Job Description

SriLankan Airlines Ltd, the National Carrier of Sri Lanka operates with a network of destinations throughout Asia, the Middle East, Europe, and Australia. The Airline has a strong presence in Maldives and Southern India. SriLankan is a member of the 'oneworld' alliance.

SriLankan IT Systems drives the airline's IT strategy through digital transformation, technology adoption, data modeling, business intelligence, and business continuity. The focus is on transforming business and operational processes, expanding digital passenger reach, and improving customer experience through solutions design, development, and integrations while enhancing airline IT domain knowledge. Award-winning SriLankan IT team is seeking a dynamic individual to join as a Cyber Security Manager.

The individual is responsible to ensure Cyber Security of SriLankan Airlines and its subsidiaries and thereby prevent undue, unexpected interruptions in IT services through implementation of service & system controls and continuous monitoring to avoid or minimize the business impact on critical and core airline business processes and operations in the airline. Cyber Security Manager is responsible for the continuous improvement of Cyber Security in the Group by setting a dynamic service relationship with internal (IT), external (business) stakeholders, third-party service providers and regulatory and legislative authorities. The role will require in-depth understanding of cyber security, technology architecture and business security whilst working in a dynamic environment dealing with complex challenges in all levels of the business operations.

Key responsibilities will include:

- Responsible to direct and enforce mitigation strategies to reduce SriLankan Group's attack surface and ultimately reduce and maintain the risk exposure of the organization within acceptable limits in consultation with senior management to formulate the cyber security strategy across the group whilst ensuring that the organization is adequately protected and resilient against cyber threats and attacks.

- Responsible to architect proactive defense mechanisms to mitigate cyber-attacks and be the focal point for cyber defense and information risk related matters. Accountable for planning, designing, and improving Cyber Security across SriLankan Airlines and its subsidiaries.

- Ensure the design of Cyber Security detection and protection is always operational and proactive. Design information security processors for required areas of work to assure mechanism are in place. Address supply chain management and performance issues within the supply chain to meet organizational objectives whilst increasing process efficiency and effectiveness.

- Coordinate and liaise with internal and external stake holders, consultants, auditors, third-party service providers and peers in oneworld Alliance and other Airline Cyber Security teams to maintain an up-to-date cyber security platform and an efficient threat exchange framework. Present findings on cyber security and Privacy Management to stakeholders, not limited to, senior management and internal audit.

- Establish a 3-year rolling plan for Cyber Security and Privacy Management within SriLankan Airlines and its subsidiaries. Coordinate with project stakeholders and advice on evaluating information security related risks. Identify root cause analysis for service outages that may have security/privacy implications and disrupt operations. Drive privacy related initiatives to be incorporated into the Cyber security program. Responsible for electronic Information protection, to prevent internal information from being disclosed or leaked. Performing activities as per Infosec Calendar, risk register and Infosec related activities. Be responsible for monitoring all "un-discovered and hidden service interruptions" at operational areas, irrespective of the level of business impact and establish a good IT services governance to manage such occurrence through appropriate solutions.

- Responsible for budgeting and capacity planning for deployed and proposed projects. Interface to resolve issues between business requirements and security requirements. Be responsible for IT service continuity requirements as stipulated in Information Security Management (ISMS) as per the latest international standard ISO/IEC 27001 (Information Security Management System) and latest ISO/IEC 27701 (Privacy Information Management System). Provide senior expertise, consultation and thought leadership for other experts in the cyber security, privacy management and service continuity domains. Ensure continued certification for latest versions of ISO/IEC 27001 and ISO/IEC 27701.

- Make all key stakeholders in IT Service Management aware on the importance of the required work and practices in Cyber Security and Service Continuity. Communicate with end users on existing cyber security policy's, new changers, new and emerging threats to the organization and educate them of the importance of adherence.

Requirements

- Bachelor's Degree* with at least 04 years post qualifying work experience at Executive level out of which at least 02 years at Senior Executive Level with industry certification from a Professional Body on relevant competency. (* Engineering, Computer Science, General Science with Mathematics, Management Information Systems, Applied Statistics)
  OR
- Full professional qualification equivalent to a degree with 5 years' experience out of which 2 years in Senior Executive level in a relevant discipline.

Age to be not more than 40 years as at 16th October 2024 which is the closing date.

Be a Sri Lankan citizen.

Influencing will be a reflection of unsuitability.

We are an equal opportunity Organization.

Employment will be offered on fixed term contract.

Please note that we will correspond with you within a month of closing the advertisement in the event your application is shortlisted for consideration.