SANTA CLARA COUNTY OFFICE OF EDUCATION
Personnel Commission

CLASS TITLE: CYBERSECURITY ENGINEER

BASIC FUNCTION:

Under the direction of the Manager - Security, Network, & Systems Engineering, designs, develops, implements and maintains a comprehensive, enterprise-wide cybersecurity program to protect the Santa Clara County Office of Education (SCCOE) systems, data, and network infrastructure from external and internal security breaches, data loss, and privacy violations; ensures that cybersecurity measures taken are in compliance with statutory and regulatory requirements regarding information access, security, and privacy; provides cybersecurity services including threat protection, incident response, and end-user training to SCCOE departments and Santa Clara County school districts.

DISTINGUISHING CHARACTERISTICS:

The Cybersecurity Engineer is highly motivated, proactive, and responsive, and must work with limited direction in a complex and rapidly evolving information technology environment. Incumbents possess a high level of technical skill, with the ability to respond quickly and effectively to security threats while providing accurate and timely incident reports and status updates to all stakeholders and IT support team members. This position requires a thorough understanding of current and emerging threats and technologies, both on-premises and in the cloud.

REPRESENTATIVE DUTIES:

The following duties are examples of assignments performed by incumbents in this classification. It is not a comprehensive list of duties, nor is it restrictive regarding job assignments.

ESSENTIAL DUTIES:

Leads the development, maintenance, and dissemination of electronic information security policies, standards, procedures, and practices for the purpose of identifying issues, developing recommendations, enhancing existing systems and/or providing solutions to current cybersecurity issues.

Designs, deploys, and manages multiple information security technology standards and procedures, including endpoint security, application security, database security, infrastructure security, and identity management solutions.

Establishes information and infrastructure security controls, including log monitoring procedures, identification of unnecessary services and applications, redundant accounts, risky applications, etc., to support system hardening and policy and procedure alignment.

Performs technical security design and review activities for the SCCOE and Santa Clara County school districts with respect to applications, networks, servers, architecture, and databases to ensure security on-premises or cloud deployments.

Resolves complex security problems or breaches; conducts and initiates security scans and audits; performs risk assessments; acts as both a technical lead and liaison for interacting with third-party vendors, forensic specialists, auditors, law enforcement, and other investigators.

Creates and delivers training on information security for IT staff and end-users to establish and oversee an institutionalized knowledge-base of current and emerging electronic information security technologies, security issues, and information privacy legislation and regulations.

Serves as a technical resource to SCCOE and Santa Clara County district staff to provide consultation, advice, and services on data security management, privacy, disaster recovery, and emergency preparedness planning.

Creates, updates, and oversees all disaster recovery and related activities including testing and validation for restoration both on premises and in the cloud.

Interprets and implements laws, regulations, policies, and procedures pertinent to cybersecurity-related incidents; collaborates with law enforcement agencies for the purpose of investigating electronic security breaches.

Conducts penetration tests to identify hardware and software assets that are vulnerable to attack; recommends and leads the implementation of countermeasures to address identified vulnerabilities.

Performs detailed technical security evaluations of information systems, solution architectures, physical security designs, vendor solicitations, contracts, and proposals to ensure that IT assets are aligned with internal and external security policies and requirements.

Communicates trending risks with SCCOE leadership and performs or provides end-user training to all staff to mitigate the risk for the human factor.

Assists and supports all SCCOE IT staff with all aspects of planning, design, development, coding, testing, debugging and implementation of complex systems administration for a variety of operating systems.

Assists with the development of bid specifications for acquisitions of network, data security, and telecommunications related equipment and services.

Promotes acceptance of security technologies within the organization, balancing business goals, security controls, and customer usability.

Operates a computer, a variety of software, and other office equipment as assigned; drives a vehicle to conduct work as assigned.

OTHER DUTIES:
Performs related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:
Information technology security standards and requirements, trends and tools, LAN/WAN networks, operating systems, and ERP systems.
Design, development, and implementation of security solutions for complex and large networks.

Firewalls, intrusion detection and prevention systems, auditing and scanning systems, VPN, and remote access systems.
Vulnerability assessment tools including but not limited to Nessus, Metasploit, and Nmap.
Specific security issues associated with common operating systems, networking, and virtualization software.
Risk and threat assessment processes and practices.
Malware including computer viruses, worms, Trojan horses, spyware, and ransomware; phishing and other social engineering strategies.
Concepts, procedures, and controls relating to CIS, ISO 27001, NIST 800, and other industry accepted Information Security frameworks.
Core security tools including, but not limited to, intrusion detection systems (IDS), security information and event management (SIEM), firewalls, and vulnerability assessment tools.
State, federal, and local laws and regulations related to cybersecurity, data privacy and protection, and data breach notification, including COPPA, FERPA, and HIPAA.
Principles, practices, and techniques of database structures and computer programming.
Change control concepts and procedures.
Project management concepts and terminology.
Incident, process, and project management applications like Cherwell, Jira, and Microsoft Project.
Proper English usage including grammar, spelling, punctuation and sentence structure.

ABILITY TO:
Maintain awareness and knowledge of contemporary standards, practices, procedures, and methods related to cybersecurity.
Understand and apply laws, regulations, policies, and procedures pertinent to cybersecurity incidents.
Effectively explain complex IT security related concepts to management and end-users using excellent presentation and communication skills.
Perform enterprise security analyses, including threat modeling, specifications, implementation, testing, and vulnerability assessment.
Organize, coordinate, and document technical vulnerability assessments, including systems and network vulnerability assessments, penetration testing, web application assessments, social engineering assessments, physical security assessments, and wireless security assessments.
Quickly respond to, diagnose, and resolve security breaches.
Clearly explain to management and show forensically how an attack was conducted or how a security breach occurred, and what steps should be taken to reduce the likelihood of similar events in the future.
Interpret technical procedures and documentation, and explain technical concepts in non-technical terms to team members, clients, and users.
Utilize computer scripting and programming languages (e.g. Python) to extend available security tools (e.g. Metasploit) while creating new custom tools designed for specific needs such as penetration testing and operating system interaction.
Maintain current knowledge of technological advances in security and related fields.
Provide leadership and technical guidance to the SCCOE, school districts, and other clients in all areas related to systems, network, and data security.
Conduct small group and end-user training.
Work under limited supervision with only occasional instruction and assistance.
Establish and maintain cooperative and effective working relationships with others.

Perform complex problem solving as well as critical thinking, using logic and reasoning to identify strengths and weaknesses to solutions and approaches.
Work with management, administrators, and other team members to solve complex challenges.
Communicate effectively in both oral and written form.

EDUCATION AND EXPERIENCE:

Any combination equivalent to: Bachelor's degree in Computer Science or a related field, and five years of progressively responsible experience in security, network design and development, computer forensics, and technology related auditing. One or more years in computer systems or programming.

LICENSES AND OTHER REQUIREMENTS:

Certified Information Systems Security Professional (CISSP) certification is desirable.

WORKING CONDITIONS:

ENVIRONMENT:
Office environment.
Evening or variable hours.
Driving a vehicle to conduct work.

Approved by Personnel Commission: September 11, 2019

Jonathan Muñoz
Director - HR/Classified Personnel Services

Date: 09/11/2019