Tulare County Office of Education
JOB DESCRIPTION **Job Title:** Coordinator, Cybersecurity (9602)

Job Summary:
Under the general supervision of the Director of Information Systems, the Cybersecurity Coordinator assists in protecting the Tulare County Office of Education (TCOE) hybrid technology infrastructure, networks, and data from cyberattacks and security breaches. This role includes continuous monitoring, analysis, and response to internal and external security threats, as well as the administration and monitoring of key security controls such as firewalls and threat detection systems. The Cybersecurity Coordinator assists with the planning, coordination, and implementation of comprehensive cybersecurity programs, policies, tools, training, communication, and services, ensuring the integrity, confidentiality, and availability of TCOE data across cloud and on-premises environments.

Essential Duties:
- Continuously monitor network traffic, systems, security alerts, and threat intelligence using SIEM and other security tools; identify potential threats and anomalous activity; investigate cybersecurity incidents, including phishing and malware; coordinate incident response, escalation, remediation, and recovery; and maintain appropriate incident records.
- Conduct and participate in cybersecurity risk and vulnerability assessments, defensive security exercises, and regular vulnerability scans of networks, applications, systems, and other technology assets; evaluate identified risks and recommend appropriate mitigation strategies.
- Coordinate and participate in the planning, development, implementation, maintenance, and governance of TCOE cybersecurity programs, policies, procedures, standards, tools, and services to support compliance with applicable TCOE policies, laws, regulations, industry best practices, and cybersecurity frameworks.
- Research emerging cybersecurity technologies, threats, standards, and best practices and recommend improvements to TCOE's cybersecurity architecture, controls, policies, and security framework.
- Assist with or coordinate investigations of IT security incidents with law enforcement agencies as directed by management.
- Review, evaluate, test, and recommend cybersecurity software, hardware, and technical controls, including firewalls and intrusion detection/prevention technologies.
- Administer, configure, monitor, and coordinate the implementation and maintenance of cybersecurity technologies and controls, including network firewalls, endpoint protection, antivirus, spam filtering, SSL certificates, and related security systems.
- Work with other IT staff to ensure the integrity and security of TCOE cloud data, applications, and infrastructure across hybrid environments.
- Assist in the development and maintenance of disaster recovery plans for TCOE technology and data; implement and maintain current recovery technologies and research new options for improving data and systems recovery.
- Coordinate cybersecurity-related activities with contractors, technology vendors, and Managed Security Service Providers (MSSPs); monitor service and contract requirements, facilitate remediation of security events, and coordinate implementation of security improvements.
- Participate in security and risk reviews of new technologies, cloud services, applications, and third-party solutions to identify cybersecurity, privacy, and compliance considerations prior to implementation.
- Develop, maintain, and communicate cybersecurity metrics, risk indicators, incident trends, and other information used to evaluate TCOE's cybersecurity posture and support management decision-making.
- Develop and deliver cybersecurity awareness training for TCOE employees to promote a culture of security and reinforce organizational security practices and protocols.
- Provide timely cybersecurity briefings and recommendations to management and stakeholders; assist with the development and execution of cybersecurity incident response and communication plans.
- Provide consultative cybersecurity support to TCOE programs and school districts by assessing needs, recommending risk-based solutions, assisting with compliance readiness, and providing practical technical guidance.
- Coordinate professional development activities for TCOE and school districts, including but not limited to events such as the annual TCOE Cybersecurity Conference.
- Plan, organize, coordinate, and provide direction to assigned staff; establish priorities, monitor work, and promote effective team performance.

- Serve as the Information Systems point of contact for TCOE cybersecurity insurance matters, assisting with annual renewals, cybersecurity questionnaires and assessments, documentation requirements, and claims management.
- Facilitate all confidential requests by the Superintendent of Schools and/or the Assistant Superintendent of Human Resources, including restricting employee access to TCOE networks and systems.
- Travel to various locations within and outside Tulare County for work-related duties.
- Perform other related duties as assigned.

Skills, Knowledge and/or Abilities:
Skills to:

- Effectively utilize SIEM and other security monitoring technologies to interpret alerts, identify anomalous activity, and support incident response.
- Apply cybersecurity risk assessment, vulnerability management, and risk mitigation methodologies.
- Configure, administer, troubleshoot, and effectively utilize cybersecurity controls, tools, and platforms used to secure network and data infrastructure, including IDS/IPS, firewalls, endpoint protection, antivirus, and other security technologies.
- Analyze security policies, trends, and intelligence using deductive reasoning and problem-solving skills to develop preventive countermeasures.
- Apply applicable cybersecurity, privacy, and regulatory requirements to organizational security practices and decision-making.
- Utilize programming and scripting languages for automating security tasks.
- Analyze complex cybersecurity problems, identify root causes, evaluate potential solutions, and respond effectively under pressure.
- Communicate complex cybersecurity information clearly and concisely, both orally and in writing, including analyses, reports, correspondence, presentations, and explanations appropriate for technical and non-technical audiences.
- Exercise sound professional judgment and make timely, informed decisions during cybersecurity incidents and other time-sensitive situations.
- Track and coordinate assigned cybersecurity tasks and projects running in parallel; organize and schedule work to maximize efficiency.

Knowledge of:

- Principles, practices, and methods of security infrastructure and vulnerability management, including evolving sources of security threats, preventive controls, and common security management frameworks (e.g., ISO 27001, NIST, GDPR, HIPAA, FERPA).
- Network security, incident response, penetration and vulnerability testing, SIEM tools, encryption, malware analysis, and intrusion detection/prevention systems.
- Cloud platforms (e.g., AWS, Azure) and related operating systems, security tools, and scripting languages.
- Network design and security practices in hybrid environments.
- Applicable principles and general understanding of voice, video, storage, and data platform operations.
- Best practices, methods, and principles of security auditing, risk management, threat modeling, vulnerability and security testing, policy development, business continuity, and disaster recovery.
- Research methods, analysis techniques, and principles of sound business communication.
- Federal, state, and local laws, regulations, and court decisions governing the area of assignment.
- TCOE mission, vision, value statements, standards, policies and procedures, operating instructions, confidentiality standards, and the code of ethical behavior.

Ability to:

- Maintain strict confidentiality of staff and student files, records, and security investigations.
- Work independently within established procedures and management direction, as well as collaboratively in a team environment.
- Establish and maintain effective working relationships with those contacted in the performance of required duties.
- Demonstrate an understanding of, sensitivity to, and appreciation for the academic, ethnic, socio-economic, cultural, linguistic, disability, and gender diversity of students and employees.

- Quickly understand and organize complex technical security information.
- Travel to various locations within and outside of the county, using personal vehicle, if necessary.

Responsibilities include: working independently under broad organizational guidelines with supervision focused on results; leading, guiding, and/or coordinating assigned staff; operating within defined budget and security framework guidelines; collaborating with other work units as needed; and contributing to the Organization's security posture, risk management, and technology services. The usual and customary methods of performing the job's functions require the following physical demands: sitting for extended periods; standing, walking, and driving between sites; light lifting, carrying, pushing, and/or pulling; occasional reaching, bending, and retrieving materials; and fine finger dexterity for frequent keyboarding and computer operation. Generally, the job requires 80% sitting, 10% walking, and 10% standing.

Education Required:

- Bachelor's degree from an accredited college or university in computer science, information technology, information security, network administration, cybersecurity, or a related field.
- Possession of a cybersecurity certification, such as CompTIA Security+, CEH, GSEC, CISSP, GIAC, AWS Certified Security – Specialty, Azure Security Engineer Associate, or an equivalent certification is preferred.

Experience Required:

- Four (4) years of experience in cybersecurity, network security administration, or system security infrastructure.

Other Requirements:

- Valid California driver's license and proof of automobile insurance.
- Department of Justice and FBI Fingerprint clearance upon hire.
- Must be able to use own vehicle to travel throughout the County, as needed.

FLSA Status: Exempt October 2026

This organization is an Equal Opportunity Employer and does not discriminate on the basis of race, color, national origin, creed, age, gender or disability. Inquiries regarding compliance procedures may be directed to our personnel office. This organization complies with the Americans with Disabilities Act. Persons with a disability who may need some accommodation in the hiring process should contact our personnel office. This organization is a Drug and Tobacco - Free Workplace. This organization requires a successful candidate to provide it with employment eligibility and verification of a legal right to work in the United States in compliance with the Immigration Reform and Control Act.