

CYBERSECURITY SPECIALIST I/II/III

DEFINITION

Under immediate (Cybersecurity Specialist I), general supervision (Cybersecurity Specialist II), or direction (Cybersecurity Specialist III), performs a variety of technical and professional duties in the support of implementing the District's information technology security program including, but not limited to, security awareness, risk assessment, business impact analysis, disaster recovery, and business continuity; monitors and evaluates the District's information security posture daily; and performs related duties as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives immediate (Cybersecurity Specialist I) or general (Cybersecurity Specialist II) supervision or direction (Cybersecurity Specialist III) from assigned supervisory or management personnel. Exercises no direct supervision over staff.

CLASS CHARACTERISTICS

Cybersecurity Specialist I: This is the entry-level classification in the Cybersecurity Specialist series. Initially under close supervision, incumbents learn and perform routine support of District security infrastructure and systems. As experience is gained, assignments become more varied, complex, and difficult; close supervision and frequent review of work lessen as an incumbent demonstrates skill to perform the work independently. Positions at this level usually perform most of the duties required of the positions at the II-level but are not expected to function at the same skill level and usually exercise less independent discretion and judgment in matters related to work procedures and methods. Work is usually supervised while in progress and fits an established structure or pattern. Exceptions or changes in procedures are explained in detail as they arise.

Cybersecurity Specialist II: This is the fully qualified journey-level classification in the Cybersecurity Specialist series. Positions at this level are distinguished from the I-level by the performance of the full range of duties as assigned, working independently, and exercising judgment and initiative. Positions at this level receive only occasional instruction or assistance as new or unusual situations arise and are fully aware of the operating procedures and policies of the work unit. This class distinguished from the Cybersecurity Specialist III in that the latter provides technical and functional direction to lower-level support staff and is responsible for the more complex work.

Cybersecurity Specialist III: This is the advanced journey-level classification in the Cybersecurity Specialist series. Incumbents work under direction and exercise a high level of discretion and independent judgment in performing the full range of duties in support of the District's information technology security program. Assignments are given with general guidelines and incumbents are responsible for establishing objectives, timelines, and methods to deliver work products or services. Work is typically reviewed upon completion for soundness, appropriateness, and conformity to policy and requirements.

Positions in the Cybersecurity Specialist class series are flexibly staffed; positions at the II-level and III-level are normally filled by advancement from the I-level and II-level, respectively. Progression to the II-level and III-level is dependent on satisfactory work performance, the incumbent meeting the minimum qualifications for the classification including any licenses and certifications, and management approval for progression to the II-level and III-level.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

Management reserves the right to add, modify, change, or rescind the work assignments of different positions and to make reasonable accommodations so that qualified employees can perform the typical functions of the job.

Positions at the Cybersecurity Specialist I-level may perform some of these duties and responsibilities in a learning capacity.

- Implements, maintains, and enforces a districtwide information technology security program including security awareness, risk assessment and mitigation, compliance monitoring, and disaster recovery.
- Analyzes and evaluates District technology and business processes for security related purposes with specific focus on District information technology security policies and guidelines governing and regulating data creation, access, retention, and destruction
- Applies technical standards, methods, and tools for the identification and investigation of information security threats and incidents; installs system security hardware, software, and related devices; audits pertinent logs, analyzes the results from information security scans, and activates defined procedures to identify, investigate, respond to, and resolve information security incidents.
- Performs regular security assessments and audits of critical information technology network, server, supervisory control and data acquisition (SCADA), and data storage infrastructure, systems, and devices to mitigate immediate and future threats; reports potential vulnerabilities; identifies strengths and gaps which require action; collaborates with other information technology and SCADA staff to develop and implement corrective action plans and mitigate future risks.
- Conducts research to identify alternatives for resolving information security issues and collaborates with other information technology and SCADA staff to develop specifications for hardware and software information security systems.
- Assists in the development of effective disaster recovery and business continuity plans.
- Advises District staff and management on security policies, computer operations, server infrastructure, SCADA, and network and data communication systems security; recommends the use of information technology and network security solutions and tools.
- Promotes and presents information technology security training and education to all staff on an ongoing basis.
- Participates in information technology security projects including assisting in working with stakeholders and management to determine project requirements, objectives, deliverables, and business needs; participates in monitoring project progress and ensuring deliverables are on time and within budget.
- Receives and manages work orders; acts as a point of contact for information technology related security incidents or violations.
- Writes and maintains user and technical operating instructions and documentation.
- Conducts research and stays current on new trends, regulatory changes, and innovative solutions for information technology security programs; recommends new technologies and process changes to improve information technology security effectiveness and services.
- Observes and complies with all District and mandated safety rules, regulations, and protocols.

- Performs related duties as assigned.

In addition, the Cybersecurity Specialist III:

- Participates in developing long-term plans, goals, and objectives to achieve District and department technology and business priorities.
- Trains and reviews the work of staff responsible for the District's security program and systems; ensures maximum performance and efficiency in work performed.
- Serves as a subject matter expert in supporting a diverse range of business applications by evaluating and implementing security strategies and tools, analyzing, designing, and configuring business process workflows to ensure that all District needs are met, and working with departments to ensure adherence to information technology security policies and procedures.
- Participates in a variety of system user and work groups to identify user needs and operational, programmatic, and/or regulatory changes affecting security, system, and data requirements.

QUALIFICATIONS

Positions at the Cybersecurity Specialist I-level may exercise some of these knowledge and abilities statements in a learning capacity.

Knowledge of:

- Information technology security management theory, principles, and practices and their application to a wide variety of services and programs.
- Industry best practices related to information technology security management and control.
- Methods and techniques of implementing security systems protocols and standards, identifying and assessing security threats and violations, and developing response and mitigation strategies.
- Operational relationships between information technology security program, application development, database management, SCADA systems, and components of technology infrastructure such as server and network systems.
- Information security forensic tools, rules of evidence, and chain of custody.
- Vulnerability management systems or services.
- Effective disaster recovery and business continuity plans.
- Applicable federal, state and local laws, regulatory codes, ordinances and procedures relevant to assigned areas of responsibility.
- Methods and techniques of eliciting information and performing diagnostic procedures on information technology systems.
- Principles and practices of developing and maintaining technical documentation.
- Record keeping and filing system methods, principles, and practices.
- Techniques for providing a high level of customer service by effectively dealing with the public, vendors, contractors, and District staff.
- The structure and content of the English language, including the meaning and spelling of words, rules of composition and grammar.
- Modern equipment and communication tools used for business functions and program, project, and task coordination, including computers and software programs relevant to work performed.

Ability to:

- Conduct risk assessments of District information technology infrastructure, systems, and devices and make recommendations on needed changes.
- Respond to and investigate, security threats, incidents, and violations.
- Troubleshoot, diagnose, analyze, and resolve information security problems and identify and recommend alternative solutions.
- Monitor information technology security vulnerability; implement approved measures to ensure integrity and security of infrastructure and systems.
- Work collaboratively with District staff to identify and implement security solutions for business process improvements and efficiencies.
- Recommend and implement new, enhanced, or modified information technology security systems and tools.
- Prepare clear and concise technical documentation.
- Understand, interpret, and apply all pertinent laws, codes, regulations, policies and procedures, and standards relevant to work performed.
- Integrate technology solutions across multiple platforms.
- Prepare clear, concise, and accurate technical documentation, user guides, reports of work performed, and other written materials.
- Communicate complex technology issues clearly to non-technical parties.
- Maintain a variety of filing, record keeping, and tracking systems.
- Organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- Use tact, initiative, prudence, and judgment within general policy and procedural guidelines.
- Effectively use computer systems, software applications relevant to work performed and modern business equipment to perform a variety of work tasks.
- Communicate clearly and concisely, both orally and in writing, using appropriate English grammar and syntax.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:

Any combination of training and experience that would provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the required qualifications would be:

Education:

Equivalent to a bachelor's degree from an accredited college or university with major coursework in computer science, information systems, or a related field.

Experience:

Cybersecurity Specialist I

- One (1) year of experience performing work related to ensuring security of information technology infrastructure and systems.

Cybersecurity Specialist II

- Three (3) years of increasingly responsible experience related to ensuring security of information technology and SCADA infrastructure and systems or equivalent and related responsibilities to experience as a Cybersecurity Specialist I.

Cybersecurity Specialist III

- Five (5) years of increasingly responsible experience related to ensuring security of information technology and SCADA infrastructure and systems or equivalent and related responsibilities to experience as a Cybersecurity Specialist II.

Licenses and Certifications:

- Possession of a valid California Class C driver's license, to be maintained throughout employment.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

The conditions herein are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential job functions.

ENVIRONMENT

Standard office setting.

PHYSICAL

- Level One

Incumbents require sufficient mobility to work in an office setting; stand or sit for prolonged periods of time; operate office equipment including use of a computer keyboard; light lifting and carrying; ability to verbally communicate to exchange information.

VISION

See in the normal visual range with or without correction; vision sufficient to read computer screens and printed documents; and to operate assigned equipment.

HEARING

Hear in the normal audio range with or without correction.

ADDITIONAL REQUIREMENTS

Performs work on weeknights, weekends, and holidays as needed for system upgrades, special projects, or in emergency situations as assigned.