## Job Description

| Title: Cybersecurity Engineer | FLSA Status: Non-Exempt | Months: 12 |
|---|---|---|
| Supervisor: Manager-Information Technology | Supervises: N/A | Range: 40 |
| Department: Information Technology | Bargaining Unit: Classified | Approved: 5/14/2026 |

**JOB SUMMARY:**

Under the direction of the Manager-Information Technology, Cybersecurity Engineer is responsible for planning, developing and maintaining a comprehensive, enterprise-wide cybersecurity program to protect electronic data and network infrastructure from external and internal security breaches, data loss, and privacy violations; ensuring cybersecurity measures taken are in compliance with statutory and regulatory requirements regarding information access, security, and privacy; and providing cybersecurity services to Lakeside Union School District sites. This role also develops and enforces policies for Artificial Intelligence (AI) use, ensuring compliance with security best practices and district regulations. The Cybersecurity Engineer manages special projects related to cybersecurity improvements, incident response, and emerging technologies.

This position provides direction, training, and oversight to ensure security measures are effectively implemented.

**ESSENTIAL DUTIES AND RESPONSIBILITIES:**

**Security Operations**

- Monitor the district's security infrastructure, including firewalls, intrusion detection systems (IDS), endpoint protection, email security, and network traffic.
- Respond to cybersecurity incidents, conduct investigations, and ensure timely remediation.
- Review security logs, alerts, and reports from various tools, (SIEM, antivirus, endpoint detection & response).
- Enforce access control policies, ensuring only authorized personnel can access critical systems.
- Work with IT staff to patch and update systems, reducing vulnerabilities.
- Conduct routine vulnerability scans and penetration tests to identify security weaknesses.
- Ensure the security of student, teacher, and administrative data in compliance with FERPA, COPPA, and other regulations.
- Manage endpoint security solutions, ensuring all district devices remain protected.
- Oversee email security measures, investigating and mitigating phishing, spam, and malicious attachments.

**Network Security & Traffic Monitoring**

- Oversee network security devices such as firewalls, switches, routers, and wireless access points, ensuring they are properly configured and maintained.
- Monitor network traffic for signs of malicious activity, unauthorized access, or potential data breaches.
- Implement network segmentation and access control policies to minimize the risk of internal threats.
- Ensure VPSs, remote access solutions, and cloud security measures are properly configured and secured.
- Work with the IT team to optimize network security settings without impacting educational or administrative functions.

- Conduct network security audits, ensuring compliance with cybersecurity best practices.
- Investigate and respond to DDoS attacks, unauthorized access attempts, and other network-related threats.
- Develop and enforce wireless security policies, ensuring strong encryption and authentication methods.

**AI Use, Policy Development, and Compliance**

- Develop, implement, and enforce AI governance policies to regulate AI usage in classrooms, administrative processes, and student interactions.
- Ensure AI systems comply with privacy, ethical, and security standards.
- Collaborate with educational leadership and legal teams to establish appropriate AI use guidelines for staff and students.
- Monitor AI applications for potential data leaks, bias, and ethical concerns.
- Research and assess new AI tools to determine security risks and benefits for district use.
- Educate teachers and staff on safe and responsible AI practices.

**System & Data Backup Management for Business Continuity**

- Oversee and maintain district-wide backup solutions to ensure reliable data protection.
- Regularly test backup and recovery procedures to verify data integrity and availability.
- Ensure disaster recovery plans are in place for all critical systems and infrastructure.
- Implement and manage redundancy strategies, such as offsite backups and cloud-based recovery options.
- Collaborate with IT staff to ensure that servers, applications, and databases are backed up according to best practices.
- Respond to and coordinate data recovery efforts in the event of system failure, cyberattacks, or natural disasters.
- Work with third-party vendors to improve backup and recovery processes, ensuring compliance with district policies and regulatory requirements.

**Special Projects and Security Initiatives**

- Lead cybersecurity initiatives such as district-wide MFA implementation, zero-trust architecture, and cloud security enhancements.
- Manage incident response plans, conduct tabletop exercises, and ensure the district is prepared for cyber threats.
- Implement cybersecurity awareness training for staff, administrators, and students.
- Work with vendors and consultants on security assessments and risk audits.
- Coordinate with law enforcement and external cybersecurity agencies in cases of major security incidents or breaches.

**Team Collaboration**

- Collaborate with the Technology team, school administrators, teachers, and external security professionals to maintain a strong cybersecurity posture.
- Serve as the primary point of contact for cybersecurity-related inquiries and incidents within the district.
- Provide training and mentorship to district staff on cybersecurity best practices.

## Required Skills & Qualifications

- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field or 5+ years of combined experience in IT security, cybersecurity operations, and network security.
- Experience with firewalls, IDS/IPS, endpoint security tools, SIEM solutions, and cloud security.
- Strong understanding of AI security risks, governance, and ethical concerns.
- Knowledge of school district educational security compliance regulations (FERPA, COPPA, CIPA).
- Experience with cyber incident response, threat hunting, and risk management.
- Excellent problem-solving, analytical thinking, and decision-making abilities.

- Strong communication and ability to explain cybersecurity concepts to non-technical staff.
- Valid California Class C Driver's License.

**Preferred Certifications**

- CompTIA Security+
- CompTIA SySA+
- Google Cybersecurity or AWS Security Certification
- GIAC Security Essentials (GSEC)

**Work Environment & Conditions**

- This position requires on-site work at the school district's technology office, with occasional travel to schools for security audits and training.
- Occasional after-hours work may be necessary during security incidents, system upgrades, or special projects.

**Work Environment**

- Indoor/Outdoor/Office environment
- Interruptions
- Driving a vehicle to conduct work.

**Physical Demands**

- Hearing and speaking to exchange information
- 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.
- Bending the waist, kneeling or crouching.
- Reaching overhead, above the shoulders and horizontally.
- Lifting, carrying, pushing or pulling moderately light to heavy objects.

**Hazards**

- Potential contact with dissatisfied individuals

**Other Duties**

- Perform related duties as assigned

The information contained in this job description is for compliance with the Americans with Disabilities Act (A.D.A.) and is not an exhaustive list of the duties performed.