LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
CLASS CODE 4799
Unit D

INFORMATION SECURITY ANALYST I

DEFINITION

Performs analysis and security reviews of information systems to identify, document, and mitigate vulnerabilities to ensure that systems meet security requirements to protect information assets.

TYPICAL DUTIES

Develops and maintains security configuration baselines for a broad range of IT assets that support District operations and identifies any unsecure deviations requiring mitigation.

Ensures that all configuration changes resulting from critical security patches released by software and hardware vendors are complete, accurate, and timely.

Reviews government, vendor, and private and open source vulnerability databases to identify and evaluate relevant software flaws, server misconfigurations, common vulnerabilities, and impact metrics for IT assets in accordance with District policies, IT operations, and information security standards.

Maps all known vulnerabilities to asset owners and business functions and produce monthly baseline reports with remediation recommendations and any unapproved changes that should be investigated.

Maintains an internal database of discovered vulnerabilities and their resolution targeting IT assets that support District-wide processes.

Conducts proactive activities to discover physical security IT assets vulnerabilities in District facilities and building systems.

Develops, maintains, and distributes a centralized vulnerability remediation schedule based on severity across the District and coordinates with stakeholders for planning.

Designs and develops cybersecurity awareness newsletters, email messages, videos, presentations, and other content for use in training students and school staff on how to protect information assets.

Trains non-technical employees and other stakeholders to be aware of common attack techniques and methods to safely use of the internet, email, network, and other District resources

Identifies and prioritizes training issues by location and user group by periodically sending simulated phishing emails to a sample of randomly selected District network users.

May transport equipment between data centers, central offices, and other job sites.

Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

An Information Security Analyst I perform a variety of technical assignments in an effort to protect information assets by testing and evaluating systems; identify and document vulnerabilities, and raises awareness of information security initiatives and practices.

The Information Security Risk Manager conducts comprehensive assessments of IT assets and services to identify and manage risks that may negatively impact the delivery of IT services and interrupt District operations.

An Information Security Analyst II plans, administers, reviews, and analyzes incident response processes of the District including policies, procedures and standards for compliance to ensure the District’s security posture is adequate.

SUPERVISION

General supervision is received from the Information Security Risk Manager. Work direction may be exercised over lower level personnel.

CLASS QUALIFICATIONS

Knowledge of:

Concepts, procedures, and controls relating to information security frameworks (e.g. ISO 27001), open-source vulnerability databases, antivirus, access control, identity management, and cryptography
Core IT infrastructure management tools including Microsoft Active Directory Domain Services, LDAP, DNS, Certificate Services
Essential components of each IT architecture layer including core IT infrastructure layer, applications layer, network layer, computing layer, physical layer, and storage layer
Vulnerability scanning tools including but not limited to Nessus, SecurityCenter, AppDetective, and WebInspect
Microsoft Windows operating system and relevant software

Ability to:

Perform complex analysis of threat trends, vulnerability, and intrusion detection systems
Troubleshoot and resolve information security issues in an efficient and effective manner
Exercise good judgment in making decisions
Formulate innovative recommendations for process improvement and enhance organizational effectiveness
Communicate effectively both verbally and in writing
Problem solve and work within established timeframes to deliver timely results
Establish and maintain effective working relationships with District personnel and the public
Maintain confidentiality have impartial and objective views

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university with a bachelor’s degree, preferably in information security, information systems, information technology, computer science, software engineering, or a related field. Qualifying experience in addition to that required may be substituted on a year-for-year basis provided that the requirement of a high school diploma or equivalent is met.

Experience:

Two years of experience in an IT data center, operating systems and/or IT security environment performing information security tasks such as monitoring systems, configuration and change management, training and awareness, systems analysis, and/or other information security responsibilities. One year of the above experience must have included experience in vulnerability management.

Special:

A Comp TIA Security+, GIAC Information Security Fundamentals (GISF), ISACA Cybersecurity Fundamentals (CSX), Certified Vulnerability Assessors (CVA) certification, or equivalent certification is preferred.
A valid driver’s license to legally operate a motor vehicle in the State of California and the use of an automobile.

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.

Revised
06-15-23
MCV