CYBERSECURITY ANALYST

DEFINITION:

Under direction of the Chief Technology Officer, develop, implement, maintain, monitor, and supervise new and existing cybersecurity systems, including but not limited to system monitoring, compliance, detect and response, and mitigating security threats, implementing security measures, and ensuring compliance with relevant regulations and policies for all District systems; analyze security data and develop response plans; prepare training materials and deliver trainings; collaborate with cybersecurity local, state, and federal agencies, and prepare security plans and reports as needed; and principals of effective personnel leadership, management and supervision. Perform other duties as assigned.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

- Have thorough knowledge of cybersecurity principles and network infrastructure integration and management practices.
- Monitor and Investigate; utilize advanced security tools and technologies to proactively monitor the school district's networks, systems, and applications for potential security breaches, vulnerabilities, and suspicious activities.
- Investigate security incidents, identify root causes, and develop appropriate remediation strategies.
- Threat Detection and Prevention; employ intrusion detection and prevention systems (IDS/IPS), firewalls, antivirus software, and other industry standard security measures to identify and respond to potential threats, malware, viruses, and other malicious activities. Conduct regular vulnerability assessments and penetration testing to identify and address vulnerabilities.
- Incident Response; develop and implement incident response plans, including incident escalation, containment, and remediation procedures. Respond promptly to security incidents, conduct forensic analysis, document findings, and recommend corrective actions to prevent future incidents.
- Security Awareness and Training; design and deliver cybersecurity awareness and training programs for staff, teachers, and students. Educate end-users about best practices in information security, phishing awareness, password management, and social engineering threats.
- Policy Development and Compliance; assist in the development, implementation, and enforcement of complex cybersecurity policies, standards, procedures, and guidelines. Stay updated with the evolving regulatory landscape (e.g., FERPA, COPPA) and industry best practices, ensuring the District's compliance with applicable regulations. Security
- Controls and Infrastructure; collaborate with all Technology Services teams to evaluate, implement, and maintain security controls, including but not limited to CIS controls, access controls, network infrastructure and segmentation, encryption, and authentication mechanisms. Continuously assess the effectiveness of security controls and recommend improvements as needed.

- Security Incident Reporting; prepare and present regular reports on security incidents, vulnerabilities, trends, and risk assessments. Communicate complex security issues in a clear and concise manner to non-technical staff.
- Security Audits and Assessments; conduct periodic security audits and assessments to evaluate the effectiveness of security controls, policies, and procedures. Collaborate with external vendors, auditors and regulatory bodies during security audits and provide necessary documentation and support. Continuous learning and staying updated on with the latest threats, technologies, security systems and industry standard practices.

QUALIFICATIONS:

Knowledge of

Cybersecurity and information systems, network security, operating systems, application security, secure configurations, threats and attacks, cryptography, incident response, risk management, compliance and regulations, security tools, security standards and frameworks, security awareness and training, effective data analysis, correct oral and written communication skills.

Ability to

Monitor and Investigate; utilize advanced security tools and technologies to proactively monitor the school district's networks, systems, and applications for potential security breaches, vulnerabilities, and suspicious activities. Develop plans for security and network infrastructure systems ; research, project manage, and deploy industry standard system and infrastructure security; document security and application incidents; solve complex security and network integration problems; analyze and take corrective action to ensure best practice system security and infrastructure uptime, availability and performance. Proficient knowledge of network protocols, operating systems, and security architectures. Proven incident response, including threat hunting, incident analysis, and containment. Strong analytical and problem-solving skills to identify and address security risks and vulnerabilities. Excellent written and verbal communication skills to convey complex security concepts to non-technical audiences. Ability to work independently, prioritize tasks, and handle multiple projects simultaneously. A solid commitment to maintaining confidentiality, integrity, and ethical standards in handling sensitive information.

Experience

Proven experience as a Cybersecurity Analyst, preferably in an educational environment or similar setting. In-depth knowledge of information security principles, concepts, and industry best practices. Proficiency in security tools and technologies, such as SIEM, IDS/IPS, firewalls, antivirus software, vulnerability scanners, and penetration testing tools. Progressive supervisory and management experience with full responsibility for maintaining and ensuring maximum security, network infrastructure operations and integration, systems availability and performance.

Education

Graduation from an accredited university with a bachelor's degree with specialization in Computer Science, Information Security, or a related field, or any combination of professional training or technical experience equivalent to a bachelor's degree Relevant certifications including but not limited to Certified Information Systems Security Professional "CISSP", Systems Security Certified Practitioner "SSCP", Certified Information Security Manager "CISM", or Global Assurance Certification "GIAC" are highly desirable.

Physical Performance Requirements

Considerable standing, walking, or sitting much of the time with some bending, stooping, squatting and twisting. Lifting often involved. Weight of materials will vary, with employees regularly lifting and maneuvering 20 to 30 pounds.

Licenses

Possession of a valid and appropriate California Driver's License.

Board Approval: August 3, 2023