

COORDINATOR, CYBERSECURITY

DEFINITION

Under general direction, designs, implements and maintains the Office's information security infrastructure to include advanced security measures, incident response, and policy/process development; ensures compliance with industry standards and regulations; provides guidance and support in identifying, assessing and remediating County school district cybersecurity needs; assists in developing and testing network and cloud systems and providing leadership to the Office's personnel on all cybersecurity-related matters; and performs related duties as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from assigned supervisory or management personnel. Exercises technical and functional direction over and provides training to lower-level staff. Exercises no direct supervision over staff.

CLASS CHARACTERISTICS

This is an advanced journey-level classification responsible for performing the most complex work in support of the Office's information security and network structure. Incumbents regularly work on tasks which are varied and complex, requiring considerable discretion and independent judgment. Positions in the classification rely on experience and judgment to oversee security of information systems; and serve as technical advisor, liaison, and project lead. Assignments are given with general guidelines and incumbents are responsible for establishing objectives, timelines and methods to deliver services. Work is typically reviewed upon completion for soundness, appropriateness, and conformity to policy and requirements.

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 essential functions of the job.

- Plans, organizes and coordinates the design, implementation and maintenance of the Office's security infrastructure, including but not limited to firewalls, intrusion detection/prevention systems (IDS/IPS), Virtual Private Networks (VPN), specialized information security tools, and endpoint security solutions.
- Provides security guidance to network staff for the maintenance of cybersecurity best practices for network, cloud and server systems.
- Produces and maintains reports related to the Office's cybersecurity posture; monitors system logs, security information and event management (SIEM) tools and network traffic for unusual or suspicious activities; interprets such activity and makes recommendations for resolution.
- Leads projects related to the implementation of network security enhancements, ensuring seamless integration and adherence to project timelines.
- Participates in incident response planning; investigates security breaches, and coordinates remediation activities.
- Participates in the development and updating of cybersecurity and business continuity policies, standards, and procedures in alignment with industry best practices and regulatory requirements.

- Conducts regular vulnerability assessments and participates in penetration testing to identify and mitigate security risks; collaborates with Integrated Technology Services (ITS) network team to address and remediate vulnerabilities promptly; ensures compliance with industry regulations and internal security standards.
- Oversees security patch management processes to ensure timely and effective patching of systems and applications.
- Analyzes security incidents, trends, and threats; recommends improvements to security controls and measures to enhance the organization's security posture.
- Develops and delivers security awareness training programs for employees to promote a culture of cybersecurity awareness.
- Provides technical assistance and user support to staff, school districts, outside agencies and others concerning cybersecurity and network architecture concerns; responds to inquiries and provides detailed and technical information concerning network design, equipment, hardware, software, security, connectivity, configuration, malfunctions, applications, practices, techniques and procedures.
- Serves as a liaison and coordinates cybersecurity and network-related projects, communications and information between the Office, local school districts, vendors, consultants and various outside agencies; resolves related issues and conflicts in a proper and timely manner.
- Prepares and delivers regular security reports to management and stakeholders, summarizing key security expectations, incidents, and risks; contributes to the development of the organization's long-term security strategy and roadmap.
- Maintains comprehensive documentation of security configurations, incident reports, and security policies and procedures.
- Participates in building and implementing ITS strategic plans; assists in the development of ITS's budget.
- Stays informed about the latest security threats, vulnerabilities, and industry trends; evaluates and recommends new security tools and technologies to enhance cybersecurity capabilities.
- Observes and complies with all Office and mandated safety rules, regulations, and protocols.
- Performs related duties as required.

QUALIFICATIONS

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 or related field.

Experience:

- Five (5) years of increasingly responsible experience involving cybersecurity audit and review, network planning, design, development and modification.

Licenses and Certifications:

- Some positions may require possession of a valid California Driver's License and a satisfactory driving record to be maintained throughout employment.

Knowledge of:

- Principles of providing functional direction and training.
- Principles and techniques for working with groups and fostering effective team interaction to ensure teamwork is conducted smoothly.
- Advanced principles, theories and techniques of network design and cyber security practices, cybersecurity frameworks and penetration testing methodologies.
- Incident response methodologies, including detection, analysis, containment, eradication, and recovery.
- Developing and enforcing security policies, procedures, and standards.
- Record keeping and filing principles and practices.
- Disaster recovery and business continuity best practices.
- Applicable federal, state, and local laws, codes, and regulations as well as industry standards and best practices pertinent to the assigned area of responsibility.
- Mandated safety rules, regulations, and protocols.
- Techniques for providing a high level of customer service by effectively dealing with the public, vendors, contractors, and Office 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:

- Plan, organize, and coordinate the work of assigned staff.
- Effectively provide staff leadership and work direction.
- Design, implement, and manage security technology tools to improve the overall cybersecurity posture of the Office.
- Identify and deploy controls and resolutions to system vulnerabilities emerging from legacy system configurations and/or configuration oversight.
- Analyze network needs and develop network plans, projects and specifications to address improvements.
- Audit network systems to ensure proper security, operation and performance; design remediation plans as needed.
- Analyze complex security incidents and vulnerabilities and implement effective solutions.
- Document security policies, reports, and deliver security awareness training.
- Understand, interpret, and apply all pertinent laws, codes, regulations, policies and procedures, and standards relevant to the work performed.
- Use tact, initiative, prudence, and independent judgment within general policy and procedural guidelines.
- Independently organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- 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.
- Effectively use computer systems, software applications relevant to work performed, and modern business equipment to perform a variety of work tasks.

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; to operate a motor vehicle and visit various SMCOE sites; vision to read printed materials and a

computer screen; and hearing and speech to communicate in person and over the telephone. This is primarily a sedentary office classification although standing in work areas and walking between work areas may be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to lift, carry, push, and pull materials and objects up to 10 pounds.

ENVIRONMENTAL CONDITIONS

Employees work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Employees may interact with upset staff and/or public and private representatives in interpreting and enforcing divisional policies and procedures.