PERSONNEL COMMISSION

Class Spec: 5310
Salary Range: 46 (M2)

CYBER SECURITY MANAGER

JOB SUMMARY

Under administrative direction, performs lead duties in the design, installation, configuration, and operation of cyber security solutions to protect all physical and digital assets; monitors, troubleshoots, and responds to incidents of hardware and software related to cyber security solutions, and end-point client protection systems; provides lead technical support to other technology staff regarding cybersecurity concerns.

EXAMPLES OF DUTIES

The classification specification does not describe all duties performed by all incumbents within the class. This summary provides examples of typical tasks performed in this classification.

- Perform a variety of specialized duties in the installation, configuration, maintenance and operation of the District's cyber-security prevention, on-premise and cloud network, firewalls, access control permission, and related equipment; assure compliance with applicable laws, codes, rules and regulations. ***E***
- Lead projects and collaborate with team members and clients to review and assess Information Technology (IT) environments, internal and external risks, and controls and provide relevant cybersecurity and IT security subject matter advice, findings, and recommendations. ***E***
- Research, evaluate, demonstrate, recommend and implement cybersecurity systems, processes and products such as VPN, IDS/IPS and Endpoint security. ***E***
- Work in collaboration with county specialists in cyber security and information technology departments, District consulting partners, and immediate supervisor to implement security and network best-practices. ***E***
- Assist in a coordinated response to cyber-incidents; identify threats and develop suitable defense measures; respond immediately to emergencies; evaluate system changes for security implications, and recommend enhancements. ***E***
- Provide advisory assessments in relation to cybersecurity breach prevention. ***E***
- Lead or assist in the development of District-wide privacy program governance components, including policies, procedures, standards, frameworks, and notices, for customers and support staff. ***E***
- Perform vulnerability, risk, and penetration assessment tests of District’s hardware, software, and cloud solutions that are aligned to industry security framework standards (i.e. CIS, NIST, ISO, etc.). ***E***
- Assess and implement 24/7 monitoring and security alerting tools including aggregation of system logs regarding network infrastructure and software services. ***E***
- Perform gap assessments of application/system disaster recovery plans. ***E***

- Train and assist District staff on cyber security prevention, software applications, hardware systems, and cloud solutions to support district-wide instructional and business operations. ***E***
- Assess Business Continuity Preparedness and as needed assist in the preparation of Tabletop Exercises. ***E***
- Investigate, assess, and report findings of daily cybersecurity events and incidents. ***E***
- Create and document practices and procedures to address cyber security issues. ***E***
- Provide operational support for security technologies implemented. ***E***
- Lead project meetings, status updates, training sessions and other events as needed. ***E***
- Transports small equipment to and from various district locations. ***E***
- Perform related duties as assigned.

Note: At the end of some of the duty statements there is an italicized "E" which identifies essential duties required of the classification. This is strictly for use in compliance with the Americans with Disabilities Act.

DISTINGUISHING CHARACTERISTICS

A Cyber Security Manager designs, installs, configures, and manages the District-wide cyber security system and policies to protect all physical and digital assets. Incumbents are expected to investigate, assess, and document any threats or breaches of data and formally report incidents to departments or administrators as needed. The position is expected to also be responsible for the training and support to District staff regarding any cyber security software applications or hardware as necessary.

Incumbents in this class perform a wide scope of complex duties and responsibilities in the establishment and monitoring of a District-wide cyber security system which involves the exercise of independent judgement and a combination of implementing policies and procedures, project management, interpersonal skills, and systems analysis.

EMPLOYMENT STANDARDS

Knowledge of:

Cybersecurity concepts, threats, proactive principles, strategies, and best practices.
Techniques, frameworks and methodologies of cyber security including: Data protection and DLP, MFA, NIST or similar Framework assessment and recommendations working with vCISO.
MS-ISAC MDBR implementation and MS-ISAC NSCR Reviews.
Incident response plan design and testing.
Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS).
Internal and External PEN testing.
Ransomware prevention.
Compromised workstation identification methods and mitigation protocols.
Microsoft 365 suite products and capabilities.
Fulfilling litigation requests/holds and responding to Public Records Act requests.
Methods and techniques of developing cyber security process models and determining best practices.

Principles and practices of providing quality customer service.
Principles and practices of supervision and training.
Principles of financial analysis and accounting including budget preparation and control.
Governmental procurement policies and purchasing services.
Writing skills to prepare clear and concise specifications.
Interpersonal skills using tact, patience and courtesy.
Applicable laws, codes, rules and regulations.
Record-keeping techniques.
Public speaking techniques.
Oral and written communication skills.

Ability to:

Plan, manage and oversee the District-wide cyber security systems, processes and products.
Establish cyber security policies and procedures based on industry best practices and standards, including systems, documentation, procedures, checklists and forms.
Determine and assign activities and resources for successful completion of projects.
Establish and maintain effective controls over financial, material and labor resources.
Analyze situations accurately and adopt an effective course of action.
Prepare and present oral and written reports and recommendations clearly, concisely and logically.
Prepare detailed project plans and documentation.
Prepare and interpret statistical computations, charts and graphs.
Conduct investigations, determine methodologies and obtain the data necessary to evaluate complex issues and recommend solutions.
Train, supervise and evaluate personnel.
Develop and prepare preliminary budgets.
Monitor and control expenditures.
Assure compliance with applicable laws, codes, rules and regulations.
Communicate effectively both orally and in writing.
Establish and maintain cooperative and effective working relationships with others.
Meet schedules and timelines.
Plan and organize work.
Operate a variety of office equipment including a computer and assigned software.
Work independently with little direction.
Prepare and deliver oral presentations.

Education and Training:

Bachelor’s degree in computer science, information technology, business administration or a related field.

Experience:

Four years of information technology cyber security experience. Experience in an educational environment is preferred.

Two years additional experience may be substituted for two years of the required education.

Any other combination of training and experience that could likely provide the desired skills, knowledge or abilities may be considered.

SPECIAL REQUIREMENTS

Applicants must provide proof of certification in two or more industry recognized security standards issued by an authorized agency at the time of application and maintain certification throughout employment in this classification

Positions in this classification require the use of a personal automobile and possession of a valid California Class C driver's license.

WORKING ENVIRONMENT

Office environment.
Driving a vehicle to conduct work.
Occasional evening and variable hours.

PHYSICAL DEMANDS

Dexterity of hands and fingers to operate a computer keyboard.
Hearing and speaking to exchange information and make presentations.
Sitting for extended periods of time.
Seeing to read a variety of materials.
Bending at the waist, kneeling and crouching to inspect work.

AMERICANS WITH DISABILITIES ACT

Persons with certain disabilities may be capable of performing the essential duties of this class with or without reasonable accommodation, depending on the nature of the disability.

APPOINTMENT

In accordance with Education Code Section 45301, an employee appointed to this class must serve a probationary period of one year during which time an employee must demonstrate at least an overall satisfactory performance. Failure to do so shall result in the employee's termination.

PCA: 03/23/2023