Adams12 Five Star Schools

Job Description
Prepared/Revised: **January 2025**

Job Title:	**Infosecurity Engineer II**	Job Code:	**130902**
Job Family:	**IT Administrative**	FLSA Status:	**Ex- C**
Pay Program:	**Administrative**	Pay Range:	**L06**
Typical Work Year:	**12 months**		

SUMMARY: The InfoSecurity Engineer II contributes significantly to bolstering the cybersecurity defenses of the District. In this capacity, this role encompasses responsibilities, including operational resilience, resource planning, security analytics, threat assessment, forensics, and incident response. Working close collaboration with other IT team members and IT managers, this position proactively identifies and addresses security risks while delivering efficient and effective cybersecurity solutions. With a strong commitment to customer service, the InfoSec Engineer II designs and maintains processes, procedures, and policies that facilitate the presentation of timely, actionable, and critical information to the InfoSec Manager. This role is pivotal in ensuring the District's adherence to information security and compliance standards, actively collaborating with IT stakeholders to achieve these goals.

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. Ensure the continuous operation, maintenance, and defense of the district's cybersecurity infrastructure, including monitoring for threats, responding to incidents, and conducting routine maintenance tasks.	D	30%
2. Demonstrate professionalism in cybersecurity practice by collaborating with key teams, providing high-quality technical configurations, and upholding industry best practices.	D	15%
3. Efficiently manage and respond to customer-generated cybersecurity tickets and service requests, addressing inquiries, incidents, and issues in a timely manner. Provide courteous and professional support to end-users, guiding them through security-related concerns, troubleshooting problems, and ensuring resolutions align with security best practices.	D	10%
4. Research emerging cybersecurity threats and technologies, conducting research to identify potential risks and innovative solutions. Participate in the assessment of new technologies for potential security risks and benefits, providing valuable input to decision-making processes.	D	10%
5. Contribute to the development and execution of the district's information security strategy, aligning security initiatives with organizational goals, and recommending strategic directions.	D	5%
6. Take on leadership responsibilities within the cybersecurity team, providing guidance, mentorship, and subject matter expertise to junior team members. Participate in shaping the strategic direction of cybersecurity efforts within the district.	D	5%
7. Architect and engineer robust and secure solutions for the district's technology infrastructure. Collaborate with senior IT technical staff to design and implement security controls based on industry standards.	D	5%
8. Generate regular reports on security incidents, vulnerabilities, and threat landscapes. Communicate security updates effectively to IT leadership and stakeholders to maintain transparency in cybersecurity operations.	D	5%
9. Lead efforts to ensure the district has the necessary technical resources, resilient design, proactive testing procedures, and physical infrastructure to minimize disruptions and maintain high-quality customer service while achieving regulatory compliance and information assurance.	D	5%
10. Assist in the development and implementation of user awareness programs to educate staff and students on cybersecurity best practices.	D	5%
11. Perform other duties as assigned.	D	5%
TOTAL		100%

EDUCATION AND RELATED WORK EXPERIENCE:

- Bachelor's degree in information systems or a related field. Four years of similar and relevant experience may be substituted for this requirement.
- Knowledge in implementing and supporting cybersecurity technologies and systems.
- Two to four years of experience in IT operations and support, with a preference for experience in cybersecurity operations.

LICENSES, REGISTRATIONS or CERTIFICATIONS:

- Criminal background check required for hire.
- Preference for candidates with current certifications relevant to cybersecurity such as CISSP, Security+, CASP, SSCP, GSEC, CEH, GCIH, OSCP, etc.

TECHNICAL SKILLS, KNOWLEDGE & ABILITIES:

- Security and Compliance
    - Apply an understanding of enterprise-class cybersecurity technologies to ensure the security of District equipment and user devices.
    - Utilize key cybersecurity technologies such as Security Information and Event Management (SIEM) systems, firewalls, end-point protection, and alert systems to enhance the District's security posture.
    - Conduct risk analysis and implement mitigation strategies for technologies including system and desktop virtualization, applications, portal services, infrastructure services, cloud services, and remote/mobile computing.
    - Assess and improve the physical security of installations, focusing on system resilience, business continuity, and access control.
    - Provide cybersecurity support for InfoSec tools, including email protection, EDR solutions, and network security.
    - Manage secure authentication services using Single Sign-On (SSO), Security Assertion Markup Language (SAML), Windows domains, and Lightweight Directory Access Protocol (LDAP) to enhance user access security.
    - Design and integrate server and cloud provisioning solutions, perform security testing, and conduct forensic analysis.
    - Utilize various software tools for communication, collaboration, project management, technical monitoring, troubleshooting, and technical design to support security initiatives.
    - Stay informed and adhere to regulatory compliance standards such as FERPA, COPPA, CIPA, and other pertinent state and federal regulations in the areas of cybersecurity, safety, and privacy.
- General Administrative and Technical Skills and Abilities:
    - Participate in on-call rotation if required, responding to urgent issues during off hours.
    - Communicate effectively with both technical and non-technical personnel to coordinating activities and deliver clear technical solutions.
    - Work collaboratively with diverse groups, fostering an inclusive environment that respects differences in culture and background.
    - Uphold confidentiality across all job functions, particularly when dealing with sensitive information.
    - Stay informed of District policies, standards, and training related to data quality, privacy, and cybersecurity, ensuring compliance with relevant guidelines for student and staff data.
    - Adhere to Board of Education and Superintendent Policies, as well as department and building procedures.
    - Recognize workplace safety as a priority, following safety protocols, using appropriate safety equipment, and reporting unsafe conditions to supervisors.

REPORTING RELATIONSHIPS & DIRECTION/GUIDANCE:

	POSITION TITLE	JOB CODE
Reports to:	Infosecurity Manager	130903

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

BUDGET AND/OR RESOURCE RESPONSIBILITY:

- N/A

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	
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			
51 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	