Adams12 Five Star Schools

Job Description

Prepared/Revised: January 2024

Job Title:	**Infosecurity Manager**	Job Code:	**130903**
Job Family:	**Non-Certified**	FLSA Status:	**Exempt**
Pay Program:	**IT Administrative**	Pay Range:	**L17**
Typical Work Year:	**12 months**		

SUMMARY: Manage infosecurity operations including incident response, proactive controls and protections, vulnerability assessments, threat assessment, technology adoption reviews, and maintaining infosecurity policies and plans. Create an effective security architecture, system resilience & capacity, and incident response capabilities while maintaining appropriate IT service levels. Act as the primary point of escalation for cybersecurity operations, and coordinate escalation paths and decision groups for incidents, risk analysis, and process review. Responsibilities also include maintaining relationships with cybersecurity agencies, organizations, and service companies, contributing to budget development, and assessing gaps in infosecurity postures in relation to peers, due diligence, standards and compliance, and the evolving threat landscape.

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. Manage the daily operations of the Infosecurity team, including risk analysis, ticket-based responsiveness, incident response, cybersecurity programs, and processes. Ensure the cyber protection of District systems, data, applications, and privacy in support of active operations and business needs. Perform various administrative tasks for the Infosecurity team including, but not limited to, manage vendor relationships, performance evaluations, evaluate staff training options, developing and monitoring budgets, etc.	D	15%
2. Supervise the daily operations of the Infosecurity team, including oversight of staff, ticket-based responsiveness, contractors, services, and partner relationships. Ensure that collaborative relationships with IT and throughout the district to facilitate staff abilities to effectively secure systems owned by other groups.	D	10%
3. Develop strategies, plans, playbooks, standards, and documented processes and procedures to ensure resilient and secure ongoing processes, balancing the business needs of the District against the cybersecurity and business continuity risks.	D	10%
4. Maintain continuous District readiness for response to cyberattack with staff cybersecurity training, tabletop exercises across various groups, business impact analysis, team incident response training, and ensuring capabilities in network forensics, malware analysis, computer analysis, vulnerability analysis,	D	10%
5. Identify, select, procure, and manage cybersecurity projects that maintain the resilience of district infosecurity controls while effectively managing a changing threat landscape, technology lifecycles, evolving district activities, and changing institutional relationships.	D	10%
6. Promote a robust cybersecurity culture across groups within IT and across the District. Plan technical training exercises, staff awareness campaigns,and inter-institutional collaborative opportunities,	D	10%
7. Collaborate effectively to allied work including physical security, software and device lifecycle management, update and system compliance management, infrastructure architecture, cloud resources, business continuity, disaster recovery, records management, computer code and script development security, and resilient services maintenance.	D	10%
8. Provide viable technical, policy, and communications strategies for ensuring appropriate privacy, information security, forensic investigation, confidentiality, and systems availability in an environment that assumes threat activity.	D	10%
9. Ensure rigorous use across technologies for cryptography, compartmentalization, monitoring, log aggregation, intrusion detection, risk mitigating measures, incident logging and response, and risk assessment.	D	10%
10. Perform other duties as assigned.	Ongoing	5%
TOTAL		100%

EDUCATION AND RELATED WORK EXPERIENCE:

- Bachelor's Degree or higher in a technology field or comparable progressive experience in cybersecurity or IT positions involving cybersecurity.
- Five (5) years of experience as a cybersecurity engineer or similar work including major cybersecurity incident response, systems protections, policy facilitation, and compliance.
- Eight (8) years of experience in an IT Enterprise-class environment working with data centers, regional networks, compute/SAN infrastructure, cloud-based resources, and significant application services and development.
- Experience leading cybersecurity teams preferred.

LICENSES, REGISTRATIONS or CERTIFICATIONS:

- Criminal background check required for hire.
- GIAC Incident handler, CompTIA Security+ or similar certifications required.
- Microsoft, Cisco, CISSP or other related technology certifications preferred.

TECHNICAL SKILLS, KNOWLEDGE & ABILITIES:

- Effectively manage incident response, coordinating other departments, and lead cybersecurity teams to effectiveness,
- Maintain a team and cybersecurity programs that lean forward in a proactive state to shore up cybersecurity defenses in relation to technology lifecycles, changing threat landscapes
- Effectively oversee cybersecurity operations for a user base of 40,000, using automation, enterprise class tools, dashboard development, and reporting structures that can sustain effective cybersecurity at this scale.
- Collaboratively manage priorities with business owners, executives, and team members to provide empowering cybersecurity services including change management, ITIL-oriented services, risk analysis, demand management, and program management.
- Strategic, current and detailed knowledge of the cybersecurity controls and practices related to enterprise-class information systems technologies and architectures at the scale of the district or greater.
- Expert knowledge and current skills in troubleshooting enterprise-class integration issues, responding to regional-scale security incidents, and designing secure systems capable of high levels of uptime, information assurance, and business resilience.
- Effective ability to perform cybersecurity analysis of technology architectural models and frameworks, and apply cybersecurity and risk theory to these in order to support effective executive choice, technical solutions, business decisions, and operational tactics.
- Ability to follow, update, and ensure compliance with Board of Education policies, District policies, and building and department procedures.
- Ability to plan and implement organization cultural campaigns in conjunction with IT leadership and others to promote best information security practices within IT and across the District
- Capability to ensure that the District is meeting 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.
- Ability to stay current with district policy, standards and training in the areas of data quality, data privacy, and cybersecurity with respect to student and staff data, and related information systems.
- Able to respond to urgent calls during emergencies and incident response 24/7 when available and provide management coverage of active incidents.

MATERIALS AND EQUIPMENT OPERATING KNOWLEDGE:

- Strategic 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, email security, 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.
- Expert cybersecurity support capabilities in support of web portals, enterprise data systems, cloud, and web applications like SharePoint, Drupal, Google Sites, email systems and services, 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.
- Advanced knowledge of security related to complex server and service integration designs, internal and external cloud provisioning, security testing and configuration, and forensic analysis.
- Capabilities to select, assign, and oversee staff and projects with appropriate coding security skills and practice.
- 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:	Academic Computing Services Executive Director	090532

	POSITION TITLE	# of EMPLOYEES	JOB CODE
Direct reports:	Infosecurity Analyst	1	130903
	Infosecurity Engineer	1-2	130902
	Systems Administrator	1-2	Varies

BUDGET AND/OR RESOURCE RESPONSIBILITY:

-

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			
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	