**Job Title:** Information Security Engineer
**Department:** Enterprise Risk Management
**Location:** Pittsburgh, PA

**Summary of the Position:**

The Information Security Engineer is a hands-on role responsible for supporting the cybersecurity objectives of TriState Capital. The incumbent must be able to work independently, and be proactive in identifying issues, troubleshooting problems, and making decisions based on established policies and information security best practices. The Information Security Engineer will be responsible for advancing TriState Capital's cybersecurity posture.

**Primary Functions of the Position:**

- Performing all functions required to support network security operations, including security monitoring of essential infrastructure
- Managing logging, and other security devices
- Creating and reviewing reports on event anomalies
- Evaluating information security solutions, and providing recommendations on information security software, hardware, policies, and procedures for implementation
- Monitoring compliance with TriState Capital's policies, and coordinating investigation and reporting of security incidents; maintaining effective Incident Response Planning efforts
- Developing and ongoing preservation of key metrics and key risk indicators that can be shared in the various Risk Committees
- Participating in various Risk Committee meetings as deemed necessary

**Education and Experience Requirements:**

- Bachelor's Degree in Information Security, Computer Science, Information Technology, or technology-related degree preferred; industry-related security certifications a plus (e.g., Relevant GIAC certifications, CISSP)
- 4-6 years of experience in information security management, vulnerability management, security infrastructure, security planning, and incident response
- Demonstrated experience in cybersecurity combined with risk analysis, audit, and compliance objectives; Strong working knowledge of information security concepts
- Experience performing technical network analysis involving threat event data and evaluation of malicious activity
- Experience with vulnerability management and incident response
- Experience securing and monitoring Microsoft Windows operating systems and mobile devices
- Experience securing and monitoring Cisco networking infrastructure; including firewalls, routers and switches
- Experience securing and monitoring critical business applications
- Experience with Data Loss Prevention, Intrusion Prevention/Detection Systems, and SIEM systems
- Demonstrates excellent critical thinking and problem-solving abilities; superb written, verbal, and presentation skills
- Familiarity with auditing and security frameworks such as NIST, SOX, GLBA, and FFIEC
- Experience with managing cybersecurity risk assessments
- Experience in banking and/or financial services would be highly beneficial