Job Title: Information Security Manager

Position Purpose

Under the direction and guidance of the Senior Vice President/Director of Information Technology, the Information Security Manager will be involved in nearly all aspects of information security and cybersecurity projects and activities for the Bank, ensuring compliance with security policies and helping to mitigate risks. The Information Security Manager is responsible for developing, implementing, and maintaining the organization's information security program in compliance with the FFIEC IT Examination Handbook and other regulatory requirements. The Information Security Manager also ensures the protection of sensitive data, manages cyber risks, and works closely with management, IT, risk, and compliance teams to enforce security policies, controls, and best practices.

Essential Duties and Responsibilities: *The following represents a list of essential duties and responsibilities; other duties may be assigned as required.*

- Policies and Procedures:
  - Participate in and/or create and refine applicable information security policies and procedures, including those related to vulnerability management, configuration management, incident management, and business continuity and disaster/recovery planning.
  - Work with internal staff on an information and cybersecurity training curriculum to educate employees on attack vectors that may indirectly or directly target employees.
  - Participate in or completes IT audit, risk assessment, and network testing remediation plans depending on disciplines in which changes are required.
  - Complete ongoing activities articulated in the Bank's information security program; develop security standards, procedures, and guidelines for multiple platforms.

- Monitoring and Maintenance:
  - Perform application user access and permission reviews, ensuring adherence to minimal access needed to conduct job functions.
  - Per strategic direction, monitor system controls in accordance with the Bank's selected security framework and systems, including review of log files from various tools such as firewalls, IDS/IPS, EDR/NGAV, SIEM, Active Directory event log monitoring, and alerting.
  - Log, track, and report security events and/or incidents that may occur within IT systems, vendor systems, or across Bank business units. Investigate, document, and action any issues.
  - Identify security vulnerabilities and remediate them with strategic solutions that increase data security.
  - Oversee the regular reporting of the FDICIA program to Senior Management and Auditors.
  - Ensures the effective management and implementation of FDICIA controls as well as assessment of these controls to ensure compliance.
  - Participate in completing required regulatory activities such as risk assessments, incident response exercises, GLBA reporting, audit testing, the Ransomware Self-Assessment Tool, and the Cybersecurity Assessment Tool. etc.
  - Keep updating the CRI 2.0, formerly the CAT Tool (Cyber Assessment Tool).

- Products, Tools and Vendors:
  - Collaborate with the Senior Vice President/Director of Information Technology to make recommendations on the selection of security products and solutions and review, implement, and configure approved solutions with the assistance of the vendor/service provider.
  - Assist the Senior Vice President/Director of Information Technology in developing and maintaining the Threat Intelligence Program and in identifying and enhancing key performance and key risk indicators and other security metrics.
  - Work with independent vendors to scope and carry out vulnerability assessment, penetration testing, and other IT assurance testing activities.

Other Duties

- Performs other job-related IT duties as assigned. The above is a description of the ordinary duties of the position. It should be expected, given the nature and speed of the cybersecurity landscape, other duties both related and unrelated to the above may be assigned and therefore required.
- Attend trainings and seminars as needed to maintain a working knowledge of the positions' requirements.
- Adhere to all Bank policies and procedures that are outlined in the Bank's Employee Guidelines, such as Work Schedules and Timekeeping.

Managerial Responsibilities

- N/A

Minimum Required Technical Skills and Qualifications

- 5+ years of experience in Information Security with a demonstrated progression of increased responsibilities.
- IT audit, vendor management, and oversight experience.
- Experience conducting risk assessments and/or compliance reviews.
- Strong understanding of Information Security frameworks, including but not limited to: Vulnerability scanning, endpoint detection and response (EDR), network access control (NAC), security and information event management (SIEM), Gramm-Leach-Bliley Act (GLBA), and intrusion detection/prevention systems (IDS/IPS).
- Knowledge of common information security management frameworks, such as ISO/IEC 27001, and NIST.
- Strong understanding of FFIEC guidelines, Information Security frameworks, PCI-DSS, GLBA and banking regulations.
- Experience with security architecture, incident response, SIEM tools, and identity access and management.
- Familiarity with cloud security, digital banking risks, and payment systems security.
- Experience in banking or financial services is highly preferred but not required.
- Ability to travel throughout the Bank's retail branch network on an as needed basis.
- Strong organization, prioritizing and communication skills; attention to detail; ability to think analytically.

Education/Certifications/Licensure

- Bachelor's degree in Computer Science, Information Systems, Cybersecurity, Information Security or a closely related field is preferred but not required.
- Industry recognized certifications such as CISSP, CISM, CCSP, CISA, CRISC, or GIAC are highly preferred.

Language Skills

- Ability to interact with all management and staff.
- Ability to write reports and business correspondence.
- Ability to effectively present information and respond to questions.
  Ability to communicate effectively (both written and verbally) with co-workers, customers and vendors.

Physical Demands

The physical demands and environmental factors described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Must be able to see and read fine print. Employee will have close visual contact with a computer monitor constantly.
- Must be able to communicate utilizing a telephone.
- Must have the mobility to allow access to all parts of the office.
- Must be willing and able to learn all the necessary computer functions.
- While performing the duties of this job, the employee is regularly required to use hands to finger, handle, or feel; reach with hands and arms; and talk or hear. The employee frequently is required to sit. The employee is occasionally required to stand and walk. The employee must occasionally lift and/or move up to 20 pounds. Specific vision abilities required by this job include close vision, distance vision, color vision, peripheral vision, depth perception, and ability to adjust focus.

Base Salary Range: $100,000-$120,000/year, actual compensation within the range will be dependent on experience, skillset, and ability to meet qualifications outlined in the above job description.

For more information on our culture and benefits, please visit our careers page:
https://www.onelocalbank.com/our-story/work-with-us