CLASSIFIED JOB DESCRIPTION

CYBER SECURITY ANALYST I

JOB SUMMARY:

Under the direction of the Information Technology Director, moves District technology goals forward by participating in software and hardware development initiatives. Provides guidance on, and develops, implements and maintains, cyber security policies and standards. Collaborates with stakeholders and internal IT resources to provide support and consulting to technology and District staff.

ESSENTIAL JOB FUNCTIONS:

- Collaborates with management and IT staff to develop policies, plans and recommendations regarding the secure use of, and access to, District systems, hardware and software.
- Collaborate with District stakeholders on the development of training materials to improve security and awareness for end-users. Develop and implement regular phishing simulations and other cyber security-related exercises.
- Collaborate with senior staff to develop disaster preparedness and recovery plans. Perform regular tests of these plans to ensure feasibility and fidelity.
- Support Risk Management department in reviewing existing and proposed District software and hardware to ensure compliance with security standards.
- Provide guidance and implement policies to ensure the District meets standards for regulatory and insurance requirements.
- Collaborate with IT staff to implement security policies on District hardware and user accounts using enterprise Security systems.
- Research and analyze security threats to determine severity and remove and mitigate risk. This includes source tracing and utilizing isolated environments to investigate malicious software.
- Regularly review and act on threat assessment and alerts from District standard security systems. This includes identity management, file repositories, network traffic, malware detection and email/communication phishing.
- Collaborate with external security partners, including state, federal and SOCs, on training, threat assessment and mitigation.
- Supports the operations for on-premises and cloud-based District standard security software solutions and applications.
- Collaborate with IT staff to implement and maintain security standards on endpoint hardware and software. Schedule, deploy and support security updates for end user equipment and software. This includes assisting senior team members in developing and deploying policies and standards.
- Communicate with vendors, developers and contractors to provide access and implement changes to District security systems.
- Collaborate with IT staff to maintain security of cloud-based and on-premises support and device management systems; This includes helping configurate and assisting senior team members in testing and troubleshooting.

- Provides guidance and training to IT staff on security concerns and mitigation.
- Keeps abreast of advancements and emerging trends relevant to District and Education Industry standards.
- Creates, maintains, and expands department knowledgebase detailing specifications, operational procedures, troubleshooting steps, and other necessary information regarding security threats, policies and procedures.
- Maintains current skills relevant to District standard technologies through research and education. Maintain current understanding of industry standard cybersecurity threats and policies.
- Performs other tasks as assigned.

ESSENTIAL JOB REQUIREMENTS - QUALIFICATIONS:

- Experience with operation and administration of Microsoft Defender and Sentinel as well as general knowledge of interdependent enterprise systems such as Microsoft Intune, Microsoft endpoint manager, Microsoft Defender, Office 365 Admin Center or cloud apps, SharePoint online, Teams, Active Directory, Azure/Entra ID and Domain services.
- Ability to effectively utilize all inherent features and settings in Microsoft Security products to research, isolate and mitigate threats.
- Experience with process automation scripting using Microsoft PowerShell and Microsoft Power Automate/Flow
- High school diploma or GED required. Two or Four-year college degree with an emphasis on technology preferred.
- CompTIA Security+, CISSP or equivalent technical certification, or minimum two years comparable work experience, required.
- General Knowledge of: Microsoft, Google and Apple Device Management solutions such as Google Workspace, Mosyle and Microsoft Intune; LAN terminology and operation.
- Other Skills: Excellent oral and written communication skills; Ability to collaborate with others in problem solving and project implementation; Ability to research relevant information as it pertains to problem solving; ability to read and follow written and verbal technical instructions; Ability to effectively convey technical information in nontechnical terms; Ability to isolate and resolve problems in the operation of District computer hardware and software.

WORKING CONDITIONS AND PHYSICAL ABILITIES:

Must be able to hear and speak to exchange information; see to perform assigned duties; possess dexterity of hands and fingers to operate a computer and office equipment.

Classified Salary Schedule: Range 44
BOARD APPROVED: 05/22/23