IT Security Specialist

DESCRIPTION OF WORK: Positions in this banded class plan, coordinate, and implement security measures to protect information and information processing assets. They design and implement network control mechanisms to control access to computer networks; manage vulnerabilities within the information processing infrastructure; manage threats and incidents impacting information resources; assure through policy the appropriate use of information resources; and educate users on their information security and privacy responsibilities. They also implement application access controls such as password authentication that grant access to only unauthorized users. They employ the appropriate intrusion detection and prevention tools and procedures to detect and prevent against hackers, worms and other malware. They may be responsible for planning, developing, and managing the physical and environmental security required to address the threats, vulnerabilities, and counter measures required to protect information assets and the premises in which they reside. Employees are responsible for the strategic and tactical development and implementation of their IT risk management, business continuity planning and disaster recovery plans and with the collaboration of the agency's/university's departments in implementation of departmental plans. Employees may be responsible for developing information security policies, standards, best practices and ensuring that state and federal information security requirements are implemented.

ROLE DESCRIPTIONS BY COMPETENCY LEVEL

Contributing: Positions at this level scan networks and systems for their level of vulnerability to threats. They also are involved in identifying any emerging vulnerabilities of the system. They will produce reports for management to identify potential risks. Positions may meet with systems administrators to identify security patches available to minimize vulnerabilities and risks. Positions at this level may serve as identify management/password authentication administrators to control users access to systems. They monitor reports of computer viruses to determine when to update virus protection systems. Positions communicate procedures and one-time passwords to users of the systems. This usually entails keeping up-to-date lists of users as well as helping employees who have forgotten passwords or accidentally violated security procedures. Positions may serve as disaster recovery analysts who advise on the development, documentation and maintenance of disaster recovery plans. They may work on information security training and awareness campaigns. Evaluate new threats and communicate them to agency or institution. They may review risk assessments and support cyber incident response.

Journey: Positions at this level may design, develop, and maintain security regulations, procedures and department-wide rules for moderately complex agencies or universities. They analyze information obtained from intrusion detection and prevention systems and work with advanced security protocols and standards including recommended blocks to apply. They will evaluate and develop approaches to security solutions. Positions proactively assess potential items of risk and opportunities of vulnerabilities in the network. They may research and help develop security practices. They analyze traffic trends and systems logs and propose security policy changes. Positions may also serve as disaster recovery analysts who establish disaster recovery programs and business continuity planning across multiple platforms. They may create Requests For Proposal (RFP) and help evaluate responses of RFP for information security projects. Review new projects, systems and applications for compliance to statewide or institution policies. Create and maintain the agency or institution's security training and awareness effort. Create and conduct risk, system and application assessments. Create and maintain cyber security incident response plan.

Advanced: Positions at this level establish security enterprise regulations and procedures based on federal and state laws and mandates. They design and manage security systems and architectures for possible enterprise-wide implementation (state-wide or large complex universities/agencies) that protect federally mandated information such as tax records, health information, research data, state security records or student educational records. They design security systems for organizations with complex network systems, major databases, emerging technologies, or systems with known vulnerabilities. Positions may be responsible for establishing and maintaining an enterprise-wide information risk management program to ensure that information assets are adequately protected. They will act as an advisor to the enterprise's business units and should have an understanding of the latest security threats, trends, technologies, and regulatory requirements. Some positions at this level may serve as forensic experts to recover information from computers and data storage devices. They often work alongside law enforcement officers helping to solve cybercrimes or find electronic evidence of other kinds of crime using forensic tools and investigative methods to find specific electronic data, including Internet use history, word processing documents, images and other files. They also transfer the evidence into a format that can be used for legal purposes (i.e. criminal trials) and often testify in court themselves. Serve as cyber incident response leader.

EXAMPLES OF COMPETENCIES:

CONTRIBUTING:
Technical Knowledge - Knowledge in system technology security testing (vulnerability scanning and penetration testing).
Technical Solution Development - Understand the IT controls available to enforce the CIA tenets of authentication & authorization.
Technical Support - Ability to recognize security incidents and report them to the appropriate security management.
Consulting/Advising – Ability to work with teams to prioritize security needs and to effectively get cooperation from IT professionals to get those security controls in place.
Professional Knowledge - Hold and maintain basic security certifications, such as Security + (where applicable) or National Security Agency – Information Assessment Methodologies (NSA-IAM)

JOURNEY
Technical Knowledge - Thorough understanding of the basic tenets (CIA) of security in complex environments: Confidentiality – protecting data from unauthorized access; Integrity – ensuring the data is as it was or should be (i.e. unchanged); and Availability – ensuring systems, data and networks are up and redundant where needed (i.e. backups).
Technical Solution Development - Ability to understand the available methodologies of authentication and authorization and which is appropriate in particular settings.
Technical Support - Ability to serve as a technical resource in solving security problems of high complexity.
Consulting/Advising – Knowledge of the security industry and regulations that have an impact on the customer's business and data protection issues and the ability to provide appropriate solution set to address the business needs.
Professional Knowledge - Hold and maintain more complex certifications such as SANS Global Information Assurance Certifications (Or Similar – ex. Carnegie-Mellon CERT); Security Essentials Certification (GSEC); Information System Security Certification Consortium (ISC)2; or Systems Security Certified Practitioner (SSCP).

ADVANCED

Technical Knowledge - Excellent technical knowledge of mainstream operating systems (for example, Microsoft Windows and AIX UNIX) 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.
Technical Solution Development - Ability to provide technical leadership on complex projects.
Technical Support - Proficiency in forensic response and reverse engineering.
Consulting/Advising – Knowledge of the IT security market and industry and federal and state regulations that have an impact on the state's technological business.

Professional Knowledge - Hold and maintain the most complex and difficult certifications available in IT security such as:

- Specialized SANS Global Information Assurance Certifications based on field of work (Certified Incident Handler, Certified Intrusion Analyst, Penetration Tester/Web Application Penetration Tester, and Certified Forensic Analyst/Examiner))
- Information System Security Certification Consortium (ISC)2 (Certified Information Systems Security Professional (CISSP))
- Vendor and Government Certifications (Seized Computer Evidence Recovery Specialist (Federal Law Enforcement Training Center), EnCase Certified Examiner Certification (EnCE), AccessData Certified Examiner (ACE), and Certified Ethical Hacker (CEH))
- Certified Information Security Manager (CISM)

MINIMUM TRAINING AND EXPERIENCE: Bachelor's degree in Computer Science, Computer Engineering or an Information Security degree or closely related field from an appropriately accredited institution; or Bachelor's degree from an appropriately accredited institution and one year of experience in IT Security or closely related area; or an Associate's degree in Information Systems Security from an appropriately accredited institution and two years of experience in IT Security or closely related area; or an equivalent combination of education and experience.

Special Note: This is a generalized representation of positions in this class and is not intended to reflect essential functions per ADA. Examples of competencies are typical of the majority of positions, but may not be applicable to all positions.