Adams12 Five Star Schools

Job Description

Job Title:	**Enterprise Systems Engineer, Senior**	Job Code:	**040505**
Job Family:	**Non-Certified**	FLSA Status:	**Ex- C**
Pay Program:	**Administrative**	Pay Range:	**L 04**
Prepared/Revised Date:	**Junly 2015**	Work Year:	**12 months**

SUMMARY: Maintain and monitor an efficient and forward-looking enterprise systems infrastructure that effectively and securely meets the computing, storage, and data communications requirements of the district. Responsible for ensuring a strong information assurance posture by evaluating, implementing and maintaining vulnerability monitoring, threat assessment, defense implementation, and incident response management systems for the district. Provide exemplary technical leadership for the Academic Computing Services (ACS) department effectively supporting the district in achieving regulatory compliance, operations resilience, business agility, education technology innovation and other district interests at the highest possible levels while maintaining high quality customer service in an ever changing environment. Under the guidance of the Principal Systems Architect and IT leadership, will collaborate with district stakeholders to develop SLAs that fulfill district objectives and then design and develop the infrastructure to meet those SLAs. Responsible for ensuring that the district makes quality and cost effective technical choices in equipment, services, and implementations. Provide top tier enterprise systems troubleshooting, incident response, and solution design across the district. Ensure broad and current technical awareness by establishing and maintaining technical and professional relationships with appropriate organizations of strategic importance to the district. Employ strong communications and organizational skills to designing and maintaining processes and procedures that ensures that timely, actionable and critical information is presented to IT leadership.

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. Provide and implement technical design and engineering solutions that support a forward-looking enterprise systems architecture that effectively and efficiently meets the computing, storage, security, and data communications requirements of the district. Ensure that complex network systems across the district are designed to efficiently achieve a high level of availability, as defined by IT leadership, in relation to the specific services and business requirements.	D	15%
2. Ensure a strong information assurance posture for the district by developing strategy, researching technologies, testing infrastructure, and implementing security designs in support of the districts systems architecture. Perform vulnerability analysis, develop threat profiles, formulate incident response and testing procedures, and implement training and scenario exercises to maintain security readiness. Do this by implementing designs, processes, configurations, and technologies based on NIST, NSA, DoD reference, RFCs, and other standards sources in additional to current professional practice and due diligence.	D	10%
3. Provide exemplary technical and leadership for the ACS department by modeling good practice, sharing expertise, providing high quality innovative technical configurations and practices, and contributing technical solutions that enhance the districts capabilities, resilience, and agility. Engage in professional development in order to maintain currency of understanding and awareness of innovative technology options for the district. Provide technical mentoring, coaching, project guidance, and training events for the technical staff in regards to customer engagement, technologies, and problem solving strategies.	D	15%
4. Ensure that the district has the technical resources, resilient design, change management, testing procedures, and physical infrastructure to 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. Provide capacity planning for district systems to ensure business continuity and cost efficiency. Assess and report on the districts situation in relation to these requirements and present strategies for ensuring that these requirements are met.	D	10%
5. Work with district stakeholders and IT leadership to design SLAs and ensure that the district infrastructure can meet its SLAs for enterprise application environments, computing resources, network availability, and related resources that fulfill district objectives. This environment	D	10%

includes virtual systems, multi-site datacenter resilience, and support for highly integrated sets of systems providing HR, messaging, security, education data, storage, telephony, database, remote access, education, and business services.		
6. Research and evaluate technologies and technology providers to ensure that the district makes quality and cost effective technical choices in systems, services, and strategies. Produce cogent and well-referenced reports that inform district strategic planning, identify risk, clarify opportunity cost, and assess total cost of solution ownership. Facilitate fair and meaningful evaluation of technology choices through RFP, technical review, Pilot, demo, user acceptance testing, and user feedback methods.	D	10%
7. Provide troubleshooting, incident response, forensics, and solution designs across the district-wide sets of systems. The range of systems that the PSE is responsible for includes IP protocol infrastructure, diverse server operating systems, various types of virtualization, streaming media and transactional services, network management systems, security infrastructure, wireless/wired clients, BYOD access, secure transaction systems, education environments and related infrastructure. Provide scripting, automated response, automated deployment, and remote servicing options to the district to support these systems.	D	5%
8. Work under the direction of IT administrative 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, security issues and innovations that might have impact on the district.	D	5%
9. Work with the IT administrative leadership to design and maintain logging, monitoring, alert, and reporting policies and procedures that provide the CITO and I.T. managers with timely and actionable information related to enterprise design, system performance, security issues and technical procedures.	D	5%
10. Perform other duties as assigned.	Ongoing	5%
TOTAL		100%

EDUCATION AND RELATED WORK EXPERIENCE:

- Bachelor's degree in systems administration and engineering or related area. Four (4) additional years of similar and relevant experience may be substituted for this requirement..
- Minimum of eight (8) years current experience in enterprise-class design, top tier incident response, strategic technology analysis, and regional infrastructure implementation.

LICENSES, REGISTRATIONS or CERTIFICATIONS:

- Criminal background check required for hire.

TECHNICAL SKILLS, KNOWLEDGE & ABILITIES:

- Strategic, current and detailed knowledge of 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 & implementing systems capable of high levels of uptime, information assurance, and business resilience.
- Ability to implement technology in relation to architectural models that might include ISO9000, CMM, SixSigma, or or frameworks such as Zacchman, Gartner, TOGFAF, or The Federated Enterprise Architecture, or others as selected and used by the SESE.
- 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 groups, standards bodies, agencies, and professional organizations should include US-CERT, NIST, NSA, CNSS, and DoD references among others. The ability to use this and common vulnerability databases to implement patch management strategies, malware protection, encryption, APT detection, IDS, DDoS resilience, and system hardening procedures.
- Ability to propose, justify, plan, and bring to closure highly complex and large scale information technology projects.
- Ability to design and implement change management processes, testing procedures, enterprise 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, Superintendent policies, building and department procedures.
- Ability to implement systems that meet FERPA, COPPA, CIPA and other relevant state and federal regulations.

- 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 be on call and/or respond to urgent calls 24/7 as part of scheduled response teams.

MATERIALS AND EQUIPMENT OPERATING KNOWLEDGE:

- Strategic knowledge of a range of enterprise class infrastructure equipment 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. Ability to perform computer and network forensics with tools like FTK, Snort, RedEye, Wireshark, NMAP, the BackTrack suite, Nessus, Metasploit, and other related technologies.
- Implement regional deployments of infrastructure related technologies including hypervisors like Xen and VMware; management and deployment systems like LANdesk, KACAE, Altris or SCCM; directory architectures like AD and LDAP; storage technologies like EMC, HDS, CommVault, LeftHand, and NetApp; Operating Systems like current server and client versions by Microsoft, Apple, and various Linux projects; enterprise malware protection software including options like those from Semantic, McAfee, Kaspersky, or Microsoft; connectivity like the 802 suite of technologies, FC, iSCSI, the IP protocol Suite; equipment like Cisco, Brocade, Juniper, HP, and Nortel; data center technologies like UPS systems, FM200, generators, HVAC and Alert systems; and enterprise management systems like HP OpenView, Foglight, or Nagios.
- Expert skill supporting the infrastructure environment for enterprise applications and databases like SAP, Infinite Campus, Oracle, PeopleSoft, etc.
- Expert troubleshooting capabilities in support of web portal, cloud, and web applications like SharePoint, Drupal, Google Sites, and others.
- Ability to provide end-to end troubleshooting of converged technologies that include VoIP, streaming media, transactional databases, and end-user devices both mobile and wired.
- Security services skill using technologies like SSO, SAML, RADIUS, Windows domains and LDAP systems.
- Expert knowledge of complex server and service integration designs, internal and external cloud provisioning, security testing and configuration, and forensic analysis.
- Advanced 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:	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 to finger, handle or feel				X
Reach with hands and arms		X		
Climb or balance		X		
Stoop, kneel, crouch, or crawl		X		
Talk			X	

PHYSICAL ACTIVITIES:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
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			
Up 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	