ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

POST OF CHIEF INFORMATION SECURITY OFFICER (ON CONTRACT)

1.1 Role Purpose:

Drive direction, development and execution of cybersecurity strategy through effective security governance and compliance, security risk surveillance and control assurance, security engineering and solutions, cyber threat management and cyber defense management with business stakeholders' collaboration to ensure enterprise-wide cyber resilience, protection of the Bank's critical digital assets, and for the Bank to confidently adopt digital and technology innovation to achieve its business outcomes.

1.2 Principal Accountabilities:

VISIONING AND DIRECTION-SETTING

- Drive cyber security vision and set appropriate direction that align with the Bank's financial stability mandate and growth through digital and technology adoption and instigate transformational change to manage risk through valued investments
- Establish cyber security strategies, framework and policies in line with the current and emerging business requirements based on global best practices
- Promote awareness of security issues and trends among senior management to ensure sound security principles are reflected in the Bank's vision and goals

CYBER AND DIGITAL TRUST STRATEGY

- Lead the development of the cyber and digital trust strategies and roadmap, and integrate them with the business to educate, advise, and influence activities with cyber risk implications
- Drive the creation of enterprise digital assets protection and capabilities for short, mid, and long terms
- Advise the Board and Senior Management committees on emerging cyber and technology risks and action plans for appropriate risk management

PROTECT ENTERPRISE DIGITAL ASSETS

- Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk program
- Conduct long-range, strategic planning efforts internally with business process owners/line departments to ensure comprehensiveness of information assets and transaction integrity controls and protection plans
- Lead and steer implementation of security technologies and standards to build organizational capabilities

TECHNOLOGY VULNERABILITY MANAGEMENT

- Lead and steer assessment of security in current and new technologies adoption in the Bank
- Provide direction on security standards development, architecture, engineering and solutions to ensure secure by-design system development
- Monitor and evaluate the effectiveness of the Bank's cybersecurity safeguards and technology risk management to ensure that they provide the intended level of protection and meet cyber resilience and digital trust objectives

CYBER THREAT SURVEILLANCE OPERATIONS

- Drive, establish and oversee the Bank's Cyber Threat Surveillance Operations
- Provide direction for continuous improvements to the Bank's Cyber Threat Surveillance Operations to ensure that they are relevant against evolving sophisticated threats

1.3 Generic Accountabilities

CYBER INCIDENT MANAGEMENT

- Establish and drive continuous improvements for the Bank's Cyber Incident Response Plan to ensure a systematic and relevant cyber incident management
- Oversee or supervise and update the Board and Senior Management on protective or corrective measures when a major cybersecurity incident or vulnerability is discovered
- Interface with external organizations (e.g., public affairs, law enforcement, committees, or councils) to ensure appropriate and accurate dissemination of incidents and other cyber defense information

CAPABILITY DEVELOPMENT AND PROGRAM MANAGEMENT

- Translate and communicate implications of the Bank's cybersecurity vision to the team and build target capabilities program that enable execution of the Bank's cybersecurity objectives
- Define, acquire and manage the necessary resources, including leadership support, financial resources, and key security leadership personnel, to support the Bank's cyber security goals and objectives
- Lead, motivate, engage and encourage staff's cybersecurity upskilling program through participation in cyber security competitions and hands-on or simulated practical training

CYBER AWARE AND RESPONSIBLE CULTURE

- Instill and drive the culture for cyber aware and responsible among all staff in the Bank
- Provide direction and execute enterprise-wide cyber security education campaign and programs to ensure continuous dissemination of cyber threats and defense measures for all staff in the Bank
- Provide direction, execute, and report results of phishing simulation and security awareness assessments, and action plans to continuously improve staff awareness

ENTERPRISE RECOVERY ASSURANCE

- Review recoverability aspects of critical business applications, IT systems and infrastructure to ensure that system is able to recover within expected timeframe, in the event of cyber incidents
- Provide regular reporting to the Board and Senior Management on system recoverability risks and improvement action plans including mitigation controls
- Ensure IT Security considerations are integrated with IT systems planning, development and acquisition

METRICS REPORTING AND IMPROVEMENT PLANS

- Drive, establish and oversee the Bank's cyber threat metrics including KPIs, KRIs and KCIs
- Provide regular reporting to the Board and Senior Management on cyber threat metrics and improvement plan status

2.0 Required Minimum Qualifications & Experience:

2.1 Educational/Professional Qualifications

Bachelor's (minimum of three (03) years) or Master's degree related to Cyber Security/Information Security/IT Security/Network Security obtained from a local or foreign university recognized by the University Grants Commission of Sri Lanka or accredited by the Institute of Electrical and Electronic Engineers (IEEE).

One or more professional certifications such as of ISACA Certified in Risk and Information Systems Control (CRISC), ISACA Certified Information Systems Auditor (CISA), ISACA Certified Information Security Manager (CISM), or (ISC)2 Certified Information Systems Security Professional (CISSP) are highly desirable.

2.2 Experience:

Minimum of 15 years of hands-on experience in the fields of Cyber Security/Information Security/IT Security/Network Security with strong knowledge of cyber security risks, emerging threats, business risks and leadership.

Knowledge of IT infrastructure and service management is an added advantage.

2.3 Preferred Competencies

Competencies in the following areas are highly desirable.

- Cybersecurity threat landscape, adversaries and best practices
- Global standards i.e., NIST/COBIT/ISMS/ISO27001
- Cybersecurity Risk and Controls, Governance and Compliance
- Enterprise Security and Technical Architecture
- IT Management, Systems and Technology
- Enterprise Risk Management and Internal Controls
- Strategic Management and Integrated Thinking
- Team building capability with drive for performance excellence
- Organizational Understanding and Holistic Collaboration

Applicants are strictly advised to submit copies of the certificates relevant to the educational/professional qualifications & work experience. Any application without the copies of the above documents will be rejected without any notice at any stage of the recruitment process.

3.0 Employment:

On contractual basis for a period not more than three (03) years. Contracts will be initially signed for one (01) year, and it will be renewed annually based on performance.

4.0 Remuneration and Other Benefits:

An attractive package on par with the market standards (negotiable) and contributions to Employees' Provident Fund & Employees' Trust Fund.

Selection Procedure

Suitable candidate will be selected based on one or more interviews

Applications

Application forms could be downloaded from the official website of the Central Bank of Sri Lanka **https://www.cbsl.gov.lk/en/careers**. Applicants are strictly advised to adhere to the prescribed application format and send the duly completed applications with all the required documents to the following address to reach the Director/Human Resources by registered post **on or before 08.11.2024**. It is required to indicate **"Application for the Post of Chief Information Security Officer (On Contract)"** on the top left hand corner of the envelope.

Those who do not possess the required qualifications and experience as at the closing date will not be eligible to apply for this post. Any application not meeting the required qualifications, received after the deadline or not in the prescribed format, will be rejected without any notice. Candidates who fail to provide originals of relevant documents at the certificate verification conducted prior to the interview, will not in any manner be considered as eligible candidates. Any form of canvassing will be a disqualification. CBSL reserves the right to postpone or cancel the recruitment. Only shortlisted candidates will be contacted for the next step of the recruitment process.

Director – Human Resources
Central Bank of Sri Lanka, No. 30, Janadhipathi Mawatha, Colombo 01.
Telephone : 011-2477330 Fax : 011-2477715