

POSITION DESCRIPTION

Information Technology Security Analyst

Position Information Technology Security Analyst
Department/Site Technology and Computer Services
FLSA Non-Exempt
Reports to Chief Information Services Officer
Salary Range 52

Summary

Under the Direction of the Chief Information Services Officer, ensures the security of data and the information technology resources of the District by evaluating, planning, designing, maintaining, monitoring and interacting with systems and applications related to information technology security. In a proactive fashion, identifies, reports, troubleshoots, diagnoses, and resolves security problems and breaches. Provides advanced technical training, support and help functions related to information technology security. Ensures District compliance with state and federal regulations regarding security of data and systems.

Essential Duties and Responsibilities

- Participates in formulating, developing, and implementing integrated security strategies for large networked computer systems. Provides planning and advanced technical expertise for securing computer and network services for both local and wide area networks and the internet.
- Configures, installs, and maintains system parameters, network addresses, directory structures, security, and network server software. Ensures continuous operations and security, responding to incidents as they occur. Configures, maintains, and participates in installation of directory structures, security applications and software.
- Continually analyzes network activity and establish approaches that prevent penetration of network and servers by unauthorized individuals. Monitors user access to networks.
- Installs and configures network users. Activates data communications ports using specialized network software. Oversees network protocols.
- Researches, defines, and proposes changes and upgrades to network infrastructure, operating systems, and applications to ensure proper security. Determines appropriate security configurations of hardware platforms and operating systems.
- Establishes and enforces system standards, protocols and procedural controls for operation of the network systems including remote access servers.
- Integrates minicomputer systems with network servers and host computer operations. Monitors network, server, workstation log files for inappropriate or malicious activity, and responds appropriately.
- Maintains server and client side antivirus software and ensures currency of threat prevention tools.
- Maintains up-to-date knowledge of developments in security technology, trends, and issues. Researches and recommends security enhancements to network and server systems, and assists in evaluation/selection of network and/or server equipment and/or software.
- Using network monitoring tools, identifies and diagnoses problems and recommends configuration changes and/or updates to applications.
- Uses network monitoring tools, access control lists and security policies to ensure a secure wireless network environment.
- Creates and maintains standard operating procedures. Maintains system log files and audit files. Creates and maintains audits of user accounts for all systems.

POSITION DESCRIPTION

Information Technology Security Analyst

- May participate with applications programmers to design custom programs and access.
- Performs other duties as assigned that support the overall objective of the position.

Qualifications

- Knowledge and Skills

- Requires specialized professional knowledge of information technology security standards and requirements.
- Requires specialized professional knowledge of current and relevant information technology security trends, threats, practices and tools.
- Requires specialized professional knowledge of personal computer based local and wide area networks; network operations through multiple servers; integration of data and tele- communications; principles and practices of data processing and systems administration, including connectivity between physical, virtual and remote servers.
- Requires in-depth understanding of encryption, SSL and authentication protocols.
- Requires in-depth understanding of line commands for managing and manipulating routers, switches, and firewalls.
- Requires a well-developed understanding of network infrastructure requirements and standards as well as the protocols and procedures for troubleshooting and performing maintenance.
- Requires a knowledge and understanding of 802.11 wireless technology standards and 802.1X wireless security protocols.
- Requires in-depth knowledge of modern network operating systems.
- Requires well-developed communication skills to convey highly technical concepts with a wide range of internal customers and provide instruction and technical assistance.

- Abilities

- Must be able to plan, design, organize, and implement an enterprise-wide IT security strategy with multiple routers, servers, systems, and applications and perform the full range of complex and technical duties described above.
- Must be able to analyze and evaluate user access needs and develop the most effective program or solution to meet those needs while maintaining data and system security.
- Must know how to configure, maintain and troubleshoot equipment, systems and programs used by the District.
- Must be able to develop programs, scripts, and systems related to security.
- Requires the ability to respond rapidly to security issues, minimize impact to operations and implement preventative measures.
- Must be able to prioritize activities.
- Must be able to read, interpret and apply complex technical information.
- Must be able to work independently with minimal direction.
- Requires the ability to develop and maintain positive working relationships with and instruct/tutor students, faculty and staff, plan and conduct group demonstrations, workshops, and training.

Physical Abilities

- Incumbent must be able to function effectively indoors engaged in work of primarily a sedentary nature.

POSITION DESCRIPTION

Information Technology Security Analyst

- Requires the ability to sit for extended periods to accomplish data entry and deskwork.
- Requires sufficient arm, hand, and finger dexterity in order to use a personal computer keyboard, multi-media presentation and other office equipment.
- Requires normal hearing and speaking skills to communicate in one-on-one and small group settings and distinguish sound prompts from equipment.
- Requires visual acuity to read printed materials and computer screens.

Education and Experience

- A bachelor's degree, and two years of computer network or operating system experience; or, in the absence of a bachelor's degree, an associate degree, or the completion of at least sixty (60) college-level semester units, and four years of computer network or operating system experience; or, in the absence of an associate degree, or the completion of at least sixty (60) college-level semester units, six years of computer network or operating system experience.

Licenses and Certificates

- May require a valid driver's license.

Working Conditions

- Work is performed indoors where minimal safety considerations exist.