

INFORMATION SECURITY ENGINEER

JOB SUMMARY

Under administrative direction, plan, implement, monitor and manage cybersecurity incident response, security engineering and vulnerability management across the District; research, develop, implement and maintain security standards across District systems; evaluate emerging threats, recommend mitigations and determine acceptable levels of exposure; 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, implement, monitor and manage cybersecurity incident response, security engineering and vulnerability management across the District; assure operational activities align with broader security requirements and compliance obligations. **E**
- Research, develop, implement and enforce security standards across District systems, translate District-wide security objectives into actionable strategies with clear, defined action steps; manage the implementation of security technologies and controls. **E**
- Respond to security incidents by analyzing logs, threat intelligence, and other sources of information; analyze alerts generated by security tools to reduce false positives and increase alert effectiveness. **E**
- Conduct root cause analysis to identify process or technology gaps from security incidents; provide remediation recommendations and directly take action in the needed systems to mitigate risk. **E**
- Serve as a liaison with District departments to track and monitor incident response status updates; document and track security alerts and incidents using internal standard tracking processes and platforms. **E**
- Develop, document, and report business-level metrics for incident response progress; develop reports, dashboards, and data visualizations as requested for District leaders and others. **E**
- Serve as a risk advisor to IT leadership by identifying and evaluating emerging cybersecurity threats, vulnerabilities, and risks to critical systems and data; support District leadership in determining acceptable levels of risk. **E**
- Identify opportunities to improve security operations through process improvements and automation across vulnerability management, technology, incident response, and related areas; collaborate with technology partners and cross-functional teams to implement and operationalize improvements. **E**
- Proactively identify and integrate threat intelligence into vulnerability management and incident response technologies and processes to enhance detection, response, and mitigation capabilities. **E**

- Install, configure, and maintain security systems and technologies such as EDR, email, firewall, WAF, VPN, SIEM, DLP, and IAM; support infrastructure operations teams in the running of security tools deployed in the environment. *E*
- Create and oversee vulnerability scanning jobs and assessment tasks within a variety of security tools for infrastructure and application; identify and resolve false positive findings in assessment results. *E*
- Serve as a point of contact on issues, dependencies, and risks related to vulnerability scanning and threat intelligence alerts; support information security risk management activities, recommend security controls, corrective and preventative actions to mitigate vulnerability risks. *E*
- Report and track the vulnerability life cycle from discovery to closure; review vulnerabilities and work with infrastructure and business teams to remediate the findings. *E*
- Research and provide guidance for addressing vulnerabilities, including system patching, deployment of specialized controls, standards, or infrastructure changes, and changes in development processes. *E*
- Communicate with contractors, technology service providers, staff and other outside organizations to coordinate information security activities, resolve issues and exchange information. *E*
- Supervise and evaluate the performance of assigned staff; interview and select employees and recommend transfers, reassignment, termination, and disciplinary actions. *E*
- Prepare a variety of records and files and prepare narrative and statistical reports and documentation related to assigned activities; prepare data for a variety of reports; review and update incident response standard operating procedures and playbooks. *E*
- Participate in and attend a variety of meetings, workshops, conferences, and training to maintain current knowledge of emerging industry trends; make presentations regarding cybersecurity program objectives, plans, and achievements. *E*
- Participate in developing the District's long-range technology strategic plans; serve on assigned steering committees. *E*
- Operate a variety of office equipment including a computer and assigned software. *E*
- Respond to after-hours emergency calls and coordinate response. *E*
- Perform related duties as assigned.

Note: At the end of some of the duty statements there is an italicized "E" which identifies essential duties required of the classification. This is strictly for use in compliance with the Americans with Disabilities Act.

DISTINGUISHING CHARACTERISTICS

Incumbents in the Information Security Engineer classification are responsible for defining, implementing, and maintaining the District's overall information security posture. This role requires expertise in multiple security domains including threat detection, vulnerability management, identify and access control and incident response. Incumbents exercise a high degree of initiative and independent judgment to safeguard District assets, ensure regulatory compliance, and maintain trust in the confidentiality, integrity and availability of critical information systems.

EMPLOYMENT STANDARDS**Knowledge of:**

Security principles, frameworks, and best practices (e.g., NIST, ISO 27001, CIS Controls).
Threat modeling, risk assessment, and vulnerability management such as vulnerability scanner, network firewalls, cloud-native security and penetration testing frameworks.
Threat landscape and intelligence feeds to identify and triage threats and vulnerabilities.
Incident detection, response, investigation and forensics methods and techniques.
SIEM platforms (e.g., Splunk, ELK, Sentinel) and log analysis.
Endpoint protection, EDR/XDR tools, and malware analysis basics.
TCP/IP, DNS, HTTP/S, VPNs, firewalls, and IDS/IPS.
Securing cloud environments across AWS, Azure and GCP, including implementation of IAM, VPCs, and security groups.
Zero trust architecture and network segmentation.
PKI, TLS, and encryption technologies.
Web application security (OWASP Top 10, API security).
Secure coding practices and DevSecOps integration.
Linux/Unix and Windows hardening.
SSO, MFA, RBAC, and PAM solutions.
Conditional access policies.
Active Directory/Azure AD security configurations.
Principles of supervision and training.
Applicable laws, codes, rules and regulations.
Strategic planning and project management techniques.
Public speaking techniques.
Record-keeping and report preparation techniques.
Oral and written communication skills.
Interpersonal skills using tact, patience and courtesy.

Ability to:

Plan, implement, monitor and manage cybersecurity incident response, security engineering and vulnerability management across the District.
Research, develop, implement and enforce security standards across District systems.
Present technical information effectively to both technical and non-technical audiences.
Apply cybersecurity tools and techniques to streamline incident response, improve detection, and strengthen overall security posture.
Design, configure and maintain information security systems and tools, including firewalls, EDR/XDR platforms, SIEM/SOAR platforms, IAM platforms, scanning tools, etc.
Conduct or support penetration testing and static/dynamic code analysis.
Become proficient in at least one scripting language (e.g., Python, PowerShell, or Perl) to automate security tasks and improve operational efficiency.
Supervise and evaluate the performance of assigned personnel.
Make sound decisions by evaluating risks, costs, and benefits to identify the most appropriate and effective course of action.
Communicate effectively both orally and in writing.

Establish and maintain cooperative and effective working relationships with others.
Prepare and deliver oral presentations.
Maintain confidentiality of sensitive and privileged information.
Maintain current knowledge of technological advances in the field.
Plan and organize work.
Operate a computer and assigned software.

Education and Training:

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

Experience:

Three years of experience in information security or information technology operations including responsibility for cybersecurity operations. Experience with scripting and automation tools such as PowerShell or Bash is desirable.

OR

Three years of experience as a Network Specialist with the Long Beach Unified School District.

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

Incumbents in this classification must possess and maintain throughout employment in this classification, at least one (1) of the following certifications:

- CompTIA Security+
- SSCP (Systems Security Certified Practitioner)

The following certifications are preferred:

- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Security Auditor)
- SANS GIAC (Global Information Assurance Certification)
- AWS Certified Security (Amazon Web)
- Cisco (CCNA or CCNP)
- Google Cloud
- Microsoft Azure

WORKING ENVIRONMENT

Office environment.
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.