Cucamonga Valley Water District
Service Beyond Expectation

LEAD INFORMATION TECHNOLOGY SECURITY SPECIALIST

Job Status:	Exempt
Date Adopted:	5-13-2025
Date Modified:	5-13-2025

Safety Sensitive Position

Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are not intended to reflect all duties performed within the job.

DEFINITION

To perform a wide variety of specialized professional support duties for the Information Technology Division of the Finance and Technology Services Department, including but not limited to leading, coordinating, and participating in the analysis, design, and implementation of IT security best practices; solutions for Supervisory Control and Data (SCADA), servers, desktops, and cloud infrastructure; develops compliance strategies for IT security programs; leads the assessment of risks of non-compliance to management policies, procedures, standards, and guidelines and reports findings to management; oversees, reviews, analyzes, and coordinates security upgrades and vulnerability management program; provides expert technical systems and infrastructure security advice, recommendations, and assistance in the development or implementation of risk-based mitigation plans.

DISTINGUISHING CHARACTERISTICS

The Lead IT Security Specialist is the experienced advanced journey level. Incumbents in this class are distinguished from the Information Technology Specialist II by performing the full range of duties assigned. At this level, incumbents perform the more complex and specialized workloads while exercising broader discretion and independent judgment within established guidelines. Emphasis is on leads and participating in the technical analysis and correlation of security data/logs to identify potential threats and vulnerabilities or to determine the root cause of a security-related event/incident; researches evaluates, and recommends security tools, products, platforms, and standards based on industry trends, business requirements, and technical infrastructure; monitors, analyzes, and responds to security event using security-event management tools; maintains awareness and knowledge of current changes within legal, and Disaster Recovery plan activities and may act on his/her behalf in his/her absence if appointed.

SUPERVISION RECEIVED AND EXERCISED

Direct supervision is received from the Information Technology Manager.

ESSENTIAL AND MARGINAL FUNCTION STATEMENTS

Essential and other important responsibilities and duties may include, but are not limited to, the following:

Essential Functions:

1. Ability to communicate and present security risk concisely and effectively (written, oral, and presentation).
2. Demonstrated leadership and problem-solving skills.

3. Ability to manage effectively and work closely with business leaders in a high-pressure, fast-paced, highly collaborative environment with multiple deadlines and competing priorities.
4. Proven knowledge of security architecture design, network security, vulnerability management, and threat intelligence analysis.
5. Experience in security, operations, control assessment, risk management, auditing, and/or internal controls.
6. Experience with security and privacy, legal, and regulatory requirements.
7. Knowledge of common information security management frameworks, such as NIST, CIS, ISO 27001, COBIT, or PCI DSS.
8. Experience performing information security risk assessments and risk analysis.
9. Strong understanding of encryption.
10. Strong understanding of networking concepts and protocols (e.g., TCP/IP, LAN, WAN, DHCP, DNS, routing protocols).
11. Expert-level knowledge of security systems such as SIEM, IPS firewalls, and related network security tools.
12. Experience with operating systems such as Windows, Unix, Apple, SQL, Azure, and Oracle databases.
13. Experience with Industrial Control Systems software such as Siemens, Wonderware, and similar platforms.
14. The ability to support and handle urgent issues after hours.
15. Competency in customer focus, change and innovation, strategic thinking, relationship thinking, relationship building and influencing talent management, results focus, and inspirational leadership.

Marginal Functions:

1. Perform related duties and responsibilities as required.
2. Support vendors in the maintenance of WAN circuits.
3. Participate in setting direction for the Information Technology Division.
4. May be designated to act on behalf of the Information Technology Manager in his absence.
5. Participate in strategic planning and reporting on budget, disaster planning, and master planning.
6. Perform maintenance and support of firewalls, routers, network equipment and work with outside vendors supporting these devices.
7. Requests for Quotes (RFQ) and Statements of Work (SOW) standard procedures.
8. Performs security assessment/penetration testing for SCADA, infrastructure, applications, databases, and cloud computing.
9. May be required to participate in the Countywide Cybersecurity Emergency Response Team, Departmental Cybersecurity Emergency Response Team, and Cybersecurity Workgroups.
10. May supervise IT staff in the performance of security-related assignments.
11. May be required to represent the department in legal matters related to IT systems security.

Lead Information Technology Security Specialist

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge of:

Extensive expertise in personal computer hardware and software, combined with a strong understanding of the fundamental principles of data processing systems.
Operation and use of operating systems using District-standard software.
Word processing, spelling, punctuation, and grammar skills using District-standard software.
Database and spreadsheet principles using District-standard software.
Application analysis, design, programming, testing, and debugging.
Computer hardware platforms, operating systems, and middleware systems.
Information Security Principles.
Principles of customer support and service.
Principles and practices of technical problem-solving.
Testing standards and procedures.
Principles and practices of project management, work planning, and status reporting.
Business processes, operating practices, and the organizational structure of a public-sector agency.
Principles and techniques of application and systems analysis and design.

Ability to:

Analyze and resolve application problems, as well as software and hardware integration.
Apply technology to provide business solutions.
Work effectively with clients, peers, and support teams to ensure that tasks are completed accurately and in a timely manner.
Communicate effectively both orally and in writing.
Evaluate and select hardware and software and work effectively with vendors to integrate solutions.
Analyze and resolve complex problems, including applications and software integrations.
Work effectively with peers and support teams to define business requirements, provide support for software, hardware, and applications, and ensure that tasks are completed accurately and in a timely manner.
Design systems that meet defined requirements and document system design for development, implementation, testing, and client use.
Research potential solutions, make implementation recommendations, and apply technology to provide business solutions.
Develop solutions and recommend technology to provide target business outcomes.
Establish and maintain effective working relationships with those contracted during the course of the work and project.
Maintain alert mental capacity that allows the capability of making sound judgments and decisions and demonstrating intellectual capabilities.
Maintain physical condition appropriate to the performance of assigned duties and responsibilities.
Maintain effective audio-visual discrimination and perception needed for making observations, communicating with others, reading, writing, and operating assigned equipment.

REQUIRED QUALIFICATIONS

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

Job Title	***Lead I.T. Security Specialist***
Experience	• Five (5) years of progressive experience operating personal computer operating systems, word-processing and spreadsheet software; database application design and development; installing and maintaining personal computer hardware and software; and programming and systems analysis experience; installing and troubleshooting networks, Windows server operating systems, Microsoft Exchange/365, Active Directory, and networked equipment including fiber optics. • Five (5) years of experience administrating, configuring, maintaining, and upgrading LAN/WAN hardware and operating systems.
Education/Training	• Possession of a Bachelor's Degree in Information Technology, Computer Science, Management Information Systems, or related fields. • Certifications in Information Technology, Networking, or Systems Administration with an emphasis on IT security.
Required License/Certification	• Possession of a certification in administrative network equipment such as Cisco Certified Network Associate (CCNA) or Cisco Certified Network Professional (CCNP).
Desirable Degree/License/ Certification	• Certified Information Systems Security Professional (CISSP) • VMware Certified Professional (VCP) Certification. • VMware Certified Technical Associate (VCTA) Certification. • Palo Alto Certified Network Security Administrator (PCNSA) Certification.
DMV Class	• Possession of a valid California Class C driver's license and a satisfactory driving record.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

The physical demands and working environment demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential job functions.

Environment:

Standard office setting; frequent interaction with District staff and the general public.

Physical:

Incumbents require sufficient mobility to work in an office setting; stand and sit for prolonged periods; operate office equipment including computer keyboard; light lifting and carrying; ability to verbally communicate to exchange information; use of hands and fingers repetitively to operate, handle, or feel office

equipment and reach with hands and arms. Employees are frequently required to stand and walk.

Mental:
While performing the duties of this class, the employee is regularly required to use written and oral communication skills; read and interpret data, information, and documents; analyze and solve problems; observe and interpret situations; learn and apply new information or skills; perform highly detailed work; work on multiple concurrent tasks; work with frequent interruptions; work under intensive deadlines; interact with District managers, staff, vendors, the public and other encountered in the course of work.

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.