Terms of Reference (ToR): Cybersecurity Lead

Entity: Digital Transformation Office (DTO)

Division: Strategy & Governance
Ministry: Ministry of Education and Higher Education (MEHE), Republic of Lebanon
Position Title: Cybersecurity Lead
Reports to: Head of Strategy & Governance Division

1. Role Purpose & Strategic Context

The Ministry of Education and Higher Education (MEHE) is establishing a Digital Transformation Office (DTO) to lead its IT modernization. The Cybersecurity Lead is a senior strategic role within the DTO's Strategy & Governance Division, responsible for architecting and implementing the Ministry's comprehensive cybersecurity program.

The primary objective is to transform the Ministry's security posture by **establishing clear security standards, building a proactive Security Operations (SOC) function, and embedding a "secure-by-design" methodology** into all technology projects, all while championing ministry-wide security awareness.

2. Core Responsibilities

- **Security Architecture & Standards:** Architect the Ministry's core security strategy, risk framework, and data governance policies. Define and publish the official MEHE IT security standards for all systems, data, and networks.
- **Security Operations (SOC):** Lead the design, implementation, and day-to-day operation of a modern SOC function to ensure proactive threat detection and rapid incident response.
- **Awareness & Enablement:** Design and deliver a continuous security and data management awareness program for all MEHE staff.
- **Governance & Project Assurance:** Act as the primary security authority for all new projects. Review all technology procurements and development plans to ensure security is built-in from the start (secure-by-design).
- **Risk & Compliance:** Lead governance initiatives (including frameworks like ISO 27001) and oversee all security audits, vulnerability assessments, and penetration tests to ensure standards are met.

Note: The responsibilities and deliverables outlined in this TOR are foundational. The DTO leadership may dynamically adjust priorities and plans to ensure alignment with the Ministry's evolving strategic objectives, which may imply changes to the mandates outlined in this ToR including its title. The candidate is required to fully abide by these changes, demonstrating flexibility and a commitment to continuous improvement.

3. Key Deliverables (First 3 Months)

1. **Security Baseline & Gap Analysis:** Deliver a report detailing the current posture against best-practice standards (e.g., ISO 27001, NIST) and a clear remediation roadmap.

2. **SOC & Security Solutions ToR (v1.0):** Finalized ToR for the "Cybersecurity Solutions & Assessment" project, with a clear focus on SOC and threat detection.
3. **Security Awareness Content (v1.0):** Content for the first mandatory staff awareness session.
4. **Foundational Standards & Policies (Draft):** Drafts of three (3) key policies/standards (e.g., Acceptable Use, Incident Response, Secure Project Lifecycle).
5. **SOC Feasibility Brief:** High-level options analysis, cost estimate, and recommended model (in-house, hybrid, managed) for the SOC.

4. Key Qualifications & Experience

- **Experience:** 5+ years in cybersecurity, including a leadership/management role.
- **SOC Expertise:** Demonstrable experience building or managing a Security Operations Center (SOC).
- **Policy & Standards:** Experience authoring, implementing, and enforcing enterprise-wide security standards and policies.
- **Frameworks:** Proven experience with security frameworks and standards (e.g., ISO 27001, NIST).
- **Technical Skills:** Strong knowledge of SIEM, EDR/XDR, cloud security, and secure development principles.
- **Education:** Bachelor's degree in CS, Information Security, or related field. (Master's preferred).
