Adams12 Five Star Schools

Job Description
Prepared/Revised: **October 2022**

Job Title:	**Cybersecurity Analyst**	Job Code:	**103904**
Job Family:	**IT Administrative**	FLSA Status:	**Ex- C**
Pay Program:	**Administrative**	Pay Range:	**L02**
Typical Work Year:	**12 months**		

SUMMARY: The Cybersecurity Analyst will provide analysis and proactive response across a range of operational resilience, security analytics, threat assessment, forensics, and incident response activities to support appropriate levels of cybersecurity at the District, working with the IT leadership team to review and address risks and provide efficient and effective solutions, always with a customer service focus. The Cybersecurity Analyst will employ strong communications and organizational skills to execute and maintain processes, procedures, policies, project plans, and communications strategies that ensure that timely, actionable and critical information is presented to IT leadership, and that IT customers are well informed of their responsibilities to ensure appropriate information security and related compliance across the district.

ESSENTIAL DUTIES AND RESPONSIBILITIES: *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. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.*

Job Tasks Descriptions	Frequency	% of Time
1. **Security Operations, Maintenance, & Defense:** Provide systems defense, troubleshooting, timely incident response, forensics, investigation, log analysis, URL filter tuning, and solution designs across the district-wide sets of systems. The range of systems that the Cybersecurity Analyst is responsible for includes any technological infrastructure where the District has risk including, diverse server operating systems, various types of virtualization, streaming media and transactional services, network management systems, security infrastructure, wireless/wired clients, Guest and BYOD access, secure transaction systems, education environments, radio communications and related infrastructure. Provide scripting, automated response, automated deployment, and remote servicing options to the district to support these systems.	D	25%
2. **Policy & Strategy**: Ensure a strong information assurance posture for the district by recommending changes to instructional policy, researching technologies, testing infrastructure, and implementing security designs in support of the district's systems architecture. Contribute to plans to implement vulnerability analysis, threat analytics, incident response and testing procedures, and implement training to maintain security readiness by implementing designs, processes, configurations, and technologies based on international and federal standards, RFCs, peer best practices, and other standards sources in additional to current professional practice and due diligence appropriate for the District. Provide support to the evaluation of strategic options of cybersecurity services, auditing, vulnerability testing, consulting, and partnerships to fulfill a range of District Cybersecurity options, while performing "build or buy" options analysis.	D	10%
3. **Professionalism in Practice:** Demonstrate exemplary cybersecurity practice, sharing expertise and collaborating with key teams and architects across IT, providing high quality technical configurations and practices, preparing end-user communications, contributing to policy, and contributing technical solutions that efficiently and effectively enhance the district's cybersecurity. Engage in professional development in order to maintain the currency of understanding and awareness of innovative technology options for the district in regards to this practice.	D	10%
4. **Resilience Planning**: Provide recommendations for technical resources, resilient design, change management, proactive testing procedures, and physical infrastructure to minimize disruption or impairment of service, achieve regulatory compliance, information assurance, operations resilience, support for innovative education practices, and other district interests at the highest possible levels as it maintains high quality customer service in an ever changing environment. Assess and report on the district's situation in relation to these requirements and present strategies for ensuring that these requirements are met and that shortcomings are mitigated or otherwise addressed.	D	10%
5. **Collaborative Service Quality:** Work within the Cybersecurity Team, and district stakeholders, IT architects and IT leadership to contribute to SLAs, cybersecurity policies and	D	10%

ensure that the district infrastructure can meet these requirements across enterprise application environments, computing resources, network availability, and related resources that fulfill district objectives. This environment includes virtual systems, multi-site datacenter resilience, and support for highly integrated sets of systems providing HR/Financial ERP, messaging, District security, education data, storage, telephony, database, remote access, education, and business services.		
6. **Research**: Research and provide security evaluation for new technologies and technology providers to ensure that the district makes secure and yet cost effective technical choices in systems, services, and strategies. Produce cogent and well-referenced reports that inform district security planning, identify risk, clarify opportunity cost, and assess total cost of solution ownership. Provide fair and meaningful evaluation of security technology choices through research, RFP, technical review, risk audits, use case proof of concept, vulnerability testing, and user acceptance methods.	D	5%
7. **Architecture & Engineering:** Provide input on and implement cybersecurity design and engineering solutions that support a forward-looking enterprise systems and lead to secure network, systems, and data footprint. Perform business analysis in support of cybersecurity technologies, solutions, and implementations that meet the District's compliance, privacy, availability, and business continuity needs at a scale appropriate for the District.	D	5%
8. **Professional Currency:** Work under the direction of IT leadership to establish and maintain professional affiliations and strategic relationships with incident response organizations, professional organizations, regulatory bodies, standards organizations, vendors, and other organizations of strategic importance to the district to ensure that the department is aware of industry best practices and is well informed in regards to service opportunities, cybersecurity issues and innovations that might have impact on the district.	D	5%
9. **Reporting and Transparency:** Work with Team and IT leadership to facilitate and maintain logging, monitoring, alert, and reporting policies and procedures that provide the CITO, I.T. directors, architects, managers, and the Cybersecurity Team with timely and actionable information related to enterprise security design, system vulnerabilities, security trends and use cases.	D	10%
10. Perform other duties as assigned.	Ongoing	5%
TOTAL		100%

EDUCATION AND RELATED WORK EXPERIENCE:

- Associates degree in cybersecurity, computer science, systems administration, information systems, or related area. Other relevant experience in cybersecurity operations or a combination of experience in an information technology position along with relevant certifications such as CKA, AWS-CSA, CySAS+, CSAP, OSCP, OSWE, or 2 other relevant certifications at this level can be considered instead of the associate's degree.
- One year experience preferred with operations and maintenance of key IT infrastructure in one or more of the following areas: desktop management, virtualization, storage, digital data communications, application server support, wired/wireless networks, software development, and systems integration preferred.

LICENSES, REGISTRATIONS or CERTIFICATIONS:

- Criminal background check required for hire.
- Preference for candidates with current certifications relevant to cybersecurity such as CISSP, CKA, AWS-CSA, CySAS+, CSAP, OSCP, OSWE, or other relevant certifications.

TECHNICAL SKILLS, KNOWLEDGE & ABILITIES:

- Detailed knowledge of the cybersecurity controls and practices related to information systems technologies and architectures at the scale of the district or greater.
- Strong knowledge and current skills in troubleshooting enterprise-class integration issues, responding to security incidents, and designing secure systems capable of high levels of uptime, information assurance, and business resilience.
- Ability to collaborate across teams in settings involving complex project management and change management, given the large backlog of project work in this space.
- Ability to implement technology in relation to relevant architectural models and appropriate frameworks.
- Ability to work with groups that vary from highly technical consultants to non-technical personnel and effectively convey issues, organize activities, and translate requirements into clear technical options. Maintained awareness of external cybersecurity groups, standards bodies, agencies, and professionals. The ability to use this awareness and common vulnerability databases to implement patch management strategies, malware protection, encryption, APT detection, SIEM, DDoS resilience, and system hardening procedures.
- Ability to implement change management processes, testing procedures, security systems and network management systems, large scale systems management technologies, service level agreements, and information assurance measures.

- Ability to promote and follow Board of Education policies, District policies, building and department procedures.
- Ability to stay current with district policy, standards and training in the areas of data quality, data privacy, and cyber-security with respect to student and staff data, and related information systems
- Ability to implement systems that meet FERPA, COPPA, CIPA and other relevant state and federal regulations related to cybersecurity, safety, privacy, content appropriateness, and related areas.
- Ability to communicate, interact and work effectively and cooperatively with all people, including those from diverse ethnic and educational backgrounds. Willingness to contribute to cultural diversity for educational enrichment.
- High level of skill in writing strategic documents, policy, and procedures in support of information systems functional requirements and the needs of the district.
- Ability to recognize the importance of safety in the workplace, follow safety rules, practice safe work habits, utilize appropriate safety equipment and report unsafe conditions to the appropriate administrator.
- Able to accept shifts of on call assignment, responding to urgent calls during that shift on a 24/7 basis.

MATERIALS AND EQUIPMENT OPERATING KNOWLEDGE:

- Working knowledge of a range of enterprise class cybersecurity technologies, and the cybersecurity aspects of enterprise-class equipment and user devices. Cybersecurity technology expertise should include SIEMs, forensic tools, firewalls, WAFs, host-based protections, DDoS protections, and alert systems. Expertise performing risk analysis, hardening, and mitigation of a variety of technologies is essential including: Internet protocol networks, system and desktop virtualization, enterprise application environments, portal services, enterprise infrastructure services, wide area networks, enterprise-scalable cloud services, telecommunications systems, end-user devices, and secure remote & mobile computing technologies.
- The ability to assess the physical security of an install base is important including aspects like physical security, system resilience, business continuity, and access control practices.
- Professional cybersecurity support capabilities in support of web portal, enterprise data systems, cloud, and web applications like Google Sites, and others.
- Ability to provide end-to end security analysis, incident response, and investigation related to converged technologies that include VoIP, streaming media, transactional databases, and end-user devices both mobile and wired.
- Secure authentication services skill using technologies like SSO, SAML, RADIUS, Windows domains and LDAP systems.
- Working knowledge of security related to server and service integration designs, internal and external cloud provisioning, security testing and configuration, and forensic analysis.
- Professional skills with a variety of office suite, communications, knowledge base, collaborative, presentation, project management, technical monitoring, troubleshooting, and technical design software and devices.

REPORTING RELATIONSHIPS & DIRECTION/GUIDANCE:

	POSITION TITLE	JOB CODE
Reports to:	Cybersecurity Manager	130903

	POSITION TITLE	# of EMPLOYEES	JOB CODE
Direct reports:	This job has no direct supervisory responsibilities.		

BUDGET AND/OR RESOURCE RESPONSIBILITY:

- Provides technical recommendations and vendor communications that support the development of budgets, RFPs, and requisitions.

PHYSICAL REQUIREMENTS & WORKING CONDITIONS: *The physical demands, work environment factors and mental functions described below are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.*

PHYSICAL ACTIVITIES:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Stand		X		
Walk		X		
Sit				X
Use hands and fingers, to handle or feel				X
Reach with hands and arms		X		
Climb or balance		X		
Stoop, kneel, crouch, or crawl		X		
Talk			X	
Hear			X	

PHYSICAL ACTIVITIES:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Taste	X			
Smell	X			

WEIGHT and FORCE DEMANDS:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Up to 10 pounds			X	
Up to 25 pounds			X	
Up to 50 pounds	X			
50 to 100 pounds	X			
More than 100 pounds	X			

MENTAL FUNCTIONS:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Compare				X
Analyze				X
Communicate				X
Copy		X		
Coordinate			X	
Instruct		X		
Compute				X
Synthesize		X		
Evaluate				X
Interpersonal Skills			X	
Compile				X
Negotiate			X	

WORK ENVIRONMENT:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Wet or humid conditions (non-weather)	X			
Work near moving mechanical parts	X			
Work in high, precarious places	X			
Fumes or airborne particles	X			
Toxic or caustic chemicals	X			
Outdoor weather conditions	X			
Extreme cold (non-weather)	X			
Extreme heat (non-weather)	X			
Risk of electrical shock		X		
Work with explosives	X			
Risk of radiation	X			
Vibration	X			

VISION DEMANDS:	Required
No special vision requirements.	
Close vision (clear vision at 20 inches or less)	X
Distance vision (clear vision at 20 feet or more)	X
Color vision (ability to identify and distinguish colors)	X
Peripheral vision	X
Depth perception	X
Ability to adjust focus	X

NOISE LEVEL:	Exposure Level
Very quiet	
Quiet	
Moderate	X
Loud	
Very Loud	