LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
Class Code 1227
Senior Management

CHIEF INFORMATION SECURITY OFFICER

DEFINITION

Directs, plans, and oversees 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

- Leads and oversees the information technology departments responsible for District security and device, identity and information management.
- Designs, develops, implements, monitors, and maintains a strategic, comprehensive enterprise-wide information security program for the District that incorporates policies, compliance, risk management, and training to mitigate cybersecurity hacks, breaches, attacks, and threats.
- Ensures scalability and adaptability of program to changing compliance regulations.
- Ensures the availability, confidentiality, integrity and authenticity of District information by designing, establishing and enforcing security standards, policies, and processes during project development of information systems.
- Collaborates with executive staff to establish the District's risk acceptability, develops a District-wide security program to ensure the protection of District information assets and designs measures to rate program success
- Oversees the system updates for District communications, information systems and network infrastructure to assess for and ensure implementation of suitable security measures.
- Serves as the District expert on security policy and protocols, cybersecurity incident and response, security compliance, and security related disaster recovery and business continuity.
- Advises executive staff on appropriate execution of decisions related to security attacks, breaches, incidents and threats.
- Advises external District partners on the District's security requirements and standards.
- Ensures vendors and other business partners meet security requirements
- Contributes to varied security policy areas across the District, including risk management, HR management, governance and other areas of District business operations to ensure incorporation of appropriate security controls.
- Monitors various state, federal, and industry security resources for emerging threats, evaluate their impact to the District, and make appropriate countermeasure strategy recommendations to management.
- Participates in IT Change Control meetings ensuring District policies and information security is maintained and assist with the evaluation of emerging technologies.
- Evaluates District initiatives for security risk/reward based on financial investments
- May make presentations to the Board of Education, executive staff and external stakeholders regarding District information security.
- Performs related duties as assigned

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

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 Director of IT, Security is responsible for the development and implementation of computer network security procedures for the information services function.

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

Administrative direction is received from the Chief Information Officer. Administrative direction is provided to lower-level information technology services administrators and managers.

CLASS QUALIFICATIONS

Knowledge of:

- 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
- Utilize a wide variety of computers, operating systems, networks, and telecommunications systems
- Think innovatively, lead and motivate cross functional interdisciplinary teams
- Enter and retrieve information using computers
- Work with vendors, negotiate and manage vendor services
- Recognize, analyze, and deal effectively with problems and issues
- Prepare reports and write clearly, concisely, and convincingly
- Speak clearly, concisely, and effectively
- 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
- Utilize the full range of subordinates' skills
- Supervise, train, and evaluate the work of direct and non-direct reporting personnel
- Promote equal opportunity in employment and maintain a work environment that is free of discrimination and harassment Maintain confidentiality.

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:

Six years of executive or management level experience in systems security, preferably with two years 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 and at least one of the following security certifications or equivalent is required:

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
11-18-22
RGK/LKD