Adams12 Five Star Schools

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

Job Title:	**Infosecurity Engineer IV**	Job Code:	**090609**
Job Family:	**Non-Certified**	FLSA Status:	**Ex- C**
Pay Program:	**Administrative**	Pay Range:	**L12**
Typical Work Year:	**12 months**		

SUMMARY: The Infosecurity Engineer IV is responsible for the strategic planning, design, and implementation of advanced information security systems and initiatives across the District. This role encompasses operational resilience, security architecture, forensics, and incident response, with a focus on mitigating high-risk threats and overseeing complex projects. The InfoSec Engineer IV collaborates with internal teams and external vendors to lead district-wide cybersecurity initiatives, ensuring that the school district's digital infrastructure is fortified against evolving threats. This position guides the District's cybersecurity strategy, ensuring regulatory compliance, and leading threat-hunting and defense operations. The InfoSec Engineer IV also plays a crucial role in mentoring and developing junior staff members and fostering cross-departmental collaboration to strengthen the district's cybersecurity posture.

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. Contribute to the development and execution of the district's information security strategy, aligning security initiatives with organizational goals, and recommending strategic directions.	D	20%
2. Demonstrate professionalism in cybersecurity practice by collaborating with key teams, providing high-quality technical configurations, and upholding industry best practices.	D	20%
3. 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	15%
4. 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	15%
5. 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	15%
6. 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%
7. 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.
- In depth knowledge in implementing and supporting cybersecurity technologies and systems.
- Seven to ten years of progressive experience in IT operations and support in a large / enterprise environment, including a minimum of four years of 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 senior-level expertise in cybersecurity controls and practices for enterprise-class systems, ensuring secure and resilient operations.
    - Diagnose and resolve complex integration issues and design secure systems to maintain uninterrupted services and business continuity.
    - Lead incident response procedures, including detection, triage, investigation, containment, and remediation of cybersecurity incidents.
    - Utilize and manage log management systems, advanced threat detection tools, and automated response mechanisms to enhance security operations.
    - Conduct comprehensive risk analysis, system hardening, and mitigation for a wide range of technologies, including IP networks, virtualization systems, enterprise applications, portal services, wide area networks, cloud services, telecommunication systems, end-user devices, and mobile computing.
    - Design and implement complex server and service integration, cloud provisioning, advanced security testing, configuration, and perform detailed forensic analysis.
    - Utilize a wide range of office suite, communications, knowledge base, collaborative, presentation, project management, and technical monitoring tools to support cybersecurity operations.
    - Manage and lead large-scale incident response efforts, ensuring quick, effective resolutions while minimizing impact, and providing clear communication to all relevant stakeholders.
    - Solve complex cybersecurity challenges by identifying risks, developing innovative solutions, and leading cross-functional teams in implementing them.
    - 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.
- System Architecture and Design
    - Lead the deployment and architecture of security frameworks, leveraging expertise in SIEMs, forensic tools, firewalls, host-based protections, cloud security, and remote automation.
    - Architect, design, and implement complex IT infrastructure solutions to meet the organization's evolving needs.
    - Evaluate and recommend new technologies and tools to enhance system performance and capabilities.
- Vendor and Stakeholder Management:
    - Manage relationships with technology vendors and service providers.
    - Collaborate with internal stakeholders to understand business requirements and align IT strategies accordingly.
- Project Management:
    - Manage and lead cybersecurity projects, including upgrades, migrations, and expansion initiatives.
    - Oversee project budgets, timelines, and resource allocation.
- Team Leadership and Mentoring:
    - Provide technical leadership to the IT team, including mentoring junior staff, coordinating team efforts, and if required, work as a team lead.
    - Lead by example in adhering to best practices and maintaining a high level of professionalism.
- General Administrative and Technical Skills and Abilities:
    - Participate in on-call rotation 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:

- 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 and/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			

WORK ENVIRONMENT:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
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	