LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
Class Code 4810
Management

DIRECTOR OF IT, SECURITY

DEFINITION

Plans, develops, and manages data, systems, and network security standards, procedures, and guidelines throughout the District.

TYPICAL DUTIES

- Plans, develops, and manages data systems, and network security standards, and procedures, throughout the District.
- Manages computer network security regarding multiple local area networks connected to a wide area network.
- Collaborates with the business area management to identify primary risk exposures and ensure the existing security architecture appropriately addresses and mitigates the exposure.
- Coordinates with all other IT functional areas to provide guidance and direction for the inclusion of appropriate security and access controls in hardware and software systems.
- Ensures appropriate processes to monitor and audit ongoing operations to detect, analyze, and correct security infractions/violations.
- Coordinates with District legal counsel, auditors, and business area management to identify all District employee, business partner, and regulatory agency data and security requirements necessary for the protection of District information.
- Establishes security policies and practices for the protection of confidential student and employee information on District information systems.
- Develops security standards and baselines to define required security controls and settings on all firewalls, servers, commercial applications, and networks.
- Directs vulnerability assessment of critical District information systems and recommends remediation and mitigation strategies as appropriate.
- Directs the management of user authentication and authorization for District Enterprise information systems.
- Establishes network intrusion detection monitoring systems.
- Establishes protocols for investigating intrusion attempts.
- Directs the development, acquisition, implementation, and administration of information system security hardware and software on the District's wide area networks, local area networks, mainframes, minicomputers, and personal computers.
- 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.
- Represents the District on all data and system security matters and serves as ITD's liaison with regulators, auditors, suppliers, and other outside entities.
- Provides advice and guidance to the Chief Information Officer relative to data and system security matters.
- Manages the budgeted resources for the security branch to optimize their use in satisfying the overall objectives of the Division.
- Evaluates staff performance and conducts progressive discipline procedures when needed.
- Interprets and applies provisions of collective bargaining agreements.
- Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

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.

A Network Security Administrator supervises and/or participates in the analysis, installation, upgrading, and monitoring of the security infrastructure including firewall systems, VPN systems, content filtering hardware and software, intrusion detection devices, and associated systems.

SUPERVISION

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

CLASS QUALIFICATIONS

Knowledge of:

- 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
- Information systems 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
- 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
- Enter and retrieve information using computers
- 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
- 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 nondirect reporting personnel
- Promote equal opportunity in employment and maintain a work environment that is free of discrimination and harassment
- Maintain confidentiality

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 or related field. An advanced degree in electrical engineering or computer science is highly preferable. Additional experience in supervising network security may be substituted for the required education on a year-for-year basis.

Experience:

Five years of professional-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:

A valid California Driver License.
Use of an automobile.
Possession of at least one of the following security certifications or equivalent is required:
Certified Information Systems Security Professional (CISSP)
GIAC Certified Information Security Officer (GISO)
GIAC Security Leadership Certification (GSLC)
GIAC Certified Firewall Analyst (GCFW)
GIAC Systems and Network Auditor (GSNA)

SPECIAL NOTES

1. Management class, exempt from bargaining units.
2. 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. Requirements are representative of the minimum level of knowledge, skill, and/or abilities. Management retains the discretion to add or change typical duties of the position at any time.

Revised
12-09-13
PJO