JOB DESCRIPTION QUESTIONNAIRE – EXEMPT POSITIONS

School District 27J ***It is expressly understood that there is a possibility, if you are requesting a reclassification, that this position may come in under the current grade. It is further understood, if that should occur, you will be frozen at your current rate of pay until the market catches up with your salary.***

PLEASE NOTE: ONLY ONE QUESTIONNAIRE SHOULD BE COMPLETED FOR EACH JOB TITLE. QUESTIONNAIRES MUST BE TYPED OR CLEARLY PRINTED.

1. Job Information

Official job title: Sr. Information Security Engineer

If you recommend a different job title, please specify the recommended job title and obtain administrative supervisor approval for the title change: Recommended title:

Name(s) of Person(s) Completing the Questionnaire Jeremy Heide

Work Telephone Number 303-655-2912 Date 12-2-2020

This position is scheduled to work: 260 days per year, and 8 hours per day.

2. Organizational Relationship

Department Technology

Location/Building NOC

Reports to: Name Jeremy Heide Title CIO

3. Summary of Job

The Senior Information Security Engineer will create an effective security architecture, system resilience and incident response capability while maintaining service levels. In addition, this position will be primarily responsible for safeguarding the organization's computer systems and networks. The role involves engineering, implementing, and monitoring security measures to protect sensitive data and systems from infiltration and cyber-attacks. This role will work within the larger IT team, working cross-functionally as needed to assist in the cyber security posture of the school district.

4. Essential Job Elements

Please list the essential (must be done) tasks performed to achieve the purpose of this job. Include up to 13 of the most important tasks. Please be brief; **the job description will be limited to two pages**. Be sure to define any abbreviations. After you have listed the tasks, estimate the frequency each task is performed -- **(D)** daily, **(W)** weekly, **(M)** monthly, **(A)** annually. **Please assign only one frequency code to each task.** Also, estimate the percentage of time each task requires on an annual basis. The total, including the percentage allocated to "other duties as assigned," must equal 100 %.

Each task should begin with an action verb, for example "develop," "implement," etc. Avoid verbs that do not describe actions, such as "perform," "handle," or "process," without descriptors that show the extent of skill required.

Daily = **D**
Weekly = **W**
Monthly = **M**
Annually = **A**

Considered on an annual basis

Job Task Descriptions	Frequency	% of Time
Determine security requirements by evaluating district strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues	**D**	**20**
Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs	**A**	**10**
Implement/maintain information security controls and protections for systems, network, and information. Identify security risks and assist with design and development of controls. Test for vulnerabilities and assist with vulnerability management process.	**D**	**10**
Manage vulnerability detection, automated prevention measures, and patch management. Including IDS/IPS, SIEM, Firewall, content filtering, packet filtering content shaping devices, Elkstack.	**D**	**20**
Monitor/respond-to/investigate/resolve/document information security breaches. Prioritize and track all issues to resolution, escalating issues as needed.	**D**	**10**
Create and update technical documentation	**A**	**5**
Review, test, update system, network, application requirements to maintain information security	**M**	**10**
Maintain a research regimen of emerging technologies, practices, and policies that might advance the capabilities, service qualities and security posture of the school district.	**M**	**10**
Other duties as assigned	**A**	**5**
Total PLEASE VERIFY THAT THE PERCENTAGES TOTAL TO 100%		**100%**

5. Qualifications: Education, Experience, Skills, Knowledge, and Licenses

Assume you are promoted to another position and are given the responsibility for finding a person to fill this job. Think of the **minimum** level of education, experience, and skill a newcomer must possess to **enter the job** and successfully accomplish the essential duties of the job. These qualifications may not necessarily reflect the qualifications that you have.

A. Education:

- ☐ Two years of high school, vocational school, or equivalent on-the-job training and experience.
- ☐ Four years of high school, completion of G.E.D., or equivalent vocational school or short term courses, such as typing, dictation, computer training, commercial driver training, commercial trade training, etc. Specify vocational or short term courses required, if applicable:
- ☐ Four years of high school or equivalent, plus specialized technical courses in business, vocational school, or community college related to a trade or skill. For example, office and secretarial work, word processing, basic computer skills, bookkeeping, or a recognized apprenticeship program toward a trade level or licensing, such as carpentry, plumbing, electrical, etc. Specify courses/area of study required:
- ☒ Four years of high school, plus post-secondary courses in business or vocational school equivalent or up to one year of college**.** The job holder may be required to have and maintain special licenses, such as journeyman or certifications acknowledged by a governmental authority. This does not include a general state automobile driver's

license, CPR or first aid training, food handler certificate, or similar licenses or certificates. Specify courses/area of study required:

☐ Four years of high school, plus specialized advanced courses in business or vocational school up to two years of college. Specify courses/area of study required:

☐ Bachelor's degree or above or equivalent advanced training pertinent to the position requirements, such as accounting, communications, business, education, purchasing, payroll transportation, nutrition, construction management, etc. Specify degree/major: Bachelor in Accounting or related Business degree.

B. Related Work Experience Check the appropriate box that best represents the **total** years of experience required for this position. Also, indicate the area(s) in which the experience is required, such as mechanics, plumbing, word processing, , dealing with children with special needs, transportation, etc. **Please check only one box. You may specify multiple areas of experience for the experience level chosen, and indicate individual experience levels required.** For example, if a grounds worker position requires three years of total experience (one year of experience in pesticide application and two years of experience in turf maintenance), he/she would check the second box, and write in "pesticide application - 1 year; turf maintenance - 2 years" on the lines provided.

☐ No experience, and up to and including two years experience in (specify area(s))

☐ Over two years, and up to and including three years experience in (specify area(s))

☒ **Over seven years** experience in (specify area(s): Information Technology administration and engineering

C. Skills, Knowledge, or Training Required To perform the essential duties of this job, please indicate the special skills, knowledge, and training the person **must** have to enter this position. This could include knowledge of a language, basic mathematics, basic writing, basic microcomputer skills, advanced microcomputer skills, computer software skills, accounting, information technology, complex maintenance or mechanical systems, dealing with children with special needs, CPR, First Aid, nutrition, asbestos removal, etc. **Microsoft Server, Desktop, and Networking experience**

D. Required Licensing, Registration, or Certification Indicate any special licensing, registration, or certification that is **required** to perform the essential duties of this job. This may include journeyman license, master level license, valid Colorado automobile driver's license*, commercial driver's license (CDL), food handler certificate, CPR, First Aid, Department of Transportation physical examination, etc. Check (√) if the license, registration, or certification is required to enter the job, is preferred at hire but not required, or can be acquired within some period after entry. If required after entry, indicate the number of months in which the license, registration, or certification must be obtained after hire.

Special Licenses, Registrations, or Certifications	Check/complete only one box for each line		
	Required for hire	Preferred at hire, but not required	Must acquire after ? months (Indicate # of months)
1. CCNA Security+	X		
2.SANS Training			X One Month
3.CEH		X	
4.CISSP		X	

* This does **not** include getting to and from work or moving between locations during the work schedule if other modes of transportation are typically available.

E. Equipment Operating Requirements Describe any special equipment, such as office equipment, computer hardware, specific heavy equipment, etc., or computer software experience required to perform the essential duties of this job. Check (√) if the ability to operate or use the equipment or software is required to enter the job, is preferred at hire but not required, or can be acquired within some period after entry.

Special Equipment Operating Requirements	Check/complete only one box for each line		
	Required for hire	Preferred at hire, but not required	Must acquire after ? months (Indicate # of months)
Servers, Desktops	x		
Network switching, Firewalls	x		
IDS/IPS		x	
System Logging - aka syslog		x	

6. Supervision/Technical Responsibility

A. Does this position supervise others? No **If "no," skip to Section 6E.**

D. Describe the capacity in which this position supervises others. Include the type of position this person holds, such as coordinator, lead in a work group, supervisor, or unit supervisor. Also, indicate the nature of this supervisory role, such as whether this position is responsible for hiring, discipline, termination, directing work, etc.__

What percentage of time does this position spend conducting supervisory responsibilities, such as training, assigning work, discipline, performance reviews, etc.? ☐ Up to 50% ☐ 51% - 75%
☐ Over 75%

List the complete job title for each title this position supervises. Include the unit name or department, and the number of employees in the positions supervised. Also, indicate whether the positions report directly to this position or through a subordinate supervisor or group leader.

Position Titles Supervised	Unit or Department Name	# of Employees	Check only one box for each line	
			Reports directly to this position	Reports to this position through sup or grp leader

E. Describe the extent this position serves as a technical resource to others in such areas as curriculum, special education, bilingual skills, technical areas (e.g., computers, heat and air conditioning systems, hazardous materials, electrical systems, electronics, plumbing, etc.), or business applications (e.g., accounting, finance, payroll, etc.). Remember, a "technical resource" means that this position helps and trains others as part of the assigned job duties**. This position will serve as a technical resource to users in the areas of day to day infosec usage and district applications.**

F. This position's technical resource responsibilities extend:
☐ Within immediate work area or unit ☐ Within immediate department ☒ Across the District

7. Judgment and Decision Making

A. How is work assigned to this position and by whom? **By directive, Chief Information Officer**

B. Summarize a typical decision made by a person in this position on a regular basis. **A typical decision in this position would be to identify security weakness, breaches, and perform security remediation.**

C. Does decision making typically involve collaboration with other individuals, departments, or resources? Yes
If "yes," with whom does this position regularly collaborate? **CIO,Network Engineers, Systems administrators, Client service technicians and District Leadership Teams.**

D. To what extent is a supervisor or manager involved in approving decisions made by a person in this position?
☐ Always ☐ Occasionally ☒ Only major decisions
☐ Never

8. Diversity of Duties

A. Summarize the scope of duties involved in this position. Include the extent the job crosses other technical areas or fields, requiring cross-training to perform the job. For example, a carpenter may be required to have knowledge of carpentry, locksmithing, cabinetry, etc. See Attachment A

B. Describe the technical skills and abilities required to solve problems while performing this job.

Windows, UNIX and Linux operating systems
Perimeter security controls – firewall, IDS/IPS, network access control and network segmentation
Router, switch and VLAN security; wireless security
Security concepts related to DNS, routing, authentication, VPN, proxy services
Practices and methods of IT strategy, enterprise architecture and security architecture
Familiarity and understanding of National Institute of Standards and Technology (NIST) standards
Network security architecture development and definition
IDS/IPS, penetration and vulnerability testing
Firewall and intrusion detection/prevention protocols
Secure ethical hacking and threat modeling
Virtualization technologies
MSSQL database platforms
Identity and access management principles
Application security and encryption technologies
Secure network architectures
Subnetting, DNS, encryption technologies and standards, VPNs, VLANs, VoIP and other network routing methods
Network and web related protocols (e.g., TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols, etc.)
Advanced Persistent Threats (APT), phishing and social engineering, network access controllers (NAC), gateway anti-malware and enhanced authentication

C. To what extent does this job crossover into other areas on a daily basis?

☐ Within immediate work area or unit ☒ Within immediate department ☐ Within building
☐ Across several other departments ☐ Across the District

9. Safety to Self and Others

Indicate how the nature of this position and/or negligence in this position could impact the safety of the person or the safety of others. The following factors should be considered:

1. **Nature of injury** For example, cuts; bruises; burns; fractured bones; disease; repetitive stress or motion injuries; loss of limb, eyes, or life; disfigurement, etc.
2. **Cause of injury** For example, motorized power equipment, working in high or precarious places, exposure to radiation or asbestos, food poisoning, extensive keyboarding, handling bodily fluids, working in/near traffic, inclement weather, explosives, fumes, airborne particles, electric shock, etc.
   Recipient of injury For example, self, co-workers, peers, students, employees, District visitors, the general public, etc.
   Exposure to safety hazards or injury:
   Low exposure = Exposure is seldom, perhaps a few times per month for employees performing the job duties.
   Medium exposure = Exposure is more frequent, perhaps two times per week for employees performing the job duties.
   High exposure = Exposure is often, perhaps once a day or hourly for employees performing the job duties.

Complete ALL boxes that apply. Please indicate only the hazards that are due to the nature of this position and/or negligence in this position, not due to individuals that this position may supervise.

Injury	Injuries Associated with this Position (√)	Cause(s) of Injury (Specify)	Recipient(s) of Injury (Specify)	Exposure Level (Low, Med, High)
Bruises				
Cuts				
Burns: Chemical				

Burns: Heat				
Fractured bones				
Hernia				
Disease				
Repetitive motion or stress				
Loss of limb				
Loss of sight				
Disfigurement				
Fatality				

10. Working Conditions

The following information regarding this position is important to determine if accommodations can be made under the Americans with Disabilities Act (ADA). Please indicate the activities, demands, functions, and environments that are experienced in performing the essential job elements. **Indicate only the activities, demands, functions, and environments that this position is exposed to due to the primary nature of the job.** The categories below would affect either job performance or safety to oneself and/or to others. The amount of time indicated should reflect the portion of a work day where that activity, demand, function, or environment is encountered.

A. Physical Activities

	Amount of Time (√)			
	None	**Under 1/3**	**1/3 to 2/3**	**Over 2/3**
Stand		**X**		
Walk		**X**		
Physical Activities continued:	**Amount of Time (√)**			
	None	**Under 1/3**	**1/3 to 2/3**	**Over 2/3**
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 or hear			**X**	
Taste or smell	**X**			

B. 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**			

C. Vision Demands Indicate the vision skills required to successfully perform the essential functions of the job. Check all the boxes that apply. Indicate only the vision demands that are required to meet the essential duties of the job.

- ☒ No special vision requirements
- ☐ Close vision (clear vision at 20 inches or less)
- ☐ Distance vision (clear vision at 20 feet or more)
- ☐ Color vision (ability to identify and distinguish colors)
- ☐ Peripheral vision
- ☐ Depth perception
- ☐ Ability to adjust focus

D. 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**			

E. **Noise** Select the level of noise that is typical in the work environment for this job.

☐ Very quiet ☒ Quiet ☐ Moderate ☐ Loud ☐ Very loud

F. **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**	
Mental Functions continued:	**Amount of Time (√)**			
	None	**Under 1/3**	**1/3 to 2/3**	**Over 2/3**
Use interpersonal skills			**X**	
Compile		**X**		
Negotiate		**X**		
Other (specify)				

11. Other Information

Use the space below to record any other information that you feel should be considered in developing the job description for this position.

12. Participant Signature

Participant Signature(s) Date

PLEASE FORWARD YOUR COMPLETED QUESTIONNAIRE TO YOUR SUPERVISOR FOR REVIEW AND SIGNATURE.

OBTAIN YOUR SUPERVISOR'S SIGNATURE ON PAGE 1 IF YOU RECOMMEND A TITLE CHANGE FOR THIS POSITION. Title change recommendations will not be considered by Human Resources without a supervisor's signature.

13. Supervisor Comments and Signature

Please review the employee's responses to this questionnaire. Does he or she adequately describe the requirements and tasks to perform this position? If you believe changes are necessary, note the changes below or write in the changes in a different color ink in the appropriate section of the questionnaire **without changing the employee's response.** Please also review the changes with the employee.

Your signature acknowledges that you have read this questionnaire and, excluding any edits or comments you make, you agree with its contents.

Jeremy Heide

Supervisor's Signature Jeremy Heide Telephone No. 303-655-2912 Date 09/24/2018

After you and your supervisor have reviewed and signed this questionnaire, please forward it to the Human Resources Department at the Administration Building. Thank you.

Attachment A

Information Security Architect

- Acquire a complete understanding of a company's technology and information systems
- Plan, research and design robust security architectures for any IT project
- Perform vulnerability testing, risk analyses and security assessments
- Research security standards, security systems and authentication protocols
- Develop requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, and related network devices
- Design public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures
- Prepare cost estimates and identify integration issues
- Review and approve installation of firewall, VPN, routers, IDS scanning technologies and servers
- Test final security structures to ensure they behave as expected
- Provide technical supervision for (and guidance to) a security team
- Define, implement and maintain corporate security policies and procedures
- Oversee security awareness programs and educational efforts
- Respond immediately to security-related incidents and provide a thorough post-event analysis

Cont.

- Create new ways to solve existing production security issues
- Configure and install firewalls and intrusion detection systems
- Perform vulnerability testing, risk analyses and security assessments
- Investigate intrusion incidents, conduct forensic investigations and mount incident responses
- Collaborate with colleagues on authentication, authorization and encryption solutions
- Evaluate new technologies and processes that enhance security capabilities
- Test security solutions using industry standard analysis criteria
- Respond to information security issues during each stage of a project's life cycle
- Supervise changes in software, hardware, facilities, telecommunications and user needs
- Define, implement and maintain district security policies
- Analyze and advise on new security technologies and program conformance
- Recommend modifications in legal, technical and regulatory areas that affect IT security
- Strong understanding of IP, TCP/IP, and other network administration protocols
- Python, Powershell or similar scripting language knowledge
- Member of the incident response team to include detecting, responding and containing internal and external cyber-attacks across the enterprise network.
- Update and upgrade security systems as needed
- Knowledge of HP/DELL server, HP Networking, CISCO firewall/routers, Aruba wireless