PLANO INDEPENDENT SCHOOL DISTRICT
Job Description

Job Title:	Cybersecurity Analyst	**Wage/Hour Status:**	Exempt
Reports To:	Director of Applications & Cybersecurity	**Pay Range:**	838
Dept./School:	Technology Services	**Date Revised:**	05/31/22

Primary Purpose:

Provides support for security activities and efforts that ensure confidentiality, integrity and availability of customer, employee, and business information in compliance with organizational policies and standards, applications and user requirements, and laws and regulations.

Qualifications:

Education/Certification:

Bachelor's degree in Cybersecurity or a related field preferred

Industry certifications such as CISSP and CASP preferred

Special Knowledge/Skills:

Knowledge and experience with Security Information and Event Monitoring (SIEM)

Knowledge and experience with vulnerability scanning solutions such as Tenable or Qualys

Knowledge and experience with EPP/EDR/XDR solutions

Knowledge and experience with analyzing security systems with an understanding of how changes in conditions, configurations, operations, or the environment will affect outcomes

Knowledge and experience with applying cybersecurity and privacy principles to organizational requirements (relative to confidentiality, integrity, availability, and authentication)

Extensive knowledge and understanding of networking (Design, TCP/IP, Security), operating systems (Windows, Linux, Mac, Chrome), and cloud/web technologies

Extensive knowledge and understanding of system data including, but not limited to, security event logs, system logs, audit logs, and firewall logs

Excellent interpersonal, verbal and written communications skills

Ability to develop and maintain effective working relationships

Ability to handle multiple and changing priorities efficiently and effectively

Experience:

Three years of experience working within a security/IT governance or risk management and audit strategies

Job Title: Cybersecurity Analyst

Three years of experience with event monitoring, correlation, and threat management

Three years of experience with incident response or similar IT security operations role

Major Responsibilities and Duties:

Investigate security events and incidents; coordinate with appropriate business resources to assess and implement corrective actions

Perform advanced security event detection, threat hunting, and analysis for complex and/or escalated security events

Analyze security metrics and reports to assess trends or indicators of compromise or failure of security controls

Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, and the effects on systems and information

Recommend mitigations and corrective actions to reduce the overall risk to information/data confidentiality, integrity, and availability

Support risk assessment activities of district resources, customers, vendors, and other 3rd parties as needed

Monitor external data sources (e.g. cyber defense agencies, Cyber Incident Response Teams) to stay up-to-date on cyber defense threat conditions and determine which security issues may have an impact on the enterprise

Provide cyber security recommendations to leadership based on significant threats and vulnerabilities

Support development and maintenance of security policy, procedures and exceptions

Contribute to cybersecurity training and awareness programs, including organizational change management communications and support of employee phishing activities

Support integrated ITIL processes with incident, change, and problem management

Ensure all system changes are well communicated, coordinated, and documented

Develop plans to resolve problems and prevent them from recurring

Work collaboratively with campus personnel, departments, and leadership to define requirements and recommend appropriate technology solutions

Demonstrate a strong customer service orientation and a desire to help others

Establish and maintain a high level of customer trust and confidence in the team's knowledge of and concern for educational and business needs

Perform R&D, remain knowledgeable of emerging trends in cybersecurity, and keep abreast of innovative practices. Attain and keep current, relevant technology certifications.

Follow all rules, regulations and policies of Plano ISD and follow directives from supervisor

Follow attendance policy as assigned by supervisor

Perform special projects, after-hours support and upgrades, and other duties as assigned

Job Title: Cybersecurity Analyst

Working Conditions:

Mental Demands:
Ability to communicate effectively (verbal and written); interpret policy, procedures, and data; coordinate district functions; maintain emotional control under stress.

Physical Demands/Environmental Factors:
Frequent districtwide travel; occasional prolonged and irregular hours. Work with frequent interruptions. Frequent standing, stooping, bending, kneeling, pushing and pulling. Prolonged use of computer and repetitive hand motions. Occasional lifting up to 50 pounds.

Acknowledgement:

Any work related experience or additional education/training resulting in acceptable proficiency levels in the above required knowledge, skills, and abilities may be an acceptable substitute for the above specified education and experience requirements at the sole discretion of District Administration.

Approved By: W. Noel McBee, Compensation Coordinator **Date:** 5/31/2022

The above statements are intended to describe the general purpose and responsibilities assigned to this job and are not intended to represent an exhaustive list of all responsibilities, duties, and skills that may be required. District administration and/or my supervisor has the right to add or change duties at any time. This job description supersedes all prior job descriptions for this position as well as rescinding all past and present job descriptions that do not reflect the current requirements of this position.

My signature below indicates I understand and acknowledge my job description.

Employee Signature: **Date:**