Killeen Independent School District
Job Description

Job Title: Cyber Security Coordinator
Reports To: Director for Information Technology
Pay Grade: AM7

SUMMARY
As part of a team, evaluates, implements, and maintains the district's enterprise security posture using security tools, software and infrastructure.

ESSENTIAL DUTIES AND RESPONSIBILITIES include the following:

Assists in the development of and carries out information security plans and

policies.

Develops strategies to respond to and recover from a security breach.

Develops or implements open-source/third-party tools to assist in detection, prevention and analysis of security threats.

Provides awareness training for district employees on information security standards, policies, and best practices.

Coordinates all security awareness, training, and discussions with all district departments.

Installs and oversees firewalls, data encryption, and other security products and procedures.

Conducts periodic scheduled network scans to find vulnerabilities.

Conducts penetration testing, simulating an attack on systems to find exploitable weaknesses.

Reviews findings with security team to determine acceptable levels of risk.

Monitors networks and systems for security breaches, through the use of software that detects intrusions and anomalous system behavior.

Investigates security breaches.

Leads incident response, including steps to minimize the impact and then conducting a technical and forensic investigation into how the breach happened and the extent of the damage.

Installs and maintains the approved district Internet Web Filtering solution.

Completes integration with security aspects of all IT systems including SCCM, JAMF, AD, O365, VMWare, Email Security solution, Cisco hardware and software, and information systems.

Performs other duties as assigned.

SUPERVISORY RESPONSIBILITIES
Directly supervises Cyber Security Analyst. Carries out supervisory responsibilities in accordance with

the district's policies and applicable laws. Responsibilities include interviewing and training employees; planning, assigning, and directing work; appraising performance; rewarding and disciplining employees; addressing complaints, and resolving problems.

QUALIFICATIONS
To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required.

- Experience designing secure networks, systems, and application architectures
- Knowledge of Disaster Recovery, computer forensic tools, technology, and methods
- Experience planning, researching, and developing security policies, standards, and procedures
- Expertise in anti-virus software, intrusion detection, firewalls, and content filtering
- Knowledge of risk assessment tools, technologies, and methods
- Expertise in designing secure networks, systems, and application architectures
- Disaster recovery, computer forensic tools, technologies, and methods
- Experience planning, researching, and developing security policies, standards and procedures
- Experience in system administration, supporting multiple platforms and applications
- Expertise with malicious code and anti-virus software identification
- Experience with Endpoint security solutions, including file integrity monitoring and data loss prevention
- Experience with AWS and cloud platform as a service (PaaS) security
- Experience with automating security testing tools
- Ability to communicate network security issues to peers and management

EDUCATION and/or EXPERIENCE
Bachelor's degree in Computer Science/Information Technology (IT), or IT security certification (CEH, CISM, CISSP, GSEC, ECSA, GPEN, SCCP, or CISA), required. Three years related IT Security Administration experience required. At least one year experience with various enterprise deployment and familiarity with LAN/WAN communication protocols, hardware standards and project management experience, preferred.

SKILLS AND ABILITIES
Ability to perform high-level of computer skills in areas of the communication protocols. Ability to design and build a disaster recovery process for Exchange Server. Excellent interpersonal and communication skills. Knowledge of Windows 2003 and 2008 Advanced Server and active directory infrastructure.

MENTAL DEMANDS/PHYSICAL DEMANDS/ENVIRONMENTAL FACTORS
Tools/Equipment Used: Hand tools and test instruments for electronic repairs and cable installations; standard office equipment including personal computers and peripherals

Posture: Prolonged sitting; regular kneeling/squatting, bending/stooping, pushing/pulling, twisting

Motion: Repetitive hand motion; frequent keyboarding and use of mouse; regular walking, grasping/squeezing, wrist flexion/extension, reaching; may climb ladders

Lifting: Regular moderate lifting and carrying (up to 44 pounds); occasional heavy lifting and carrying (45 pounds and over)

Environment: Work is performed in an office environment; frequent on-call and after-hours work; occasional districtwide travel; may be required to be on-call 24 hours a day.

Mental Demands: Work with frequent interruptions; emotional control under stress

Revised Date: January 2023

The foregoing statements describe the general purpose and responsibilities assigned to this job and are not an exhaustive list of all responsibilities, duties, and skills that may be required.