# NETWORK SECURITY ENGINEER

SALARY GRADE: C1-73

DEFINITION:

Under the direction of an assigned supervisor, serve as a project leader. The position is responsible for applying advanced skill and knowledge of complex network and systems security solutions and of multiple operating systems in gathering, analyzing, synthesizing, planning and designing unique and original solutions for integrating new or updating existing security solutions.

DISTINGUISHING CHARACTERISTICS:

The Network Security Engineer resolves the most complex security problems and breaches. Acts as technical liaison for security vendors. Installs, supports, maintains, and programs security solutions for the District. Researches and performs analysis to identify system expansions to meet anticipated future requirements. Evaluates complex security performance analysis and recommends appropriate action. Conducts and initiates security scans, audits and performs risk assessment.

EXAMPLE OF DUTIES AND RESPONSIBILITIES:

Depending upon assignment, duties may include, but are not limited to, the following:

1. Regularly evaluate new and emerging technology and apply to innovative security solutions in the context of institutional needs.
2. Resolve the most complex security problems and network data breaches; maintain, troubleshoot and diagnose security equipment and software configurations.
3. Evaluate the performance of complex security implementations and recommend appropriate action to improve speed and functionality to supervisor.
4. Act as technical lead for security vendors and law enforcement agencies as required.
5. Install, configure, support, program and maintain network security systems and solutions for the District as assigned; monitor equipment functions and usability, review performance utilization, maintain systems to maximize availability and accessibility.
6. Research and perform analysis to identify security systems expansions to meet anticipated future requirements.
7. Install, configure and maintain network security monitoring hardware and software.
8. Install, configure and maintain network equipment and software as it relates to security.
9. Develop original solutions for inter/intra operability of security systems, network devices and applications.
10. Communicate with outside organizations regarding equipment maintenance, materials and product capabilities.
11. Research and recommend new architecture of security systems for maximum technical advantage.
12. Develop, design, program and administer equipment infrastructure and Internet and Intranet security devices; coordinate the design of equipment components.
13. Prepare written documentation for network security design and processes; maintain a database of services provided.

14. Conduct security scans, audits and risk assessments. Conduct proactive security monitoring.

15. Assist in the development of disaster prevention and recovery plans.

16. Design, inventory, install, program, test and repair equipment hardware and systems associated with network and data security, including but not limited to firewalls, intrusion detection systems, and traffic analyzer.

17. Assume project leadership roles and responsibilities in the completion of network security, network and telecommunications related systems projects.

18. Assist with the development of bid specifications for acquisitions of network and data security and network and telecommunications equipment and services.

19. Assist in the development of policies and procedures to ensure ongoing continuity. Develop and document security standards.

20. Perform related duties as assigned.

EMPLOYMENT STANDARDS:

Knowledge of:

1. Advanced knowledge of security for networks and systems.
2. Working knowledge and use of complex network hardware, protocols and configurations, TCP/IP, LAN, WAN, Wireless, and operating systems as they relate to switched and non-switched telecommunications networks.
3. Knowledge of computer hardware systems, software applications and languages utilized by the District.
4. Knowledge of the principles, practices and techniques of database structures and computer programming.
5. Working knowledge of firewalls, intrusion detection and prevention systems, auditing and scanning systems, VPN, and remote access systems.
6. Working knowledge of operating systems including but not limited to Microsoft Windows server and client, and one of the following: UNIX, Linux or Solaris.
7. Working knowledge of email and calendaring systems, Microsoft Office software applications as related to security concerns.
8. Familiarity with information security regulations such as FERPA, HIPPA, SOX, and CALEA.
9. Familiarity with credit card PCI compliance requirements.
10. Familiarity with security practices including but not limited to physical security, network infrastructure, and servers.
11. Technical aspects of field of specialty and working knowledge of related specialties.
12. Record-keeping techniques.
13. Oral and written communication skills.
14. Interpersonal skills using tact, patience and courtesy.

Ability to:

1. 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.
2. Apply independent technical judgment to complex technical situations.
3. Coordinate schedules and resources with systems and network programmers, engineers, users, technical services staff, risk management and District police department.
4. Design, develop and implement security solutions for large networks.
5. Apply extensive application of knowledge in integrating security protocols to complex solutions and understanding relationships between applications.
6. Demonstrate working knowledge of the principles, practices and techniques of database structures and computer programming.
7. Operate computers and peripheral equipment properly and efficiently.
8. Diagnose and quickly respond to and resolve security breaches and understand reasons for systems failures.

9. Maintain current knowledge of technological advances in the field.
10. Communicate effectively both orally and in writing.
11. Maintain records and prepare reports.
12. Prioritize and schedule work.
13. Analyze situations accurately and adopt an effective course of action.
14. Work independently with little direction and provide work directions to others.
15. Establish and maintain cooperative and effective working relationships with others. Effectively use interpersonal skills with tact, patience and courtesy.
16. Place network security devices and secure these devices into racks and cabinets.

## Education and Experience

Any combination equivalent to:

1. Bachelor's degree in computer science or a related field.
2. Five (5) years of experience in security, network design development and support, computer systems, and computer programming responsibilities

## License or Certification

1. Possession of a valid class C California driver's license.
2. CISSP or equivalent certification.

## WORKING CONDITIONS:

### Environment:

1. Office environment.
2. May include travel to conduct work.
3. Accessing communications closets and data centers.

### Physical Abilities:

1. Hearing and speaking to exchange information in person and/or on the telephone.
2. Dexterity of hands and fingers to operate a computer keyboard and test equipment.
3. Sight to view computer monitor and read various materials.
4. Regularly stand, walk, and sit for extended periods of time.
5. Ability to walk, climb ladders, stoop, kneel, crouch, reach, push, pull, grasp, and perform repetitive motions.
6. Lift moderate to heavy objects up to 60 lbs.

### Hazards:

1. Extended viewing of computer monitor.

Date Approved: August 2011
EEO Code: H-50