NETWORK SECURITY ENGINEER

DEFINITION

Under general direction, plans, manages and oversees network security controls and programs for the District; leads the effort in gathering, analyzing, synthesizing, planning, and integrating new or updating existing security solutions; and performs related work as required.

SUPERVISION RECEIVED AND EXERCISED

Receives direction from the Computer Network Supervisor. May exercise technical and functional direction over lower-level staff.

CLASS CHARACTERISTICS

Responsibilities include performing diverse, specialized, and complex work involving significant accountability and decision-making responsibility. The incumbent manages day-to-day network systems security programs, resolves complex security problems and breaches, and complex network security projects and/or functions to meet current and anticipated future requirements. Successful performance of the work requires an extensive professional background as well as skill in coordinating work with that of other District units, divisions, and departments, and external agencies.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

- Evaluates, recommends, installs, configures, supports, programs, and maintains network security systems and solutions for the District; monitors equipment functions and usability, reviews performance utilization, maintains systems to maximize availability and accessibility; modifies firewall, router, and network monitoring system configurations to enable new servers or applications.
- Evaluates the effectiveness and performance of the District's security portfolio hardware and best practices; researches and recommends changes to products or services as well as new architecture of security systems for maximum technical advantage.
- Uses metrics to monitor and report on the effectiveness of security controls and compliance with security policies; ensures new additions and changes to District technology do not affect the integrity of network security.
- Ensures that noncompliance issues and other variances are resolved in a timely manner.
- Investigates security breaches and threats and recommends changes to address security issues.
- Conducts security scans, audits, and risk assessments; monitors intrusion detection and prevention devices; install and maintain security configurations for server, database, and application systems; evaluates resource needs.
- Assists in the physical installation of network security devices and appliances.
- Stays abreast of new trends, laws, regulations, and innovations in the related field of information services specifically system security; evaluates new and emerging technology to apply to security solutions in the context of institutional needs; attends training on security practices and products; participate in professional meetings as required.

- Resolves the most complex security problems and network data breaches; maintains, troubleshoots, and diagnoses security equipment and software configurations; modifies and verifies internal access control lists.
- Acts as technical lead for security vendors and law enforcement agencies; serves as a liaison to other District units, divisions, departments, and outside vendors; negotiates and resolves product and security issues.
- Researches, recommends, and implements solutions for inter/intra operability of security systems, network devices, and applications.
- Programs and administers equipment infrastructure and Internet and Intranet security devices; coordinates the design of equipment components.
- Develops and prepares written documentation for network security design, standards, and processes; maintain a database of services provided.
- Assists in the development of disaster prevention and recovery plans.
- Assumes project leadership roles and responsibilities in the completion of network security, network, and telecommunications related systems projects.
- Assists with the development of bid specifications for acquisitions of network and data security and network and telecommunications equipment and services.
- Performs related duties and responsibilities as required.

QUALIFICATIONS

Knowledge of:

- Principles and practices of security issues and practices related to physical security, network infrastructure, servers, and computer systems.
- Principles and procedures for use of complex network hardware, protocols and configurations such as Transmission Control Protocol/Internet Protocol (TCP/IP), Local Area Network (LAN), Wide Area Network (WAN), wireless, and operating systems as they relate to switched and non-switched telecommunications networks.
- Firewalls, intrusion detection and prevention systems, auditing and scanning systems, virtual private networks (VPN), and remote access systems.
- Principles of database structure management and computer programming.
- Common security controls and frameworks including Process Control Instrumentation (PCI).
- Hardware and software security controls including access control, software development security, business continuity and disaster recovery planning, cryptography, Information Security Governance and risk management, legal regulations investigations and compliance, security operations, some physical (environmental) security, security architecture and design, telecommunications, and network security.
- Operation of enterprise security hardware and software including anti-virus/malware, internet use reporting, access rights monitoring/reporting, encryption, and e-discovery tools.
- Applicable information security laws and regulations such as: Federal Education Rights Privacy Act (FERPA), Communications Assistance to Law Enforcement Act (CALEA), Computer Fraud and Abuse Act, Health Information Portability and Accountability Act (HIPPA), and California Data Security Breach Law (SB24).
- Internet Protocol addressing and routing such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Interior Gateway Routing Protocol (IGRP).
- Encryption Public Key Infrastructure (PKI).
- Payment Card Industry Data Security Standard (PCI-DSS) compliance requirements.

- Operating systems including but not limited to Microsoft Windows server and client, and one of the following: UNIX, Linux, or Solaris.
- Security concerns relevant to email and calendaring systems, including Microsoft Office software applications and cloud-based Software as a Service (SaaS) solutions.
- Recent and on-going information services related developments including information technology, current literature, and sources of information related to the operations of assigned functional area.
- Recordkeeping principles and procedures.
- English usage, grammar, spelling, vocabulary, and punctuation.
- Techniques for providing a high level of customer service by effectively dealing with the public, students, and District staff, including individuals of diverse academic, socio-economic, ethnic, religious, and cultural backgrounds, disability, and sexual orientation.

Ability to:

- Demonstrate understanding of, sensitivity to, and respect for the diverse academic, socio-economic, ethnic, religious, and cultural backgrounds, disability, and sexual orientation of community college students, faculty and staff.
- Apply independent technical judgment to complex technical situations.
- Coordinate schedules and resources with systems and network programmers, engineers, users, technical services staff, risk management, and District police department.
- Design, develop and implement security solutions for large networks.
- Apply extensive application of knowledge in integrating security protocols to complex solutions and understanding relationships between applications.
- Interpret, apply, explain, and ensure compliance with applicable information security regulations, technical written material, and District information services policies and procedures.
- Diagnose and quickly respond to and resolve security breaches and understand reasons for systems failures.
- Maintain current knowledge of technological advances in the field.
- Use English effectively to communicate in person, over the telephone, and in writing.
- Organize and prioritize a variety of projects and multiple tasks in an effective and timely manner; organize own work, set priorities, and meet critical time deadlines.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.
- Use tact, initiative, prudence, and independent judgment within general policy, procedural, and legal guidelines.
- Maintain records and prepare reports to summarize and present administrative and technical information and data in an effective manner.

Education and Experience:
Any combination of training and experience that would provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the required qualifications would be:

Equivalent to graduation from an accredited four-year college or university with major coursework in management information systems, computer science, business or public administration, or a related field and three years of experience managing network security devices.

Licenses and Certifications:

- Possession of, or ability to obtain, a valid California Driver's License by time of appointment.
- Possession of, or ability to attain, a Certified Information Systems Security Professional (CISSP) or equivalent certification.

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer, and to operate a motor vehicle to visit various District and meeting sites; vision to read printed materials and a computer screen; and hearing and speech to communicate in person, before groups, and over the telephone. This is a sedentary office classification although standing and walking between work areas may be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to occasionally lift, carry, push, and pull materials and objects up to 50 pounds with the use of proper equipment.

ENVIRONMENTAL ELEMENTS

Employees work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances.

Salary Grade: C1-73
FLSA: Non-Exempt
EEO Code: H-50
Board Approved: April 2021