Class Concept

The IT Security and Compliance Specialist I plans, coordinates, and implements security measures for information systems to regulate access to computer data files and prevent unauthorized modification, destruction, or disclosure of information. Work involves the design and implementation of network control mechanisms that serve to control users' access to computer networks through such processes as firewalls. Work also involves the implementation of application access control that keeps unauthorized users from accessing a particular computer or network or program. Work involves security scans on network systems, application systems and other computer equipment. This role is responsible for the tactical development and implementation of their agency's/university's risk management, business continuity planning and disaster recovery plans. Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks. Work may involve the testing, implementation, deployment, maintenance, review, or administration of infrastructure hardware and software that are required to effectively management the network and security resources. Monitors network to actively remediate unauthorized activities and responds to crises or urgent situations within the infrastructure to mitigate immediate and potential threats. Work also involves performing assessments of systems and networks within the network and identifying where those systems/networks deviate from acceptable configurations, agency policies, and/or state and federal regulations.

Recruitment Standards

Knowledge, Skills, and Abilities

- Basic knowledge in system technology security testing (vulnerability scanning and penetration testing) and proficient use of various tools and techniques, including risk, business impact, control and vulnerability assessments, used to identify business needs and determine control requirements.
- Basic knowledge of the implementation and maintenance of firewalls.
- Understand the basic tenets of security: confidentiality, integrity, and availability.
- Basic knowledge of network/systems controls, patching and migration of vulnerabilities.
- Working knowledge of IT controls available to enforce the tenets of authentication & authorization including principle of least privilege and password constructs and controls and can determine and provide users access/accounts with only privileges needed to complete their assigned tasks.
- Ability to recognize security incidents and report them to the appropriate security management personnel and assist the higher-level security officers with incident response by providing logs, removing the system from the network, and providing expertise on the specifics of the system.
- Ability to work with teams to prioritize security needs and to effectively get cooperation from IT professionals to get those security controls in place and possesses strong conflict management skills in order to work with senior management to ensure security and data protection rules and regulations are in place on protected private information.
- Ability to apply incident handling methodologies and recognizing, categorizing types of vulnerabilities and associated attacks
- Ability to provide timely detection, identification, and alerting of possible attacks. intrusions anomalous activities, and misuse activities

Minimum Education and Experience

Bachelor's degree in Computer Science or a related IT related field or closely related field from an appropriately accredited institution and one year experience in IT Security; or

Associate degree in Computer Science or a related IT related field or closely related field from an appropriately accredited institution and two years of experience in IT Security; or an equivalent combination of education and experience.

Note: This is a generalized representation of positions in this class and is not intended to identify essential functions per ADA.