**Overview**: The Chief Information Security Officer (CISO) is responsible for establishing and maintaining the enterprise vision, awareness, strategy and programs to ensure information assets and technologies are adequately protected. The CISO will provide executive leadership over the information security and information governance functions of the organization. They will work with Information Technology (IT) and other business programs in identifying, developing, implementing, and maintaining technologies, processes, procedures, and protocols across the organization to ensure the security, integrity, and appropriate handling of information and to reduce information and information technology (IT) risks. This position will report to Chief Risk Officer.

**Position Responsibilities:**

* Drive awareness and articulate the business value of information/data security and governance throughout the enterprise
* Lead strategic planning to achieve business goals by identifying and prioritizing initiatives and setting timetables for development, deployment, and evaluation
* In partnership with Information Technology and other business programs, oversee
	+ The identification, development, implementation, evaluation, and maintenance of technologies, processes, procedures, and protocols to ensure the security, integrity, and appropriate handling of information and to reduce information and IT risks
	+ The development and maintenance of contingency plans
* Ensure comprehensive risk analysis to identify gaps, integration of appropriate security tools and analysis capabilities
* Oversee the management of security breaches
* Oversee the communication and education/training to increase and maintain information security awareness and vigilance and to ensure compliance with regulations and security policies.
* Provide technical leadership in developing and maintaining cost effective services and resources.
* Maintain State Fund’s Information Security Program, identify gaps, communicate status to Executive/Board of Directors, and follow up with programs for gap remediation,
* Establish a governance process that meets government, partner, and company expectations for customer information privacy.
* Lead an Enterprise Security program that operates at the highest level to support IT and business partners in information security and governance, fostering sound business practices, cost effectiveness and accountability.
* Lead an information security team that
	+ Makes recommendations to business partners on risk mitigation
	+ Maintains Information Security Policies, Sub-policies, and Standards in partnership with IT
	+ Assists internal customers with confidential computer investigations
	+ Develops a process to evaluate State Fund’s security awareness and recommend appropriate training
	+ Chairs the Information Security Advisory Committee
	+ Anticipates and responds appropriately in conjunction with IT to information security breaches and incidents
	+ Works with IT and business partners to ensure security in the software development lifecycle
	+ Gathers threat intelligence and shares with IT counterparts as applicable
* Lead an information governance team that works with business partners as needed to
	+ Ensure the proper handling of information throughout its lifecycle until it is deleted or destroyed
	+ Maintain a data classification policy and implement data classification across the enterprise
	+ Make recommendations and provide guidance and support on information governance practices and maturity
* Develop specifications, select and manage vendors responsible for implementation of Enterprise Security applications.
* Facilitate, establish and build strong working relationships and partnerships with business units and senior management to assess operational needs and recommend technologies that support the organization.

**General Management Responsibilities:**

1. Monitor key performance metrics to drive continuous improvement efforts in all areas and provide regular updates to senior leadership to ensure prompt attention to areas of concern.
2. Enable the successful performance and development of employees by establishing expectations and goals at the beginning of the appraisal year, providing constructive feedback throughout the year and in the annual performance evaluation process. Ensure personnel are appropriately trained according to the regulatory policies and procedures.
3. Uphold and ensure that operations meet the highest ethical standards.
4. Foster a performance-based, accountable environment.
5. Provide quality customer service in an ethical and timely manner.
6. Establish and maintain effective working relationships.
7. Follow the principles of State Fund’s Equal Employment Opportunity guidelines.
8. Maintain a safe working environment.
9. Defend State Fund against fraudulent activities.

**Position Requirements:**

* 7 years significant experience in the Information Security and/or IT audit arena (minimum of 2 years of Information Security experience is required).
* Bachelor’s degree, MBA or equivalent preferred.
* Possess exceptional technology skills and have a comprehensive understanding of information security paradigms and technologies
* Outstanding financial and analytical skills.
* Superior communication, organizational, and project management skills.
* Proven ability to independently manage multiple priorities.
* Ability to lead effectively and proactively within a team setting.
* Capacity to actively engage and communicate with a wide variety of employees, senior leaders and external vendors to drive change and problem solve.
* Skilled in researching, interpreting, and presenting data in a concise manner.
* Demonstrated strong ability to effectively plan, organize, and delegate.
* Occasional travel as required.