Chain Bridge Bank, N.A.

Job Title: Vice President, Deputy Director of Information Technology
Department: Information Technology
Job Location: McLean, VA
Reports to: SVP, Director of Technology

About Chain Bridge Bank, N.A.

Chain Bridge Bank, N.A., headquartered in McLean, Virginia, is a nationally chartered bank offering a comprehensive range of commercial and consumer banking services, including traditional deposit accounts, mortgages, and loans, as well as trust and wealth management services. The Bank integrates personal service with technology and strictly complies with financial and regulatory standards.

Compensation

The bank offers competitive pay, a comprehensive benefits package, and participation in the Chain Bridge Bank, N.A. Incentive Compensation Plan. Training and career development opportunities are also provided.

Position Overview

The Deputy Director of Information Technology will support the Director of Technology in overseeing the bank's IT infrastructure, cybersecurity, regulatory compliance, and digital transformation initiatives. This leadership role will ensure the security, reliability, and efficiency of the bank's technology operations while aligning IT strategies with business objectives. The position requires a strong background in financial sector cybersecurity frameworks, including FFIEC, NIST, and Zero Trust Architecture**,** as well as expertise in Microsoft Azure, cloud computing, and enterprise security**.**

This role plays a critical function in implementing and enforcing cybersecurity policies, regulatory compliance, incident response, and disaster recovery planning**.** The Deputy Director will also manage IT staff, oversee vendor relationships, and assist with key technology projects to enhance operational resilience.

Key Responsibilities

IT Infrastructure & Systems Management

- Assist in managing the bank's IT infrastructure, including Microsoft 365, Azure, AVD, and cloud environments.

- Oversee the administration of Windows Server, Active Directory (Entra ID), networking, VoIP, and endpoint security.
- Assist with the deployment and management of Microsoft Defender, Intune, BitLocker policies, and compliance automation.
- Ensure patch management and vulnerability remediation.
- Assist with maintaining technology asset management, including hardware lifecycles and software licensing.
- Oversee Azure infrastructure, cloud migrations, identity and access management, and cloud security best practices.

Cybersecurity & Compliance Oversight

- Enforce FFIEC/ NIST standard security controls, ensuring the bank's compliance with regulatory requirements.
- Support the implementation of Zero Trust security principles, identity management, and least privilege access.
- Oversee DLP strategies in Microsoft Purview to prevent data loss and unauthorized access.
- Conduct vulnerability assessments, penetration testing coordination, and risk remediation tracking.
- Respond to cyber incidents, SOC alerts, and regulatory audits, ensuring timely resolution.

IT Governance & Regulatory Compliance

- Assist with the development and enforcement of IT policies, disaster recovery (DR), and business continuity plans (BCP).
- Assist in vendor management and third-party risk assessments, ensuring compliance with FFIEC guidelines.
- Collaborate with internal teams to update the risk register, incident response plans, and AI governance policies.

IT Operations & Support

- Serve as Tier 2/3 escalation for complex IT issues related to security, cloud, and endpoint management.
- Use of Microsoft compliance tools and eDiscovery solutions to support audit and legal requirements.

Leadership & Training

- Assist in the management and mentoring of IT staff, providing training on cybersecurity awareness, compliance, and emerging threats.
- Act as a backup for the Director of Technology, assuming leadership responsibilities as needed.
- Attend and assist with tabletop exercises, cybersecurity drills, and BCP testing to ensure readiness.

Qualifications

Skills & Knowledge:

- Expertise in Microsoft 365, Azure, Windows Server, AVD, cloud security, and enterprise IT**.**
- Strong understanding of FFIEC, NIST, Zero Trust, and financial sector cybersecurity regulations**.**
- Experience with endpoint security, Microsoft Defender, and SIEM solutions.
- Familiarity with banking software, including Jack Henry (preferred but not required).
- Strong project management and leadership skills, with the ability to manage IT budgets and vendor contracts.

Education, Certifications & Experience:

- Minumum Education: Bachelor's Degree in Information Technology, Computer Science, or a related field.
- Academic honors such as Dean's List, summa cum laude, or membership in Beta Alpha Psi, Beta Gamma Sigma, or other honor societies.
- Minimum Experience: 5+ years of experience in IT systems administration, cybersecurity, or IT management
- Prior experience in banking or financial IT environments, with knowledge of banking software and security regulations

How to Apply

Please submit a resume, cover letter, and transcripts to HR@chainbridgebank.com. We encourage highly qualified candidates to apply and look forward to reviewing your application.

Additional Information

Complying with all applicable safety and soundness and consumer compliance laws and regulations, taking the annually required consumer compliance courses, and adhering to the policies and procedures that facilitate compliance will all be factors considered when evaluating individual performance. Individual performance is rewarded in annual salary adjustments.

Bank compliance with laws and regulations is a factor considered in the calculation of incentive compensation. The ratings that the Bank receives from its regulators and its auditors are factored into the annual incentive compensation calculation. Your adherence to these laws and regulations and the policies and procedures that support them directly affect the Bank's compliance. Annual incentive compensation rewards team performance. An employee will not be eligible for incentive compensation unless he/she takes the consumer compliance courses required of all employees and all the required consumer compliance courses for his/her job description or job responsibilities by the end of each calendar year. All required consumer compliance courses for the applicable year will be outlined in the Compliance Management Program made available to all employees.