LONG BEACH UNIFIED SCHOOL DISTRICT | PERSONNEL COMMISSION *Excellence and Equity*

Class Code: 05339
Salary Range: 55 (M2)

INFORMATION SECURITY OFFICER

JOB SUMMARY

Under administrative direction, plan, organize, control and direct the District's cybersecurity and data privacy programs and operations; assure information assets, applications, systems, infrastructure, and processes are protected in the digital ecosystem in which the District operates and cybersecurity measures comply with statutory and regulatory requirements regarding information confidentiality, integrity, and availability; perform related duties as assigned.

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.

- Plan, organize, control and direct the District's cybersecurity and data privacy programs and operations; assure compliance with applicable laws, codes, rules, and regulations. ***E***
- Facilitate an information security governance structure in alignment with existing District technology governance programs, including the formation of an information security steering committee or advisory board. ***E***
- Develop, socialize and coordinate approval and implementation of cybersecurity policies. ***E***
- Provide regular reporting on the status of the information cybersecurity program to the Chief Technology Officer, Superintendent of Schools, and the Board of Education in support of student outcomes. ***E***
- Work with procurement and legal representatives to assure information security and privacy requirements are included in contracts and third-party data sharing is compliant with applicable laws and regulations. ***E***
- Establish an information security awareness training program for employees, contractors, and other approved system users; establish metrics to measure the effectiveness of security training programs for the different audiences. ***E***
- Continually assess the District's cybersecurity maturity model and cyber risk posture and develop continuous improvement plans. ***E***
- Develop an information security vision and strategy aligned to organizational priorities and enable and facilitate the District's business objectives; assure senior stakeholder buy-in and mandate. ***E***
- Direct the information security function across the District to assure consistent and high-quality information security management in support of the business goals. ***E***
- Direct the work of staff and contractors, including the work of project teams engaged in designing, configuring, implementing, and monitoring the District's cybersecurity controls systems. ***E***

- Design the District's cybersecurity controls systems in accordance with applicable frameworks such as National Institute of Standards and Technology (NIST) 800-53, Center for Internet Security (CIS) and Internal Standardization Organization (ISO) 27001. ***E***
- Oversee the development and implementation of cybersecurity controls to assure the confidentiality, integrity, and availability of confidential data that is stored and retrieved online including student data, employee data, health information, and payment information. ***E***
- Supervise and evaluate the performance of assigned staff; interview and select employees and recommend transfers, reassignment, termination, and disciplinary actions. ***E***
- Test, evaluate and recommend new and emerging technologies for consideration and adoption into District technology systems; direct the implementation of innovative technologies and procedures for technology systems. ***E***
- Conduct cybersecurity reviews of new and existing information systems, data products, and instructional applications; recommend fitness for use and/or develop risk acceptance criteria. ***E***
- Provides clear risk mitigating directives for information systems owners, including the application of controls. ***E***
- Oversee and review system specifications, bids, and Requests for Proposals to assure technical requirements and standards are met; make presentations and provide recommendations to the Chief Technology Officer regarding the purchase of cybersecurity services and tools. ***E***
- Communicate with business leaders, legal, auditors, contractors, technology service providers, staff and other outside organizations to coordinate program activities, conduct investigations, incident response, resolve issues and exchange information. ***E***
- Develop and prepare preliminary budgets for assigned functions; analyze and review budgetary and financial data; authorize and control expenditures in accordance with established limitations. ***E***
- Prepare or direct the preparation and maintenance of a variety of records and files and prepare reports related to assigned activities; prepare data for a variety of reports. ***E***
- Participate in and attend a variety of meetings, workshops, conferences, and training to maintain current knowledge of emerging cybersecurity trends; make presentations regarding cybersecurity program objectives, plans, and achievements. ***E***
- Operate a variety of office equipment including a computer and assigned software; drive a vehicle to conduct work and visit sites. ***E***
- Perform related duties as assigned.

DISTINGUISHING CHARACTERISTICS

The Information Security Officer is distinguished from other information technology classes in that it requires specialized subject matter knowledge and experience in establishing and managing cybersecurity and data privacy programs and operations for a large enterprise to assure information assets and associated applications, systems, infrastructure, and processes are adequately protected in the digital ecosystem in which the District operates. The Information Security Officer sits outside of traditional IT

infrastructure operations and DevOps but manages information security operations and incident response, including coordination with third parties.

EMPLOYMENT STANDARDS

Knowledge of:

Information security principles, practices, and procedures.
NIST and CIS cyber security controls frameworks.
California Privacy Rights Act (CPRA), Family Educational Right and Privacy Acts (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Children's Internet Protection Act (CIPA), Payment Card Industry Data Security Standards (PCI-DSS), and other relevant privacy and information security laws and regulations.
Cybersecurity risk assessment techniques.
Cybersecurity software and tools including next generation firewall (NGFW), web application firewall (WAF), security incident and event management (SIEM), endpoint detection and response (EDR), data loss prevention (DLP), and virtual private network (VPN).
Identity management and user access controls, including authentication, authorization, and encryption technologies.
Vulnerability management.
Digital forensics techniques for investigating cybersecurity incidents.
Contract and vendor management.
Principles of administration, employee supervision, and training.
General principles and practices of government purchasing and contract administration.
Strategic planning and project management techniques.
Records management and e-discovery techniques.
Report preparation techniques.
Oral and written communication skills.
Interpersonal skills using empathy, self-awareness, and positivity.

Ability to:

Plan, organize, control and direct the District's cybersecurity and data privacy programs and operations.
Prepare and present oral and written reports and recommendations clearly, concisely and logically to a variety of audiences.
Maintain current knowledge of industry trends and technological advances in the field.
Prepare detailed project plans and documentation.
Analyze and interpret data.
Analytically and logically evaluate information, propositions, and claims.
Make decisions and choose optimal courses of action in a timely fashion.
Understand, interpret, and assure compliance with applicable laws and regulations.
Respond positively to change and modify behaviors as situations require.
Focus on details of work content, processes, and products.
Conduct work with integrity and ethics.
Develop and maintain trust through honesty and personal accountability.

Design and manage processes and procedures that can be executed by and through others.
Work collaboratively with others to achieve shared goals.
Engage effectively in dialogue with a variety of stakeholders.
Communicate effectively both orally and in writing.
Establish and maintain cooperative and effective working relationships with others.
Maintain composure to identify and resolve conflicts.
Train, supervise and evaluate assigned personnel.

Education and Training:

Bachelor's degree in cybersecurity, computer science, engineering, information systems management, software engineering or a related field. A Master's degree is preferred.

Valid Certified Information Systems Security Professional (CISSP) certification.

Experience:

Five years of cybersecurity management-level experience in a large user environment, including two years of experience providing cybersecurity services in a regulated industry with one or more of the following information security compliance objectives (FERPA, HIPAA, PCI-DSS, CJIS, CPPA).

Experience in a public K-12 educational environment is preferred.

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

Any other combination of education, training and experience, which demonstrates that the applicant is likely to possess the required skills, knowledge or abilities, may be considered.

SPECIAL REQUIREMENTS

The following certifications are desirable:

Certified Information Security Manager (CISM).
GIAC Information Security Officer (GISO)
GIAC Security Leadership Certification (GSLC)

Positions in this class 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.
Evening and variable hours.
Emergency call out.

PHYSICAL DEMANDS

Dexterity of hands and fingers to operate a computer keyboard.
Seeing to read a variety of materials.
Sitting or standing for extended periods of time.
Hearing and speaking to exchange information in person and on the telephone.
Bending at the waist, kneeling, or crouching.
Reaching overhead, above the shoulders and horizontally.

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 (1) 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: 10/17/2024