DATA COMMUNICATIONS SECURITY SPECIALIST

DEFINITION

Under general supervision of the assigned manager/supervisor, designs, implements and administers data security mechanisms for enterprise-wide, local and wide-area networks. Oversees the coordination of network security issues districtwide; provides technical advice to district and campus staff on complex issues involving network design, data security design, configuration, performance, and operation of secure networks and other related work as required.

TYPICAL DUTIES

Designs, implements, and administers the security components of complex enterprise-wide, local and wide-area network management systems, including Virtual Local Area Networks (VLAN), Wireless Local Area Networks (WLANs), and Virtual Private Networks (VPNs). Provides technical leadership, direction and assistance to district information technology staff on complex issues involving data systems security. Leads in the development of and advises management on issues regarding data systems security. Evaluates, designs, installs, customizes, optimizes, and monitors network routers, firewalls, intrusion detection systems, and other data security systems. Analyzes and monitors network data security systems to assure a balance of user access and data security concerns. Maintains device patching methodologies consistent with accepted standards and procedures. Plans, tests, and implements upgrades to data security software and hardware; performs upgrades and installations through the use of coordinated change management methodologies and procedures. Uses diagnostic equipment and extensive network monitoring programs to detect malicious activity and to research possible violations of policies. Analyzes specifications and design criteria for data security programs and devices and makes recommendations for new or revised data security architectures, applications, and equipment. Remains cognizant of evolving state and federal laws and mandates regarding the protection of critical personal data and privacy. Maintains working knowledge of current industry information, vendor direction, new products and technical architectures/approaches related to needs. Writes specifications for acquisition of new data security hardware and software. Analyzes, recommends and maintains accurate records of network security hardware, software and configurations. Manages and maintains all security scans and penetration tests, including remediation support and follow-up. Installs and uses systems management software to monitor data security systems at multiple sites. Participates in periodic disaster recovery tests involving network hardware and software. Maintains a daily log of activities related to data security hardware and software problems, temporary circumventions and reconfigurations. Manages and maintains primary districtwide DNS (domain name system). Advises and trains staff on approaches for ensuring the security of District networks, systems and data. Performs related duties as assigned.

QUALIFICATIONS

EXPERIENCE/EDUCATION

A Bachelor's degree with a major in computer sciences, management information systems, engineering or a closely related field AND four years of experience directly related to the job duties; OR, a Bachelor's degree and six years of experience directly related to the job duties; OR, an Associate's degree in computer sciences or closely related field and eight years of experience directly related to the job duties.

KNOWLEDGE OF

Knowledge of principles of enterprise-wide, local and wide-area network data security design, implementation, and administration. Knowledge of principles of design, development, implementation, storage, and operation of data (both local and wide-area), and video and voice telecommunications systems. Knowledge of characteristics, capabilities, and uses of network system components, including switches, firewalls, intrusion protection equipment, bandwidth shapers, web servers, routers. Knowledge of computer networks; including but not limited to, ETHERNET, 10 Base-T, LAN, WAN,

and voice over IP systems. Knowledge of communications network, architectures, and communications hardware; network security and access control such as Intrusion Protection Systems (IPS), firewalls, and Virtual Private Network (VPN) appliances; firewall solutions; components, capabilities and uses of servers and other computer equipment; operation and application of a wide variety of network and server software; troubleshooting methods and equipment used in the detection of malfunctions and the maintenance of optimum operating efficiency of data security systems; principles of recordkeeping; and principles of training. Knowledge of technical problem solving; methods of long-term strategic technical planning; and current industry information, vendor direction, new products and new technical architectures.

SKILLS IN

Skill in generating a number of different approaches to problems, determining the long-term outcomes of a change in operations; reorganizing information to get a better approach to problems or tasks; and evaluating the likely success of an idea in relation to the demands of the situation. Skill in understanding written sentences and paragraphs in work related documents; communicating effectively with others orally and in writing as indicated by the needs of the audience; finding ways to structure or classify multiple pieces of information; and listening to what other people are saying and asking questions as appropriate.

ABILITY TO (ESSENTIAL FUNCTIONS)

The ability to perform the functions of the position; sustain regular work attendance; work a flexible schedule as needed to perform specific jobs and/or assignments; work cooperatively and effectively with faculty, students, staff, peers, and management; exercise initiative and mature judgment; work as a member of a team; and develop and meet schedules and time lines. The ability to plan, organize, prioritize, and direct the workload of assigned areas of responsibility and work independently with minimum supervision; provide team leadership and direction; understand and explain complex procedures and instructions; and learn and adapt to new technologies, procedures and policies. The ability to design and implement complex network data security systems such as firewalls, routers, intrusion protection systems, and network access control; and monitor network data security and devise solutions when problems occur. The ability to learn, modify and lead implementation efforts related to network data security software configurations, procedures and policies; analyze network data security systems problems and devise solutions; write technical specifications for the acquisition of network data security hardware and software; write concise and comprehensive status reports related to management of assigned activities; apply principles and techniques of network security design to meet specific user/office needs; assess user needs and provide appropriate training and support; create clear guidelines and procedures; and provide leadership and technical assistance to others. The ability to use software to monitor data security equipment, and to detect malicious activity; maintain installation, service and repair records; establish and maintain cooperative working relationships with District personnel, network users, and equipment service personnel; analyze and express difficult concepts in oral and written communications; learn the characteristics of new computer systems, software, and hardware and update technical skills to adapt to changing technology.

Physical and Environmental Factors: Move, lift, and maintain computers and/or related equipment; stand, sit and maneuver for long periods; reach, grasp, pull, push equipment; stoop and crouch.

TYPICAL EQUIPMENT USE (May include, but not limited to)

Current office technologies, including mainframe computer, personal computers, servers, printers, copiers, and fax machines.