MIDCOUNTRY FINANCIAL CORP

Director of Information Security

JOB SUMMARY:
The Director of Information Security is responsible for developing, coordinating and implementing policies, standards, and procedures to safeguard MidCountry's information systems and data.

Position accountabilities include:

1. **Governance -** Responsible for developing, defining, and directing the information security program.

2. **Security Architecture -** Responsible for analysis, definition, and implementation of technology and policy architecture.

3. **Outreach and Awareness -** Responsible for championing awareness, influencing compliance with security policies, and providing solutions for business- specific security issues.

4. **Engineering -** Responsible for day-to-day security operations.

5. **Business Continuity -** Responsible for oversight of corporate BCP program

6. **Regulatory Compliance -** Serves as lead for information security regulatory compliance programs (SOX, GLBA, FFIIEC, etc.)

JOB RESPONSIBILITIES:
1. Establish information security policies and procedures consistent with business goals and regulatory requirements, such as set forth by the FFIEC, FTC, OCC, and relevant state regulators.
- Develop new and review current policies and standards.
- Review and approve (if applicable) exceptions to policy.
- Ensure training to team members on information security policy topics.
- Ensure regular audits and applicable assertions or certifications are obtained as to the compliance of MidCountry with relevant requirements and standards

2. Serve as Corporate Information Security Officer and oversee the implementation of processes to safeguard customer information.
- Maintain Information Security Program (GLBA)
- Report on effectiveness of the Information Security Program (GLBA)

3. Ensure that MidCountry Financial Corp. is compliant with all information security related requirements and meets contemporary applicable best practices.
- Keep up to date with the cyber security landscape

4. Provide technical leadership to the IT department and other relevant parties at MidCountry as it relates to information security, both internal and outside entity facing systems.
- Meet regularly with IT Leadership.
- Participate in IT Steering Committees.
- Create and lead as-hoc security teams and/or directly reporting technical security to administer and monitor computer and network equipment logs, intrusion prevention, anti-malware, and other data loss prevention systems.

5. Participate in oversight of the IT department, with an emphasis on information integrity and security. Perform IT Risk Assessments.
- Oversee Monitoring Program.

6. Be responsible for corporate Business Continuity Planning (BCP) Program.
- Provide oversight and coordination of planning and testing activities

7. Oversee threat management and security incident handling, including the coordination of investigations

and reporting of security incidents, in alignment with business needs and regulatory requirements.
- Develop and maintain Incident Response program.
- Coordinate, escalate and report incidents and trends.

JOB REQUIREMENTS:
Education:
Required: Bachelor's Degree in Related field

Certifications:
Experience (Number of Years and Focus):
Required: 4 - 6 years previous related work experience in banking, consumer finance or compliance

Knowledge/Skills/Abilities:
Comprehensive risk management and regulatory knowledge in the context of financial services; system development life cycle experience helpful; public company experience helpful; strong interpersonal skills working with internal and external customers; must have demonstrated people skills to listen, understand, influence, and coach staff; must be able to multi task, prioritize activities and meet deadlines while working in a fast paced environment; outstanding written and verbal communication skills; proven judgment ability, served by strong problem analysis as well as problem solving methods; proficient in interpreting complex regulatory provisions; extensive knowledge of consumer banking laws and regulations in the context of information security; ability to interact effectively with all levels of employees; detail oriented with strong analytical skills.