CLASS TITLE: Security Engineer

BASIC FUNCTION:

Under the direction of an assigned supervisor, provide technical leadership, coordination and planning in support of KCCD's IT Security systems and initiatives; and design, develop, test, install, monitor, and maintain information technology (IT) security systems for the district.

REPRESENTATIVE DUTIES:

Serve as the security engineer supporting security initiatives district-wide and advising District office and College IT staff on IT Security matters. ***E***

Coordinate with District office and College IT staff in troubleshooting and resolving IT Security related support requests in a timely manner. ***E***

Coordinate team efforts to research, select, plan, implement and support effective IT Security controls, monitoring tools and practices. ***E***

Assist with performing periodic and scheduled IT security audits, vulnerability scans and/or risk assessments to identify vulnerabilities and potential threats, and recommend mitigation practices. ***E***

Conduct assessments and implements strategies for ensuring KCCD meets IT Security compliance requirements, including those associated with FERPA, PCI, and HIPAA. ***E***

Monitor security systems and identify, troubleshoot, diagnose, resolve and report IT security problems and incidents; help coordinate and conduct investigations of suspected breaches in IT Security; respond to emergency IT security situations. ***E***

Maintain vendor contacts, partnerships, and relationships related to the implementation and support of KCCD's IT security architecture and programs. ***E***

Research, recommend and facilitate adoption of IT Security Standards for KCCD IT systems and networks (e.g. servers, routers, databases). ***E***

Monitor external IT Security threat environment for emerging threats and advise on appropriate course of action. ***E***

Develop, maintain, and present IT Security awareness training for staff and faculty. ***E***

Develop and maintain documentation for KCCD's IT Security architecture and programs. ***E***

Receive, prioritize and respond to help desk service tickets for IT Security-related issues. ***E***

Develop and maintain help desk knowledge base articles for respective areas of responsibility.

Backup other IT Security, Network and Systems team members as needed.

Keep current with the latest developments in IT Security industry.

Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

A variety of IT and security concepts including several of the following:

- Multiple operating systems including recent desktop and server versions of Microsoft Windows and Redhat Linux or other Linux distributions.
- IT architecture including data centers, cloud deployment, containers, etc.
- Networking including routing and switching concepts, Ethernet, wireless networking, TCP/IP, and NetBIOS.
- Programming or scripting ability in at least one language such as Python, PHP or Powershell.
- Security Protocols including WPA/WPA2, Kerberos/AD, IPSEC, SSL/TLS, and SSH.
- Security assessment and scanning tools such as Nessus, Nmap, oclHashCat, Kali.
- Detection and monitoring tools including network-based IDS/IPS software and appliances, and endpoint detection and response software.
- Computer forensics and incident response tools and procedures.
- Security standards and frameworks such as NIST, PCI-DSS, OWASP, or CIS Critical Security Controls.
- Effective communication, documentation and writing skills.
- Effective customer service skills and practices.

ABILITY TO:

- Effectively interact and negotiate with vendors.
- Assess and remedy system performance problems.
- Troubleshoot and resolve complex hardware and software problems.
- Plan, organize, implement, and complete complex IT security projects.
- Work independently with little direction.
- Prepare and follow work plans and timelines for projects and tasks.
- Learn new skills and adapt to changes in technology.
- Communicate effectively, both orally and in writing.

- Establish and maintain cooperative and effective working relationships with others.

EDUCATION AND EXPERIENCE:

Any combination equivalent to:

Bachelor's degree in computer science, information technology, or a related field and three years of experience in a system administration, networking, or IT security role.

OR

Associate's degree in computer science, information technology or a related field and five years of experience in a system administration, networking, or IT security role.

OR

A high school diploma, GED or equivalent certificate of competency and seven years of experience in a system administration, networking, or IT security role.

Preferred: One or more relevant technical security certifications such as the CCNA: Security, Offensive Security Certified Professional (OSCP), or a SANS certification. At least two years of experience in an IT security role.

WORKING CONDITIONS:

ENVIRONMENT:
Office environment.
Driving a vehicle to conduct work

PHYSICAL DEMANDS:
Incorporated within one or more of the previously mentioned essential functions of this job description are essential physical requirements. The chart below indicates the percentage of time spent on each of the following essential physical requirements.

1. Seldom = Less than 25 percent
2. Occasional = 25-50 percent
3. Often = 51-75 percent
4. Very Frequent = 76 percent and above

4 a. Ability to work at a desk, conference table or in meetings of various configurations.
2 b. Ability to stand for extended periods of time.
4 c. Ability to sit for extended periods of time.
4 d. Ability to see for purposes of reading printed matter.
2 e. Ability to hear and understand speech at normal levels.
4 f. Ability to communicate so others will be able to clearly understand a normal conversation.
2 g. Ability to bend and twist.
2 h. Ability to lift 25 lbs.

2 i. Ability to carry 25 lbs.
4 j. Ability to operate office equipment, computer or related peripherals.
3 k. Ability to reach in all directions.

This job description is intended to describe the general nature and level of work being performed. It is not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of individuals so classified.