Electricity Company Ghana Limited

Job Description

Chief Information Security Officer

Job Summary

The Chief Information Security Officer (CISO) is responsible for establishing and maintaining the information security program to ensure that information assets and associated technology, applications, systems, infrastructure, and processes are protected in the digital ecosystem in which ECG operates

This role will also work very closely with the executive leadership team to determine acceptable levels of risk for the organisation. They will proactively work with business units, engineering teams and ecosystem partners to implement practices that meet agreed-on policies and standards for information security.

The CISO should understand and articulate the impact of cybersecurity on the business and be able to communicate this to the board of directors and other senior stakeholders.

The CISO would report to the Managing Director of ECG.

Role and Responsibilities

1. Leads the information security function across the Company to ensure consistent and high-quality information security management in support of the business goals.

2. Determines the information security approach and operating model in consultation with stakeholders and aligned with the risk management approach and compliance monitoring of non-digital risk areas

3. Develops an information security vision and strategy that is aligned to organisational priorities and enables and facilitates the organisation's business objectives, ensures senior stakeholder buy-in, and is responsible for establishing and maintaining best practices to comply with the IT security requirements for regulations and standards

4. Establishes and leads an Information Security Governance structure including appropriate committees and advisory boards

5. Be knowledgeable about both internal and external business operating environments, and ensure that information systems are maintained in a fully functional and secure mode and are compliant with legal, regulatory, and contractual obligations

6. Creates an information security awareness training program for all team members, contractors, and approved system users, and establishes metrics to measure the effectiveness of this security training program for the different audiences

7. Creates and manages a unified and flexible, risk-based control framework to integrate and normalize the wide variety and ever-changing requirements resulting from relevant laws, standards, and regulations

8. Liaises with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organisation maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies

9. Liaises with the enterprise architects and project leadership to build alignment between the security and enterprise architectures, thus ensuring that information security requirements are implicit in these architectures and security is built in by design

10. Works with Compliance to ensure that all information owned, collected or controlled by or on behalf of the Company is processed and stored in accordance with applicable laws and other relevant regulatory requirements, such as data privacy

11. Develops and oversees effective disaster recovery policies and standards to align with the enterprise business continuity management (BCM) program goals

12. Coordinate the development of implementation of incident response plans and procedures to ensure that business-critical services are recovered in the event of a security event; provides direction, support and in-house consulting in these areas

13. Provide regular reporting on the current status of the information security programme to enterprise risk teams, senior business leaders and the Board of Directors as part of a strategic enterprise risk management programme, thus supporting business outcomes.

14. Understand and interact with related disciplines to ensure the consistent application of policies and standards across all technology projects, systems and services, including privacy, risk management, compliance and business continuity management.

15. Ensure full implementation of all cyber and information security programmes, driven by regulations (Cybersecurity Act, 2020), the Directive for the Protection of Critical Information Infrastructures (CIIs) or any information and cybersecurity programme approved by the Board of Directors of the ECG.

16. Coordinate security response activities with relevant stakeholders at the national level and third-party vendors.

17. Provide clear risk mitigating directives for projects with components in IT, including the mandatory application and implementation of security controls.

18. Coordinate with Procurement and Vendor Management Departments to ensure that information security requirements are included in contracts by liaising with vendor management and procurement organisation.

19. Serve as a Focal Point on Cybersecurity regulations in view of ECG's designation as a Critical Information Infrastructure (CII) Owner)

20. Other duties as may be assigned by the Board or Management.

Qualifications And Education Requirements

1. Bachelor's Degree in information Security, Computer Science or related field, or an equivalency of education and work experience. Post-graduate qualification in relevant area is recommended

2. Certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Audit and Implementations Certification. or other similar credentials.

3. Minimum of ten (10) years of experience in a combination of IT/cyber risk management, information security and IT or OT jobs (at least five (5) must be in a senior leadership role).

4. Experience successfully executing Information Security Standards in meeting the objectives of excellence in a dynamic business environment

5. Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate information security and risk-related concepts to technical and nontechnical audiences at various hierarchical levels, ranging from board members to technical specialists.

6. Strategic leader and builder of both vision and bridges, and able to energize the appropriate teams in the organisation

How to apply:

Please e-mail a copy of your CV, a covering note with the email subject line "**ECG CISO Job Application**" to camartey@ecggh.com