LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
Class Code 1231
Senior Management

DEPUTY CHIEF INFORMATION SECURITY OFFICER

DEFINITION

Assists the Chief Information Security Officer in securing the District's information security infrastructure by directing, planning, and overseeing the development and implementation of enterprise-wide security design, controls, protocols, policies and resiliency plans for the District's applications, databases, computing devices and websites.

TYPICAL DUTIES

- Directs the day-to-day administration and operations of the information technology departments responsible for District security and device, identity and information management.
- Builds, develops and directs the implementation and monitoring of a comprehensive information security program and framework based on industry standards which includes policies, compliance, risk management, and training to mitigate cybersecurity hacks, breaches, attacks, and threats.
- Collaborates with security, network, and software application architecture teams to ensure compliance to changing regulations and technical standards.
- Manages the availability, confidentiality, integrity and authenticity of the District during project development of information systems.
- Collaborates with the Chief Information Security Officer and executive staff to develop the District's information security program strategy while prioritizing and ensuring alignment with the District's goals and initiatives such as the protection of District information assets.
- Oversees and directs security architecture, cloud security, governance, risk and compliance, training and education and other security programs.
- Defines the blueprint and multi- agency/multi-disciplinary operational plan for defense and response, including vulnerability/risk assessment and penetration tests for applications, networks, cloud and other security risk areas
- Oversees the documentation and design of the District's cybersecurity architecture, systems, services and alignment to industry best practices and standards.
- Works with architecture teams to build synergy between security architecture, network architecture and software application architecture to ensure technology builds and designs comply with technical standards.
- Develops security standards and baselines to define required security controls and settings on all firewalls, servers, commercial applications, and networks.
- Assists the Chief Information Security Officer in ensuring appropriate processes to monitor and audit ongoing operations to detect, analyze, and correct security infractions/violations
- Oversees the monitoring of the external threat environment for emerging threats, and advises relevant stakeholders on the appropriate courses of action.
- Establishes and administers a data and systems security awareness program for all District customers to ensure they are aware of security threats, policies, and procedures necessary for the efficient and effective use of District information systems
- Liaises with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept abreast of relevant/potential threats.
- May represent the District on data and system security matters and serves as the Information Technology Services liaison with regulators, auditors, suppliers, and other outside entities.
- Performs related duties as assigned

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

The Deputy Chief Information Security Officer is responsible for assisting in the development of a strategic, comprehensive, and adaptable information security program designed to protect the District's information assets and provides the overarching strategy for District information security and acts as the Chief Information Security Officer, as required.

The Chief Information Security Officer is responsible for the development of a strategic, comprehensive, and adaptable information security program designed to protect the District's information assets and provides the overarching strategy for District information security.

The Chief Information Officer is responsible for the development of strategic, innovative information services plans and the day-to-day operations of the information services function.

SUPERVISION

The Deputy Chief Information Security Officer receives administrative direction from the Chief Information Security Officer and provides administrative direction to lower-level information technology services administrators and managers.

CLASS QUALIFICATIONS

Knowledge of:

- Security architecture, cloud security, and governance
- Broad range of IT security and risk management frameworks
- Common information security management frameworks, such as ISO/IEC 27001 and NIST Networking, application systems, Internet, Intranet, and client server operation
- IT security principles, access controls, and confidential information protection principles
- Firewall technology, remote access security, voice, data, and advanced local-area and wide-area networking technologies
- Agile (scaled) software development or other best in class development practices
- Cloud computing/Elastic computing across virtualized environments
- Information system auditing
- Encryption technologies, software, and applications
- Access control systems and methodology
- Security management practices
- Security architecture and models Law, investigation, and ethics surrounding IT security
- District business disciplines, such as finance, HR, contracts, compliance and District operations Methods of project and process control, budgeting, and cost analysis and prediction
- Principles of organization, personnel management, and progressive disciplinary procedures
- Pertinent employee and student confidentiality, safety laws, regulations, and District policies and procedures

Ability to:

- Develop long and short-range plans
- Think innovatively, lead and motivate cross functional interdisciplinary teams
- Work with vendors, negotiate and manage vendor services
- Recognize, analyze, and deal effectively with problems and issues
- Communicate clearly and effectively both orally and in writing
- Work effectively with District personnel, the public, and representatives of manufacturers and other organizations
- Reviews contracts, service level agreements and other documents to verify they meet information security needs and requirements

Work well under pressure of multiple priorities and short deadlines Manage through direct reporting personnel
Supervise, train, and evaluate the work of direct and non-direct reporting personnel

Special Physical Requirement:

Effective vision to review and resolve network security issues via computers promptly.

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university, preferably with a major in computer science, telecommunications management, electrical engineering, business management or related field. An advanced degree in the aforementioned areas is highly preferable.

Experience:

Four years of executive or management level experience in systems security, preferably with two years of experience in systems security management in a K-12 and/or university setting. The experience must have included telecommunications and networking security, application and systems security, application development security, user authentication and authorization management, information systems vulnerability assessment and physical data security. Experience with training in systems analysis and information/telecommunications security is highly preferable.

Special:

Possession of the Certified Information Systems Security Professional (CISSP) or equivalent is required. The following security certifications or equivalent are preferable:

GIAC Certified Information Security Officer (GISO)
GIAC Security Leadership Certification (GSLC)
GIAC Certified Firewall Analyst (GCFW)
GIAC Systems and Network Auditor (GSNA)

A valid driver's license to legally operate a motor vehicle in the State of California and the use of a motor vehicle.

SPECIAL NOTE

An employee in this class may be subject to the reporting requirements of the District's Conflict of Interest Code.

This class description is not a complete statement of essential functions, responsibilities, or requirements. Entrance requirements are representative of the minimum level of knowledge, skill, and/or abilities. To the extent permitted by law, management retains the discretion to add or change typical duties of a position at any time, as long as such addition or change is reasonably related to existing duties.

New Class
04-06-23
JAP