Requirement	Compliance
1	The vendor must provide documented Service Level Agreements (SLAs) for MDR services.	
2	The MDR service must provide 24/7 monitoring coverage, including weekends and public holidays.	
3	The vendor must define incident response times based on severity levels (e.g., Critical, High, Medium, Low).	
4	The MDR service must provide timely notification to TLTB for confirmed security incidents.	
5	The vendor must provide monthly security reports summarizing detected threats and incident activity.	
6	The MDR service must include access to a customer portal or dashboard for viewing alerts and incidents.	
7	The vendor must provide named escalation contacts for incident response coordination.	
8	The vendor must maintain secure handling of TLTB security data and logs in accordance with data protection best practices.	
9	The vendor must clearly define roles and responsibilities between the vendor SOC and TLTB ICT staff.	
10	The MDR service must include active threat investigation by security analysts and not rely solely on automated alert forwarding.	

9.0 Data Residency, Privacy and Ownership

Tenderers must provide responses indicating compliance with the following requirements

No	Requirement	Compliance
1	The vendor must clearly describe the data storage architecture of the proposed solution, including where security telemetry	

	and logs are stored.	
2	The vendor must specify the geographic location(s) of all data centers used to store or process TLTB security data.	
3	The vendor must confirm that TLTB retains ownership of all security data, logs, alerts, and telemetry generated by the solution.	
4	The vendor must ensure that TLTB security data is handled in accordance with internationally recognized data protection standards and best practices.	
5	The vendor must provide details of compliance with relevant security certifications or standards such as ISO 27001, SOC 2, or equivalent.	

10.0 Governance and Reporting

Tenderers must provide responses to the following compliance requirements:

No	Requirement	Compliance
1	The solution must provide centralized security dashboards displaying endpoint protection status, alerts, and threat activity.	
2	The platform must support security reporting for operational and executive-level stakeholders.	
3	The solution must provide customizable reports covering threats detected, incidents investigated, and response actions taken.	
4	The platform must provide regular security posture reports summarizing protection status across all endpoints.	
5	The vendor must provide monthly or periodic security reports summarizing threats detected, incidents handled, and overall security trends.	
6	The solution must provide audit logs capturing administrative activities and configuration changes.	
7	The platform must allow export of reports and security data in common formats such as PDF, CSV, or API integration.	
8	The vendor must provide recommended security configuration baselines and best practice guidance for the deployed solution.	
9	The vendor must provide documentation covering system architecture, deployment configuration, and operational procedures.	
10	The vendor must provide administrator training or knowledge transfer to enable TLTB ICT staff to manage the platform effectively.	
11	The solution must support integration with external monitoring or SIEM platforms for centralized security governance.	
12	The vendor must provide recommended metrics and key performance indicators (KPIs) for measuring security effectiveness.	
13	The solution must support alert prioritization and risk scoring to assist administrators in identifying high-risk threats.	
14	The vendor must provide periodic security posture improvement recommendations based on observed threats and platform analytics.	

11.0 Other Requirements

Tenderers must provide responses to the following compliance requirements:

No	Requirements	Compliance
1	Provide details of the corporate and ownership structure, including identification of any holding company or parent companies.	
2	Provide a profile of the company and any parent entity. If the company is a subsidiary, the Tenderer must provide full details of the legal and financial relationship between the subsidiary and parent. The names of all directors and officers of the company.	
3	Provide a full description of the current operations of the company. A financial statement for the last 3 years may be requested.	
4	Provide a copy of the company's Certificate of Incorporation.	
5	Provide confirmation that the company has the capacity to bid for the Services and that there is no restriction under any relevant law to prevent it from bidding.	
6	Provide details of any legal proceedings that are in progress against the company.	
7	Confirm the number of years the company has been in business.	
8	Confirm the tenderer holds relevant security certifications/accreditations for the services proposed. This must include evidence of authorization/partner status to supply and support the proposed endpoint security solution, and details of vendor product certifications held by staff who will implement and support the solution. Where MDR/SOC services are proposed, provide evidence of the SOC's security assurance (e.g., ISO 27001 / SOC 2) and analyst qualifications.	
9	The company must demonstrate that it has the experience and capability to successfully deliver, implement (if required), and support the proposed enterprise endpoint protection solution for TLTB. Provide details, case studies, and/or client references demonstrating comparable engagements, including deployment and support of endpoint protection (EPP/NGAV), EDR (and XDR/MDR if proposed) for organizations of similar size and complexity.	
10	The bidder must provide a detailed description of approach for each work stream as outlined in Section 5 – Technical Requirements.	
11	The bidder must provide a project schedule with proposed timelines and milestones and deliverables dates.	
12	Tenderers are to submit pricing inclusive of all requirements specified in the requirements documented on the previous pages.	