REQUEST FOR PROPOSALS

EG IT SYSTEM – EXTERNAL SECURITY AUDIT

The Egmont Group Secretariat (EGS) is seeking to receive proposals from potential vendors to conduct an external (independent) security audit (ESA) of its IT system based on the requirements provided by the EGS. The successful candidate will be selected based on their experience and the appropriateness of their proposals in meeting the needs of the Egmont Group (EG).

BACKGROUND

The IT system utilizes Microsoft Entra ID, Microsoft 365 applications, and Microsoft Azure. Azure hosts several EG IT solutions hence utilizing different Azure components.

The system has been running efficiently for over two years. For the Microsoft 365, the key requirements are to ensure by end-to-end encryption that only the intended participants of any communication can access its content. When it comes to Azure resources and applications, the main requirement is to ensure that only designated users have access to specific resources. The security audit is to ensure that the system is in line with EG requirements.

SCOPE

The ESA must have a manual component (i.e., external penetration testing, which must follow the Microsoft Cloud Penetration Testing Rules of Engagement as described here). In addition, the ESA must include an assessment of the technical configuration of the system, as well as an automated process. The ESA must also include a risk assessment of malicious attacks such as malware, viruses, and phishing.

One of the most important Egmont Group requirements is that only designated users can have access the data, not even the system's administrators, or any other third-party including Microsoft. In that regard, the audit trails, identity, and access management must be of primary focus for the ESA, as well as the key generation and key management, VM access, end-to-end message encryption and secure storage of all data.

The ESA must focus on the following main components:

- **Configuration –** Includes the operational framework's cybersecurity policies, security practices, misuse monitoring, and controls.
- **External Access –** analyzes network availability, the main access method is through the web, as well as the identity, authentication mechanisms, and infrastructure security.
- **Unauthorized access to Data –** Encompasses the security measures and tools involved in protecting the confidentiality, integrity, and authenticity of data within the Egmont Group network (potentially while using test accounts).

- **Hardware Security Module (HSM)** – Refers to the level of security & hardening implemented in the HSM.
- **Compliance** – NIST and ISO 27001 Gap Analysis and other international standards applicable.
- **Deliverables** - Documented findings of audit and recommendations applicable with a suggested Plan of Action (POA) that defines actions needed to strengthen the EG IT system.

The ESA must also assess the IT security policies regulating the system.

MAIN COMPONENTS OF THE NEW EGMONT GROUP IT SYSTEM

The new Egmont Group (EG) IT System is built on a hybrid architecture combining Microsoft 365 services and Azure cloud, designed to ensure highly secure, confidential, and controlled environment. The system incorporates several layers of operational, technical, and security components that collectively uphold the EG's strict confidentiality and access control requirements.

1. Microsoft 365 Environment

The Microsoft 365 (M365) environment is a cloud-based suite of productivity and collaboration services, forming an integral part of the Egmont Group's IT system architecture. Key applications within M365 include Outlook (Exchange) for email, SharePoint for document management and collaboration, Teams for messaging and meetings, OneDrive for secure file storage, and other Microsoft applications supporting organizational workflows.

2. Azure Based Application Environment

The Azure environment consists of applications, each hosting multiple dedicated resources.
Components include but not limited to:

- Virtual Machines (VMs)
- Storage accounts
- Networking and infrastructure security elements
- Identity services and access controls

These Azure resources support modules where designated users require dedicated, isolated access to specific environments, following EG's access control standards.

3. Confidentiality and Access Control Framework

A foundational requirement of the EG IT System is that no one outside of FIUs, including administrators or external parties, may access system content.
Accordingly, the system architecture emphasizes:

- Robust audit trails
- Strict identity and access management
- Secure key generation and key management practices
- Strong VM access controls
- End-to-end encryption mechanisms

These confidentiality requirements guide the design and security posture of all system components.

CONFIDENTIALITY REQUIREMENTS

The successful vendor must sign a non-disclosure agreement provided by the EGS.

TIMELINES/DELIVERY SCHEDULE

The project in its entirety, including the presentation of the final report, needs to be completed within three (3) weeks of the project kick-off. If more time is needed, the candidate should specifically mention it in their Proposal.

The project must include minimum two (2) rounds of review on the draft report.

PROPOSALS MUST CONTAIN:

- Scope of work
- Project work plan with the specific number of days of effort for each deliverable
- Fee (please note currency) including expected time to complete
- Proposed payment schedule
- Curriculum Vitae, which must describe the following:
    - Qualifications and at least five (5) years of experience
    - Certifications and designations, for example, Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Cloud Security Professional (CCSP), Systems Security Certified Practitioner (SSCP), Certified Encryption Specialist (EC-Council ECES), Certified Expert Penetration Tester (CEPT), ISO/IEC 27001, etc.
    - Documentation demonstrating having proper security clearance for the vendor and staff who would be involved in the ESA. *Note: people performing the ESA must be hired staff. No third-party professionals will be accepted*.
    - Biography of each person performing the ESA
    - Description of similar projects completed for government and/or security-sensitive companies, including recommendation letters with their contact information.
- Support that will be expected from the EG

SELECTION CRITERIA

Proposals will be evaluated against the following criteria:

- The vendor must successfully pass the security screening. Additional information may be required to complete the background check.
- Lowest responsive offer
- Proposed payment schedule
- Adherence to specifications and requirements
- Delivery commitments are exclusive and inclusive of the lowest price
- Qualifications and experience of the vendor and person performing the audit
- Vendor’s compliance with instructions for submitting required documentation

APPLICATION METHOD

All submissions must be sent to ESAProposal@egmontsecretariat.org no later than March 13 2026, with the following subject line: **EG IT System – External Security Audit.**

All proposals must be in ENGLISH. Only the selected candidate will be approached for further contract-related negotiations and provided with the full framework.