IT INFRASTRUCTURE SECURITY MANAGER

DEFINITION

Plans, directs, and develops strategies for critical IT Infrastructure security initiatives and validates that business units, technical staff, third party vendors, and overall operations, including enterprise security solutions are functioning in a secure and stable manner.

TYPICAL DUTIES

- Plans, directs, develops, and applies IT Security operational plans impacting District business and integrated security requirements.
- Plans and oversees the development, implementation, and evaluation of enterprise-wide IT Infrastructure security initiatives.
- Directs the development, implementation, and maintenance of technical standards in alignment with District policies to ensure compliance with the system development life cycle.
- Develops, implements, and maintains team processes to proactively assess and remediate team and customer compliance with security policies and standards.
- Coordinates with other Information Technology (IT) functional areas to identify, evaluate, and implement process and systems improvement to ensure that appropriate security and access controls.
- Coordinates the development and maintenance of necessary internal and customer-facing documentation for assigned systems, projects, and tasks.
- Creates team goals that align with District strategies and defined IT security policies.
- Manages the daily workload and distributes assignments based on varying skillsets and abilities.
- Coaches and mentors team members, identifies training needs and recommends professional development programs.
- Manage operational processes to adhere to audit and compliance recommendations.
- Develops metrics and tracks against established goals and reports pertinent performance information to management.
- Collaborates with IT Security on researching, assessing, and acting upon threats, vulnerabilities, and exploits that may compromise the District's information assets.
- Collaborates with IT Security to address incident response and threat management, device monitoring and management, authentication and access management, and network security activities.
- Prepares and documents technical information for professional services, supplies, equipment, and/or general services contracts as needed to meet project goals and timelines.
- Collaborates in the development of the Disaster Recovery/Business Continuity plan.
- May represent the unit regarding complex technical issues.
- Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

The IT Infrastructure Security Manager develops strategies for critical IT Infrastructure security initiatives and leads a team of security engineers to ensure the proper design and implementation of infrastructure security services.

The IT Administrator, Shared Technical Services plans, organizes, and directs the activities of a branch that is responsible for the planning, administration, and maintenance of enterprise-wide

servers, databases, operating systems and related software and multiple data center operational functions.

A Cyber Security Engineer III is responsible for the overall design, administration, and installation, upgrades, and management of the security infrastructure and security controls.

SUPERVISION

General direction is received from the IT Administrator, Shared Technical Services or other higher level administrator. Supervision is exercised over Cyber Security Engineers and other lower-level IT personnel.

CLASS QUALIFICATIONS

Knowledge of:

- Systems Development Life Cycle
- Principles of program documentation, including preparation of manuals, systems analysis, configuration, and testing and practices
- Principles of web-based transactions, business intelligence, and/or data warehousing concepts emphasizing enterprise-wide performance management
- Structured programming and design techniques
- Project Management Methodologies
- Modeling, prototyping, simulation, and performance analysis
- Limitations of information technology hardware, software and services
- Relational Database Management Systems concepts and tools
- Database design and modeling
- Oracle database and development toolsets and programming languages such as OBIEE, OWB, Designer, and PL/SQL
- Microsoft .NET software development toolset
- Java application development toolset
- Open source languages such as PHP, HTML, and XML
- Applicable education code laws, regulations, and guidelines related to cyber security
- Procurement policies and procedures
- Personnel policies and procedures

Ability to:

- Analyze problem situations, define problems, identify relevant factors and relationships, formulate solutions, and recognize the implications of those solutions
- Estimate project requirements and organize resources to meet established deadlines and goals
- Express difficult concepts orally and in writing in a clear and concise manner
- Schedule and lead a project team through to successful project completion
- Coordinate systems design with user needs, data, regulations, and other factors
- Communicate with all levels of users and personnel
- Think creatively in developing new procedures, methods, or approaches
- Reengineer work flow for users
- Train subordinates and others
- Resolve conflicts and promote cooperation
- Plan work assignments and estimate needs for staff and time
- Manage multiple concurrent projects
- Work under the pressure of deadlines in a fast-paced environment
- Maintain a positive customer service attitude
- Recommend improvements to the system platforms processes and/or technically within functional and budgetary constraints

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university with a bachelor's degree in computer science, information systems, engineering or a related field. Qualifying experience in addition to that required may be substituted on a year-for-year basis provided that the requirement of a high school diploma or equivalent is met. A graduate degree in systems management, engineering, or computer science is preferable.

Experience:

Six years of professional-level experience in the administration, implementation and management of security controls projects and/or enterprise technologies for a large organization. Experience must have included working in a K-12 school district, writing technical materials, and working in a supervisory capacity. Experience may have been concurrent.

Special:

Certified Information Systems Security Professional (CISSP) is required and must be kept valid during the term of employment
Any GIAC security- related certification is preferable
Information Technology Infrastructure Library (ITIL) Foundation level certification is preferable
Project Management Professional (PMP) certification is preferable
A valid California Driver License
Use of an automobile

SPECIAL NOTES

Employees in this class may be subject to call at any hour.

This class description is not a complete statement of essential functions, responsibilities, or requirements. Entrance requirements are representative of the minimum level of knowledge, skill, and /or abilities. To the extent permitted by law, management retains the discretion to add or change typical duties of a position at any time, as long as such addition or change is reasonably related to existing duties.

Revised
05-14-18
PJO