



Job Description

POSITION TITLE:	Coordinator IV, Cybersecurity Architect Enterprise Services/Information Technology Business Services	#6242
------------------------	---	--------------

SALARY PLACEMENT:	Management Salary Schedule Range 14
--------------------------	--

SUMMARY OF POSITION:

Under the general direction of the Director of Enterprise Services, the Cybersecurity Architect is responsible for planning, designing, building, testing, implementing, and maintaining of information security systems within the SJCOE/DP JPA, and will serve as a resource for cybersecurity related matters for SJCOE and DP JPA member districts.

MINIMUM QUALIFICATIONS-EDUCATION, TRAINING, AND EXPERIENCE:

Possess a Bachelor's Degree from an accredited College or University with a concentration in computer-related technology and/or Business Administration; or equivalent experience in management information systems.

DESIRABLE QUALIFICATIONS – EDUCATION, TRAINING, AND EXPERIENCE:

Five years of increasingly responsible experience with information systems in a large-scale information technology environment including administering IT security controls and compliance assessments. Knowledge of cybersecurity operations and services, laws, regulations, policies, procedures, incident response and disaster recovery. Experience designing, building, implementing, and supporting enterprise-class information security systems to mitigate IT security threats. Experience performing security assessments, including security program reviews, penetration testing, vulnerability testing, risk analysis. Familiar with security configuration and policies for network systems and the ability to analyze system logs, and network traffic for unusual or suspicious activity. Ability to write and prepare elaborate proposals, contracts, and scopes of work. Previous experience supervising, leading, and evaluating staff. Experience with educational administrative systems. Experience in a public education environment.

KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge of:

- cybersecurity laws, regulations, policies, procedures, and standards (e.g. OWASP, SANS, CIS, NIST etc.)
- a wide range of California K-12 specific requirements, including but not limited to California Ed Code, SOPIPA and Public Records Act; familiarity with a wide range of federal requirements, including but not limited to COPPA, CIPA, FERPA, PPRA, HIPAA
- proper office methods and practices
- operational requirements of networked computer systems
- applications including Microsoft Office and others
- Chromebooks, Macintosh, Windows, and Windows Server operating systems
- mobile computing platforms including smartphones and tablets
- modern computer techniques, methodologies, principles, and practices

Ability to:

- conduct daily cybersecurity operations and services, use of scripting languages and technologies to administer, and automate information security systems
- be flexible and receptive to change
- follow manuals and read complicated instructions

- understand and carry out oral and written instructions
- use appropriate and correct English, spelling, grammar, and punctuation
- perform arithmetic calculations with speed and accuracy
- operate and have a sound technical understanding of a variety of computing systems, operations, hardware, and software
- maintain and actively pursue personal knowledge of current industry trends and technological advancements within the computing field
- work independently
- establish and maintain effective working relationships with others in a large diverse user environment

Possess:

- leadership skills in planning, setting agendas, and coordinating/conducting meetings/trainings
- management skills in the areas of scheduling, inventory control and communication with staff and the community
- a valid California driver's license and proof of liability insurance coverage in the minimum amount required by SJCOE policy; insurable by the SJCOE carrier. Must furnish own transportation as required to fulfill job duties.

DISTINGUISHING CHARACTERISTICS:

The Coordinator series represents advanced management positions and has four levels.

ESSENTIAL FUNCTIONS:

Essential functions may include, but are not limited to:

1. Work effectively with school districts, community organizations, government agencies, parents, students, and/or staff.
2. Maintain confidentiality on issues concerning program and staff.
3. Hire, supervise and evaluate staff.
4. Participate, coordinate, or conduct a variety of meetings, staff developments, committees, trainings, workshops, and/or conferences in order to present materials and information concerning department programs, services, operations, and activities; represent the SJCOE at local, regional, and state meetings, conferences, in-services, boards, councils, and events.
5. Maintain current knowledge and interpret applicable rules, regulations, policies, procedures, contracts, State and Federal laws, codes, and regulations.
6. Communicate effectively both orally and in writing.
7. Analyze situations accurately and adopt an effective course of action.
8. Establish and maintain cooperative and effective working relationships with others.
9. Work independently with little direction.
10. Meet schedules and timelines.
11. Prepare reports as needed for program.
12. Oversee and manage budgets.
13. Utilize computing hardware and software, word-processing, spreadsheet, and database applications to perform basic duties including documentation, reporting, scheduling, and user support.
14. Provide cybersecurity training and support to a diverse customer base.
15. Create, recommend, and update cybersecurity standards, policies, procedures, and incident response plans.
16. Analyze existing or proposed projects and requests to determine alignment with cybersecurity policies and procedures.
17. Comply with all standards, procedures, controls, and policies as established by San Joaquin County Office of Education, participating school districts, and the Information Technology department.
18. Acts as a cybersecurity subject matter expert to communicate complex technologies and security issues to non-technical individuals.
19. Design, build, implement, and support enterprise-class information security systems.
20. Identify and communicate current and emerging IT security threats, security needs, and priorities.
21. Design security architecture elements to mitigate IT security threats.
22. Plan, research, and design robust security architectures for assigned IT projects.
23. Perform security assessments, including security program reviews, penetration testing, vulnerability testing, risk analysis, and provides recommendations related to findings.
24. Create IT security solutions that effectively balance business requirements with information and cybersecurity requirements.

25. Review and recommend security configuration and policies for firewalls, VPN systems, routers, and intrusion detection systems.
26. Serve as a resource and provides Tier-2 support in response to security-related incidents.
27. Collaborate with other teams to ensure SJCOE and DP JPA districts electronic systems are secure.
28. Review and analyze system logs, SIEM tools, and network traffic for unusual or suspicious activity, and makes recommendations to restore secure operations.
29. Review and test new security software, tools and/or technologies to determine applicability to SJCOE operations.
30. Perform other related duties as required.

PHYSICAL REQUIREMENTS:

Employees in this position must have the ability to:

1. Sit and stand for extended periods of time.
2. Enter data into a computer workstation, operate standard office equipment and use the telephone.
3. Hear and understand speech at normal levels and on the telephone.
4. See and read the computer screen and printed matter with or without vision aids.
5. Speak so that others may understand at normal levels to small or large groups, and on the telephone.
6. Stand, walk, and bend over, reach overhead, grasp, push, pull and move, lift and/or carry up to 50 pounds to waist height.

WORK ENVIRONMENT:

Employees in this position will be required to work indoors in a standard office environment and come in direct contact with SJCOE and school district staff, students, parents, outside agency staff and the public. Employees may be required to work outside of normal workdays and office hours for emergency situations, troubleshooting, critical demand periods, scheduled vacations or to meet installation deadlines. Requires travel within San Joaquin County and occasionally elsewhere within California.

9/2/2021 final sc