Job Description: Chief Information Security Officer (CISO)

Position: Chief Information Security Officer (CISO)

Reports to: Chief Executive Officer (CEO)

Location: Cyberjaya, Malaysia

About MyDigital ID Sdn Bhd (MyIDSB)

MyIDSB is a Tier 1 Government-Linked Company (GLC) wholly owned by MOF Inc., tasked with operating MyDigital ID (MyDID), Malaysia's national digital identity platform. MyDID is classified as National Critical Information Infrastructure (NCII) under the oversight of Majlis Keselamatan Negara (MKN). Our mission is to provide a secure, sovereign, and trusted digital identity infrastructure for Malaysia, safeguarding national security while enabling the digital economy.

Role Overview

The Chief Information Security Officer (CISO) will lead the development, implementation, and management of MyIDSB's cybersecurity strategy, ensuring the resilience and trustworthiness of MyDID. This role is critical in protecting the integrity of Malaysia's national digital identity, managing cyber risks, ensuring compliance with national and international standards, and maintaining stakeholder confidence.

Key Responsibilities

- Strategic Leadership
  - Define and execute the organisation’s cybersecurity strategy in alignment with MyDID’s role as NCII.
  - Advise the CEO, Board, and regulators (MKN, NACSA, MOF) on cybersecurity posture, risks, and mitigation.
- Risk & Compliance
  - Ensure compliance with NCII management guidelines, ISO/IEC 27001, NIST SP 800-63C, Common Criteria (CC), and other relevant standards.
  - Lead risk assessments, security posture analyses (SPA), and regular audits.
  - Develop and enforce information security policies, incident response plans, and disaster recovery procedures.
- Operational Security
  - Oversee identity lifecycle security, PKI, post-quantum cryptography migration, blockchain trust layer, and federated identity assurance.
  - Manage security monitoring, threat intelligence, and incident detection/response.
  - Coordinate independent penetration testing and red-team exercises.
- Stakeholder Engagement
  - Serve as the main liaison with regulators, government security agencies, and industry partners on cybersecurity matters.
  - Promote a culture of security awareness across the organisation through training and education.
- Team Leadership
  - Build and manage the cybersecurity team (internal or outsourced functions as required).
  - Ensure continuous professional development for the team to keep pace with evolving threats.

Qualifications & Experience

- Bachelor’s or Master’s degree in Computer Science, Cybersecurity, Information Systems, or related field.
- Professional certifications such as CISSP, CISM, CISA, or equivalent.
- Minimum 10–15 years of experience in information security, with at least 5 years in a senior leadership role.
- Proven track record in managing cybersecurity for critical infrastructure, financial services, or government systems.
- Strong understanding of cryptography, identity management, PKI, and cloud security.
- Familiarity with Malaysian regulatory frameworks (PDPA, NCII guidelines, upcoming DIGA) and international standards.

Personal Attributes

- High integrity and professional ethics, with a strong commitment to national security.
- Strategic thinker with the ability to balance security, usability, and operational realities.
- Excellent communication skills to explain complex risks in simple terms to non-technical stakeholders.
- Ability to work under pressure and make critical decisions in high-stakes situations.

Why Join Us?

- Play a pivotal role in safeguarding Malaysia’s digital sovereignty.
- Lead security for one of the nation’s most critical infrastructures.
- Work with top government stakeholders and international partners on cutting-edge identity and cybersecurity initiatives.