Alameda Contra Costa Transit District
Classification Specification

Exhibit-D

Senior Network Security Engineer - DRAFT

Class Code	FLSA Status	EEO-CAT	Rep Status	Salary Grade	Effective Date	Resolution #
TBD	Exempt	Computer Technician	AFSCME	10	10/13/2021	21-036

DEFINITION: Under general direction, performs Innovation and Technology (IT) security functions associated with designing and maintaining a secure and reliable network infrastructure. Works independently to identify and remediate potential threats and maintain security of internal and external networks; and in a team environment to accomplish larger department goals. This is the advanced, lead-level within the classification series. There are two (2) levels within the Network Security Engineer series that are distinguished from one another by the technical complexity of the assigned duties and the level of discretion and independent judgment exercised. Positions at this level are responsible for performing activities for highly complex systems projects.

This classification is distinguished from the Network Security Engineer in that the senior-level provides technical and functional direction to District and contract staff and participates in the more difficult and complex assignments. Incumbents at the senior level are expected to operate with a significant degree of independence and possess extensive knowledge of the District's enterprise systems and software products, and security systems and protocols.

REPRESENTATIVE FUNCTIONS may include, but are not limited to the following:

- Plans, organizes, and directs the daily functions, operations, and activities of the Network Security Engineering work unit responsible for a wide range of enterprise systems and software projects.
- Analyzes and monitors network traffic to provide early intrusion detection and prevention, and rapid reaction to unexpected and suspicious situations such as unusual traffic volume, port attacks, and rogue devices in the network.
- Performs operational processes related to satisfying regulatory requirements, including requirements of the Payment Card Industry's Data Security Standards (PCI-DSS); and refines security awareness programs and communications and security policy and procedure documents required for compliance.
- Performs regular internal and external IT security assessments and network penetration testing, reporting, and issue resolution to ensure the security of traffic that passes through the network, and that robust security is built into the design and implementation of all networks, servers, and storage.
- Performs routine audits of hardware and software entities on the network in order to find and address security vulnerabilities.
- Documents computer and network security and emergency measures; and tests and monitors compliance with information security procedures and policies.
- Serves as the District's network security resource to IT project team members, and consults on security issues with other District departments.
- Provides consultation and reviews on project designs with infrastructure components, and ensures compliance prior to moving designs into production.
- Performs operational processes related to satisfying regulatory compliance requirements.
- Develops, maintains and refines security awareness program communications and security policy and procedure documents required for regulatory compliance.
- Provides infrastructure design solutions that conform to the security standards and requirements of the District, as well as IT best practices, as applicable.
- Configures and troubleshoots software and hardware issues.
- Performs detailed analyses of web server security.
- Maintains up-to-date knowledge of available and emerging technologies as they relate to networks, network security, and information systems.
- Performs related duties as required.

MINIMUM QUALIFICATIONS

Senior Network Security Engineer

Knowledge of: Principles and practices of computer networks in virtualized client-server, and operating environments consistent with current technologies; PCI-DSS controls, and procedures for maintaining compliance; security analysis tools and techniques, including Nessus, Webinspect, Paros, Fiddler, sql injection, MiTM and OWASP; Cisco security products including ASA firewalls, routers, switches, IDS/IDP sensors, and wireless LAN controllers; Active Directory authentication including Radius, TACACS, and Kerberos; change control concepts in a highly regulated environment; VMware and Windows hardening, as well as client OS hardening; large or complex Firewall and IDP/IPS environments; IPSEC and IKE security protocols; Windows security tools and products including PKI and ISA; security concepts including Netlogon logging, and Group Policy; third party security tools including Microsoft Anti-Virus and web filter proxies including Websense; security websites and vulnerability disclosure reports from Mitre, SANS, Security Focus, Microsoft and Cisco; and virus breakout mitigation and prevention.

Ability to: Monitor multiple computer networks on an ongoing basis; use forensic investigation tools and techniques, as well as chain of custody; identify, contain, and mitigate virus intrusions; develop strategic technical documentation and written communications relative to field of expertise, including Security Policies, standards documents, and procedural documents; implement changes in a large network environment; maintain strong analytical skills commensurate with changing IT technology and security requirements; organize and plan work effectively, and perform duties quickly and accurately in emergency situations, and under firm deadlines; work both independently, and collaboratively in a team environment, and lead teams when required; communicate effectively in English, both orally and in writing with District staff at all levels; develop and deliver effective presentations to various District departments; plan, organize, and coordinate the work of staff; provide leadership and work direction to team members; train staff in work procedures; establish and maintain effective working relations with District personnel using principles of excellent customer service.

Education: A Bachelor's degree in computer science, management information systems or related field. Additional experience beyond the minimum may be considered in lieu of the required education on a year-for-year basis.

Experience: Eight (8) years of recent and verifiable experience in Information Technology, including two (2) years in security infrastructure or or three (3) years of experience at a level equivalent to the District's Network Secutiry Engineer classification.

License and Certification(s): None.

Physical Requirements: (1) Must maintain the physical condition necessary to perform tasks in an office setting and operate computers, keyboards, and other peripheral equipment; and (2) lift up to fifty (50) lbs. (3) must possess the mobility necessary to travel expeditiously within a large office building and to other District facilities.

Special Environmental Conditions:

Established Date: (Res. #)