Tender Scope for Email Security Gateway

1. Introduction

The **Civil Aviation Authority of Fiji (CAAF)**, hereinafter referred to as "the Authority," is seeking proposals from qualified and experienced vendors to supply, implement, and support an **Email Security Gateway** solution. The Authority has recently migrated from an on-premise Exchange server to **Microsoft 365 with Exchange Online** for approximately **80 users**. To enhance email protection and security, the Authority intends to deploy an email security gateway that integrates seamlessly with Microsoft 365 and provides advanced features such as email recall (pull back), advanced threat protection, data loss prevention, and more.

2. Objectives

- **Enhance Email Security**
  - Provide robust protection against spam, phishing, malware, ransomware, and other email-borne threats.
  - Implement advanced threat protection capabilities, including zero-day threat detection and sandboxing.
- **Improve Email Management and Compliance**
  - Enable features such as email pull back (recall) to manage erroneous or malicious emails.
  - Implement data loss prevention (DLP) policies to protect sensitive information.
  - Ensure compliance with relevant regulations through archiving, encryption, and audit trails.
- **Seamless Integration and User Experience**
  - Integrate smoothly with Microsoft 365 and Exchange Online.
  - Provide a user-friendly interface for both administrators and end-users.
  - Offer comprehensive reporting and analytics for email traffic and security incidents.
- **Professional Services**
  - Supply all necessary software licenses and subscriptions.
  - Configure and deploy the email security gateway according to best practices.
  - Provide as-built documentation and training for the Authority's IT staff.
  - Offer ongoing support and maintenance services.

3. Scope of Work

The selected vendor will be responsible for delivering the following services:

A. Email Security Gateway Solution

1. **Solution Design and Planning**
   - Assess the Authority's current email infrastructure and security posture.

- Design an email security gateway solution that meets the Authority's requirements.
- Develop an implementation plan outlining the deployment process, timelines, and resource requirements.

2. **Licensing and Supply**
   - Provide all necessary licenses for 80 users, with scalability options for future growth.
   - Ensure that the solution includes all required features and functionalities.
3. **Implementation and Configuration**
   - Deploy the email security gateway solution in the Authority's environment.
   - Configure policies and settings to optimize security and compliance.
   - Set up integration with Microsoft 365 and Exchange Online.
   - Implement security features such as:
     - Spam and phishing protection.
     - Malware and virus scanning.
     - Advanced threat protection (e.g., sandboxing, zero-day threat detection).
     - Data loss prevention (DLP) policies.
     - Email encryption.
     - Email pull back (recall) functionality.
     - Archiving and retention policies.
4. **Testing and Validation**
   - Perform comprehensive testing to ensure the solution functions as intended.
   - Validate the effectiveness of security features and policies.
   - Conduct user acceptance testing with the Authority's IT team.
5. **Documentation**
   - Provide as-built documentation, including:
     - Solution architecture diagrams.
     - Configuration settings and policies.
     - User guides for administrators and end-users.
     - Maintenance and troubleshooting procedures.
6. **Training**
   - Conduct training sessions for the Authority's IT staff on:
     - Managing and maintaining the email security gateway.
     - Monitoring and responding to security incidents.
     - Updating policies and configurations.

B. Post-Implementation Support

1. **Warranty and Support**
   - Offer a warranty period for the implemented solution.
   - Provide support services, including:
     - Technical support (e.g., helpdesk, escalation procedures).
     - Regular updates and patches.
     - Access to knowledge bases and support resources.
2. **Service Level Agreements (SLAs)**
   - Define SLAs for response times, issue resolution, and system uptime.

- Commit to maintaining high availability and reliability of the email security gateway.

4. Requirements

A. Technical Requirements

1. **Integration**
   - Seamless integration with Microsoft 365 and Exchange Online.
   - Support for hybrid environments, if applicable.
2. **Security Features**
   - **Spam and Phishing Protection**
     - Advanced filtering to block spam and phishing emails.
     - Real-time threat intelligence updates.
   - **Malware and Virus Protection**
     - Multi-layered scanning engines.
     - Protection against known and unknown threats.
   - **Advanced Threat Protection**
     - Sandboxing capabilities to analyze suspicious attachments and links.
     - Zero-day threat detection and prevention.
   - **Data Loss Prevention (DLP)**
     - Ability to create and enforce DLP policies.
     - Pre-defined templates for common compliance standards (e.g., GDPR, PCI DSS).
   - **Email Encryption**
     - Options for automatic and manual encryption.
     - Support for various encryption standards (e.g., TLS, S/MIME).
   - **Email Pull Back (Recall)**
     - Ability to recall or delete emails from recipient mailboxes, including external recipients if possible.
     - Audit trail of recalled emails.
3. **Compliance and Archiving**
   - **Archiving**
     - Long-term storage of emails for compliance and legal purposes.
     - Secure and tamper-proof archiving solutions.
   - **Retention Policies**
     - Ability to define and enforce email retention periods.
     - Automated policy enforcement.
   - **Audit and Reporting**
     - Detailed logs of email activities and administrative actions.
     - Compliance reports and audit trails.
4. **Management and Monitoring**
   - **Administrative Interface**
     - User-friendly dashboard for administrators.
     - Role-based access controls.
   - **Reporting and Analytics**

        - Real-time and scheduled reports on email traffic and security incidents.
        - Customizable reports and alerts.
    - **User Experience**
        - Quarantine management for end-users.
        - Notifications and options to release or block emails.
5. **Scalability and Performance**
    - Capable of handling current and future email volumes.
    - High availability and redundancy options.
6. **Support and Maintenance**
    - Regular updates and security patches.
    - Access to technical support and resources.

B. Non-Technical Requirements

1. **Vendor Qualifications**
    - Proven experience in deploying email security solutions for organizations of similar size.
    - Partnerships or certifications with the proposed solution's vendor.
    - Availability of local or regional support resources.
2. **Compliance and Standards**
    - Solution must comply with relevant industry standards and regulations.
    - Support for data sovereignty requirements.

5. Deliverables

The vendor is expected to provide the following deliverables:

- **Email Security Gateway Solution**
    - All software licenses and subscriptions for 80 users.
    - Configured and fully functional email security gateway.
- **Documentation**
    - Solution design and architecture documentation.
    - Configuration and policy settings.
    - User guides for administrators and end-users.
    - Maintenance and troubleshooting guides.
- **Training Materials**
    - Training manuals and resources for IT staff.
    - Training session schedules and agendas.
- **Project Reports**
    - Implementation plan and schedule.
    - Testing and validation reports.
    - Post-implementation support plan.
- **Support Agreements**
    - Service Level Agreements (SLAs).
    - Warranty and support terms.

6. Vendor Qualifications

Prospective vendors must demonstrate the following qualifications:

- **Experience**
  - Proven track record in implementing email security solutions, particularly with Microsoft 365 environments.
  - Experience with organizations of similar size and complexity.
- **Technical Expertise**
  - Certified professionals as part of the project team.
  - Expertise in email security, Microsoft 365 integration, and compliance requirements.
- **Support Capability**
  - Ability to provide timely technical support and maintenance services.
  - Availability of local or regional support staff.
- **Training and Documentation**
  - Experience in providing comprehensive training and knowledge transfer.
  - Ability to deliver high-quality documentation.

7. Proposal Requirements

Vendors should include the following information in their proposals:

- **Executive Summary**
  - Overview of the proposal and alignment with the Authority's objectives.
- **Company Profile**
  - Background information, including years in business, areas of expertise, and organizational structure.
- **Relevant Experience**
  - Examples of similar projects completed, including client references.
- **Project Team**
  - Bios and qualifications of key personnel assigned to the project.
- **Technical Solution**
  - Detailed description of the proposed email security gateway solution.
  - Features and capabilities aligned with the Authority's requirements.
- **Methodology and Approach**
  - Implementation plan with timelines and milestones.
  - Training and knowledge transfer plan.
  - Support and maintenance strategy.
- **Cost Proposal**
  - Detailed breakdown of all costs, including licenses, services, training, and any additional charges.
- **Compliance Statement**
  - Confirmation of the ability to meet all requirements outlined in this tender.
- **Additional Information**

    - Any other relevant information that supports the proposal.

8. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- **Understanding of Requirements** (20%)
    - Demonstrated comprehension of the project scope and objectives.
- **Technical Solution** (35%)
    - Suitability and quality of the proposed email security gateway solution.
    - Compliance with the specified technical requirements.
- **Experience and Expertise** (20%)
    - Relevant experience and qualifications of the vendor and project team.
- **Methodology and Approach** (10%)
    - Soundness and effectiveness of the implementation and support plan.
- **Cost Effectiveness** (10%)
    - Value for money and transparency of the cost proposal.
- **References and Past Performance** (5%)
    - Feedback from provided references and track record of delivering similar projects.

9. Submission Instructions

- **Proposal Submission Deadline**: **29th November 2024**
- **Submission Method**: Proposals must be submitted electronically in PDF format to **tenders@caaf.org.fj**.
- **Inquiries**: All questions or requests for clarification must be submitted in writing to **tender.enquiries@caaf.org.fj**
- **Proposal Validity**: Proposals must remain valid for a period of 90 days from the submission deadline.

10. Terms and Conditions

- The Authority reserves the right to accept or reject any or all proposals without assigning any reason.
- All costs incurred in the preparation of the proposal shall be borne by the vendor.
- The successful vendor will be required to enter into a formal agreement with the Authority.
- The vendor must comply with all applicable laws and regulations.
- All work products and deliverables developed during the project will become the property of the Authority.

11. Compliance Matrix and Evaluation Criteria

To ensure a transparent and objective selection process, the Authority will use the following compliance matrix to evaluate vendor proposals. Vendors are required to complete the matrix by indicating their level of compliance and providing comments or references to their proposal where appropriate.

Compliance Matrix

Instructions for Vendors

- **Vendor Response**: Indicate your level of compliance with each criterion by selecting **Yes**, **Partial**, or **No**.
- **Comments/Reference**: Provide brief comments or references to sections in your proposal that address the criterion.
- **Points Awarded**: This column will be filled out by the evaluation committee based on the quality of your response.

Scoring Guidelines

- **Yes**: Full compliance; the vendor meets or exceeds the requirement. Eligible for full points.
- **Partial**: Partial compliance; the vendor meets some aspects of the requirement. Eligible for partial points.
- **No**: Non-compliance; the vendor does not meet the requirement. Zero points awarded.

Evaluation Criteria and Point Allocations

No.	Criteria	Description	Maximum Points	Vendor Response (Yes/Partial/No)	Comments/Reference	Points Awarded
1	**Understanding of Requirements**		**20**			
1.1	Comprehension of Project Scope	Demonstrated understanding of the tender's objectives and requirements	10			
1.2	Alignment with Authority's Goals	Proposal aligns with the Authority's strategic goals and needs	10			

2	**Technical Solution**		**35**			
2.1	Solution Features and Capabilities	Proposed solution meets or exceeds the specified technical requirements	20			
2.2	Integration with Microsoft 365	Seamless integration and compatibility with Exchange Online	10			
2.3	Security and Compliance	Adequacy of security features and compliance capabilities	5			
3	**Experience and Expertise**		**20**			
3.1	Relevant Project Experience	Experience in implementing similar email security solutions	10			
3.2	Qualifications of Project Team	Expertise and certifications of team members	10			
4	**Methodology and Approach**		**10**			
4.1	Implementation Plan	Clarity and feasibility of the proposed implementation and support plan	7			
4.2	Training and Knowledge Transfer Plan	Effectiveness of the training and knowledge transfer approach	3			
5	**Cost Effectiveness**		**10**			
5.1	Cost Transparency	Clear breakdown of	5			

		costs, fees, and expenses				
5.2	Value for Money	Competitive pricing relative to the services and solution offered	5			
6	**References and Past Performance**		**5**			
6.1	Client References	Positive feedback from previous clients	3			
6.2	Track Record	Demonstrated ability to deliver projects on time and within budget	2			
	Total Points		**100**			

Minimum Qualification Threshold

Vendors must achieve a minimum score of **70 out of 100 points** to be considered for final selection.

Evaluation Process

The evaluation committee will review each proposal against the criteria listed in the compliance matrix. Points will be awarded based on the level of compliance and the quality of the vendor's response. The vendor with the highest total points, meeting or exceeding the minimum qualification threshold, will be considered for contract award.

Please ensure that your proposal includes a completed compliance matrix. Failure to do so may result in disqualification.

We look forward to receiving your proposal and thank you for your interest in working with the Civil Aviation Authority of Fiji.