KERN COUNTY SUPERINTENDENT OF SCHOOLS
NEW/APPROVED JANUARY 2018
TECHNICAL/SPECIALIST SERIES
RANGE: 57.5
CLASSIFIED
CODE: NONE

NETWORK SYSTEMS ENGINEER III
SECURITY SPECIALIST

DEFINITION

Under the general direction of the Executive Director of Technology, the Network Systems Engineer III – Security Specialist is responsible for undertaking broad and complex assignments in support of highly complex, multi-platform network systems and developing and implementing procedures, policies, strategies and standards in the management of the IT Security program.

EXAMPLES OF DUTIES

The Network Systems Engineer III – Security Specialist may be responsible for any or all of the following activities of similarly related jobs:

responsible for Unix systems installations and operations;

assist with the development and implementation of business continuity and disaster recovery plans;

assist in supporting the maintenance and functionality of all servers;

assist in the implementation and deployment of specific applications;

design and installation of Microsoft Windows Server systems for specialized applications and systems;

install and deploy software such as Microsoft Windows Server 20xx, Microsoft SQL Server 20xx;

maintain system and user accounts as required by software vendors;

prepare a variety of technical reports and correspondence;

maintain comprehensive documentation of all systems in operation;

perform related duties as required;

work with business unites to facilitate IT risk and management process, this includes identifying location, type, sensitivity, ownership and access requirements for data being used by KCSOS;

monitor the external threat environment for emerging threats and advise on appropriate course of action;

research, identify, coordinate, and play key role in the implementation of appropriate IT security systems, technology and controls including firewalls, intrusion detection/prevention and vulnerability scanners;

develop, implement and manage KCSOS wide IT security incident response processes and procedures;

develop, implement, maintain, disseminate and oversee enforcement of IT security related policies and procedures;

develop and implement strategies for complying with applicable Federal, State and other legal compliance requirements related to IT security;

develop, implement and manage a KCSOS wide IT security awareness and training program.

QUALIFICATIONS

Knowledge of:

Network technology in local-area networks;

must possess knowledge of and willingness to stay abreast of trends, innovations and practices in both microcomputer and networking technology, including hardware and software;

understanding of effective IT security system and network architectures, concepts, techniques and tools;

understanding and experience managing network and system security components such as firewalls and intrusion detection/prevention systems;

knowledge of and exposure in developing and testing business continuity and disaster recovery plans.

Ability to:

Prepare and present network administration training sessions to lay and professional audiences;

inspect, troubleshoot, diagnose, and resolve a variety of software, hardware, and application problems;

design, construct, install, and deploy secure Microsoft-based application server systems using protocols and applications described above;

read, interpret, and develop technical diagrams and equipment specifications; perform mathematical calculations accurately;

communicate effectively in both oral and written forms;

establish and maintain accurate records and files to include preventative maintenance schedules;

ability to identify, analyze, prioritize and communicate impact of IT security risks and exposures;

experience in organizing, prioritizing, developing, implementing, and communicating status on IT security strategies and projects;

proficiency in IT security management, industry best practices and standards;

experience in and knowledge of IT security auditing and monitoring;

exposure to the operation of institution wide networks, systems and applications;

ability to follow-up and follow-through in a coordinating role across multiple constituencies to achieve tactical and strategic goals;

agility in adapting to and thriving in a dynamic work environment including shifting of project objectives, deadlines, resources and priorities;

self-directed/driven.

Experience:
A minimum of five (5) years experience in Windows-based server administration, including Windows network protocol configuration, Active Directory Services, user administration and system configuration;

a minimum of three (3) years experience with other Microsoft application software, such as IIS, and Microsoft SQL Server 2000 and above; SQL experience to include database creation, maintenance, optimization, backup, security configuration, and user administration;

a minimum of five (5) years Network Security experience desirable;

a minimum of two (2) years experience in development of security best practices desirable;

and a minimum of two (2) years experience in the design, installation, repair, and maintenance of server hardware systems, with emphasis on HP-based server systems desirable.

Education:
The Network Systems Engineer III – Security Specialist must be a graduate of a four-year college or university, with a bachelor's degree in business administration or computer science highly desirable;

an equivalent experience in an applied setting regarding the above technology can be substituted for the college degree.

Conditions of employment:
Must maintain proof of privately owned automobile insurance and possess a valid California Motor Vehicle operator's license.

Fingerprint clearance by both the Federal Bureau of Investigation and the California Department of Justice is a condition of appointment after all other required job conditions have been met.

Must present verification of completion of Child Abuse Mandated Reporter training or obtain verification within six (6) weeks of hire and annually thereafter, as required by the California Child Abuse and Neglect Reporting Act.

This position has a probationary period of six months or 130 days, whichever is longer.

TS: gs
1/9/18
G:\Network Systems Engineer III – Security Specialist.doc