RFP for Email Cybersecurity System

1. Background

The Local Government entity is seeking proposals from qualified vendors to implement a robust email cybersecurity system as part of its broader initiative to enhance digital security, protect sensitive information, and ensure compliance across its network. With increasing threats such as phishing, malware, and data leakage via email, this project aims to reinforce the organization's cybersecurity posture through a comprehensive, cloud-based protection solution.

2. Goals

- Prevent unauthorized access, phishing attacks, and malware threats through advanced email filtering.
- Detect and block suspicious URLs, attachments, and outbound communications containing sensitive data.
- Strengthen user login security through integration with SSO and multi-factor authentication systems.
- Support real-time threat intelligence and automated incident response tools.
- Ensure the solution integrates seamlessly with existing systems and supports compliance and reporting.
- Enhance protection for all users, including faculty, staff, and students, over a 3-year licensing term.

3. Scope of Work

The selected vendor will be responsible for delivering a fully integrated email cybersecurity solution with the following capabilities:

- Filter incoming and outgoing messages using keyword detection, content filtering, and attachment analysis.
- Provide advanced spam filtering, phishing protection, anti-virus scanning, and malware detection.
- Enable sandboxing to isolate and analyze suspicious links and attachments.
- Integrate real-time threat intelligence for proactive identification of emerging risks.
- Monitor outbound email content to detect and prevent unauthorized data sharing.
- Include built-in tools for incident response, investigation, and reporting.
- Offer multi-factor authentication support and integration with existing SSO infrastructure.
- Provide URL scanning and rewriting features to block malicious links in real time.
- Allow centralized administration of email address/domain whitelisting and blacklisting.
- Support user quarantine features and geofencing capabilities based on login or message location.

4. Project Details

- Location of Work: Offsite

- Proposal Type: Fixed-term
- Proposal Deadline: April 11, 2025, 9:59 AM