IT Security & Compliance Specialist II

Class Concept

The IT Security and Compliance Specialist II recognizes and identifies potential areas where existing data security policies and procedures require change, or where new ones need to be developed, especially regarding future business expansion. Provides management with risk assessments and security briefings to advise them of critical issues that may affect customer, or enterprise security objectives. Evaluates and recommends security products, services and/or procedures to enhance productivity and effectiveness. These positions are responsible for the strategic 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. 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 state and federal regulations. This level is distinguished from level I by the responsibility for the integrity of and access to enterprise systems, files, and data elements.

Recruitment Standards

Knowledge, Skills, and Abilities

- Thorough technical knowledge of mainstream operating systems and a wide range of security technologies, such as network security appliances, identity and access management systems, cryptography, anti-malware solutions, automated policy compliance and desktop security tools.
- Working knowledge in developing, documenting, and maintaining security policies, processes, procedures and standards, strategic planning, implementation, and maintenance of information security programs.
- Detailed understanding of technical, substantive, and methodological issues and theories to direct technical staff.
- Ability to provide technical leadership on complex projects.
- Ability to integrate knowledge of other work specialties to achieve solutions to problems of high complexity.
- Ability to recommend information technology security and privacy solutions to address complex and emerging information security and privacy issues.
- Ability to plan, implement and maintain strategic information security program inclusive of information security policies, regulations, standards, and procedures.
- Proficiency in forensic response and reverse engineering and insightfulness to discover the latest exploit methodologies.
- Ability to provide information security solutions to reduce information security and privacy risks and to provide security best practice recommendations as required by federal and state regulatory requirements.
- Working knowledge of the IT security industry and federal and state regulations that have an impact on the state's technological business.
- Ability to provide security expertise and consulting to committees, boards, and lower-level technical analyst/specialist on a regular basis and to design information security awareness training programs.
- 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
- Ability to provide guidance to legal, risk management, audit, compliance, and external entities on the resolution of information security issues.
- Ability to provide resource assistance in the implementation of security best practices for business continuity planning, risk management and disaster planning to senior level management and IT

specialists to assist agency/university's development and maintenance of appropriate business continuity, risk management and disaster plans.

Minimum Education and Experience

Bachelor's degree in computer science or a related IT field or related degree from an appropriately accredited institution and two years of progressive experience in IT Security or closely related area; or

Associate degree in computer science or a related IT field or related degree from an appropriately accredited institution and three years of progressive experience in IT Security or closely related area; 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.