Lead Information Security Specialist

Job Code	20001122	**Job Family**	Technology		
Department	ITS Information Security	**Reports to**	Sr Mgr ITS Information Security	**Union Status**	Non-Represented
FLSA Status	Exempt	**Pay Grade**	2060		
Last Updated	10/01/2025				

Accountability for Workplace Culture

Our PUD values are at the center of our culture. Putting the safety, health, and well-being of our communities and those we work with is valued above all else and everyone on Team PUD must meet this commitment daily. Nothing we do in achieving our Mission is worth a single injury, and all who interact with us must feel they are valued and welcomed as individuals.

Everyone on Team PUD, in all positions, is accountable for achieving this safe and welcoming culture by:

1. Taking full ownership for the safety of themselves and their coworkers, while ensuring everyone feels valued and welcomed.
2. Taking action to identify and eliminate their own and others' at-risk behaviors, including the behaviors that may undermine another's feelings of being welcomed and valued.
3. Following all safety rules and regulations and ensuring the PUD's expectations for conduct and respect are maintained.
4. Openly sharing near-misses, safety learning opportunities, and ways we can learn to be a more welcoming place while encouraging others to do the same.
5. Utilizing Stop Work Authority to intervene with anyone, anytime, in any place.
6. Intervening or seeking guidance to stop actions that are harmful to the wellbeing, health, or sense of belonging of others, and which are detrimental to our PUD values.

Job Summary

The Information Security Lead is responsible for safeguarding District information systems, data, and networks against threats, vulnerabilities, and cyber attacks. This role is accountable for delegating and/or overseeing a team on the installation, configuration, and management of security technologies—including firewalls, data encryption, and cloud-based monitoring tools—and ensuring compliance with security and regulatory standards. The Team Lead prepares incident reports, contributes to the design and implementation of security systems, and supports the identification, prioritization, and resolution of infrastructure and security issues that may impact business operations. Provides comprehensive support to employees, while managing other complex projects independently.

In addition, this position drives the strategic development of security programs and services for the District and its stakeholders. The Team Lead owns the business strategy behind these initiatives, defines functional requirements, and manages the launch of new features and capabilities. Coordinating across multiple teams, the role ensures alignment with organizational goals and overall success of the security program.

Accountabilities

Accountability #1

Security Program Strategy, Roadmap & Fiscal Stewardship

Set the strategy, roadmap, and feature definition for security programs and services; influence how they are designed, built, and launched by orchestrating planning, prioritization, and execution. Lead in leveraging technology and prudently managing costs to deliver outstanding value to our customers and stakeholders by adhering to best practices and standards, participating in infrastructure, software, and vendor selections, and providing input to solutions that continually enhance operational processes, and similar responsibilities.

Accountability #2

Business Innovation, Service Excellence & Continuous Improvement

Increase service excellence and customer satisfaction through the exploration of new ways to improve existing programs and services; monitor and analyze market trends and practice continuous improvement. Participate in and lead the implementation of system changes and the deployment of new systems based on business needs, including configuration/development/administration, testing, documentation, time and effort estimation, and status updates to project management—generally prioritizing changes with higher risk and business impact—to ensure delivery of quality technical solutions that reliably and sustainably meet the needs of the District, and similar responsibilities.

Provide leadership to staff on new system deployments adhering to best practices and standards, provide direction and guidance to ensure timelines and system deliverables are met.

Accountability #3

Cyber Security (Security, PII and Confidentiality) & Compliance

Achieve the highest level of employee and community trust in how the District manages data and system security by leading in the security and confidentiality of technological systems, processes, and data. Apply cybersecurity best practices through system administration, development, and configuration; ensure access to protected data (PII, HIPAA, etc.) is limited to authorized personnel; provide input to solutions that ensure cybersecurity; and continually adjust operational processes to improve and ensure security and privacy requirements and compliance to all applicable standards by following established processes, and similar responsibilities.

Accountability #4

Systems Operations & Program Delivery

Ensure program and service requirements are understood through regular interface with development leads and stakeholders; suggest workable solutions with consideration for contracting, positioning, and customer requirements. Ensure timely and quality release of program and service enhancements by managing prioritization and trade-offs between customer experience, business impact, performance, and post-launch support while working cross-functionally with design and technology teams. Achieve the highest level of employee and community trust in how the District manages systems operations by leading the configuration, administration, support, and maintenance of the District's computer systems to ensure they are highly available and ready for use; install, set up, and test hardware and software systems; troubleshoot and resolve technical issues and implement improvements using recognized methodologies (e.g., Agile, ITIL, industry standards), and similar responsibilities.

Accountability #5

Customer & Service Engagement

Ensure customer understanding and adoption of programs and services through the development and delivery of training and post-launch support. Build awareness and understanding of new and enhanced services by acting as a subject matter expert and creating buy-in for the program vision internally and with key external partners. Provide customer service (internal and external) through effective communication and collaboration to ensure technology needs are met in support of the District's mission of providing reliable and cost-effective service; build and maintain effective relationships with stakeholders (e.g., customers, peers, cross-functional partners, external vendors, alliance partners); lead and model an inclusive and equitable working environment that encourages every team member to share ideas in an open and inclusive manner, provide postive development and similar responsibilities.

Accountability #6

Leadership & Mentorship

Contribute to career growth opportunities for other security staff through coaching and mentoring, and similar responsibilities. Create a culture of caring, mutual respect, and trust that empowers employees to do their best work by serving as a lead, coach, mentor, and trainer to other employees.

Accountability #7

Accountability #8

Accountability #9

Accountability #10

Minimum Qualifications Note

The minimum qualifications listed below are representative of the knowledge, skills, and abilities needed to perform this job successfully, as described in the Accountabilities. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential Accountabilities (duties and responsibilities) of this position. If you need assistance and/or a reasonable accommodation due to a disability during the application or recruiting process, please contact Human Resources at HRRecruiting@snopud.com, or by phone at 425-783-8655.

Qualifications – Education and Experience

Minimum **Required Education and Experience:**

Bachelor's Degree in Computer Science, Information Technology, Business/Public Administration, or related field, AND
Six (6) years of experience in Information Technology, program or product management, service delivery, account management, or related;

OR

Associate's Degree in Computer Science, Information Technology, or related field, AND Eight (8) years of Information Technology experience; program or product management, service delivery, account management, or related

OR

Ten (10) years of Information Technology experience, program or product management, service delivery, account management, or related.

Preferred **Education and Experience:**

Qualifications – License(s) and/or Certification(s)

Minimum **Required License(s) and/or Certification(s):**

Preferred **License(s) and/or Certification(s):**

Any Information Technology or Information Security certification from any of the following recognized industry groups, or equivalent: $(ISC)^2$, CompTIA, ISACA, SANS, GIAC, EC-Council, ITIL

Qualifications – Skills and Abilities

Minimum **Required Skills and Abilities:**

Information (cyber) security principles
Data classification and privacy principles
Identity and Access Management (IAM) principles
Communicate effectively, both verbally and in writing, with internal customers, contractors, and outside agencies.
Participate as a team member at various levels and across department and functional lines.
Promote the success of others and constructively resolve disagreements.
Research, investigate, and resolve problems.
Collect data from various sources and analyze and develop reports/documents.
Use computers, automated systems, and databases.

Learn, identify, interpret, apply, and communicate related District programs, projects, methods, and procedures.
Learn, interpret, and apply District Directives.
Coordinate a variety of tasks simultaneously.
Use independent and discretionary judgment in accordance with leadership-defined criteria.
Handle confidential information.
Work in a flexible, self-directed team environment.
Develop and maintain project and program schedules.
Meet critical timelines and deadlines.
Adapt and change priorities as necessary
Firewall configuration principles
Information technology backup and disaster recovery principles
Utility industry and public organization regulatory compliance standards
Information Technology Infrastructure Library (ITIL) IT Service Management practices
IT architecture principles
Provide work direction, guidance and technical assistance to others
Assist in training other department personnel in the area of expertise
Overall leadership and management principles, methodologies, tools and skills

***Preferred* Skills and Abilities:**

Research and analysis principles
Presentation skills and techniques
Familiarity with auditing principles
Report writing principles
Contracts and purchasing processes
Financial planning and budget development

Competencies

The following competencies describe the cluster of behaviors associated with job success in the job group identified as “Leader” at the Manager level.

Adaptability
Aligning Performance for Success
Building Customer Relationships
Building Talent
Coaching
Communication
Continuous Improvement

Continuous Learning
Courage
Creating a Culture of Trust
Creating an Inclusive Environment
Customer Focus
Delegation and Empowerment
Driving for Results
Driving Innovation
Emotional Intelligence Essentials
Empowering Decision Making
Execution
Guiding Team Success
Initiating Action
Inspiring Others
Leveraging Feedback
Positive Approach
Professional Knowledge and Aptitude
Selecting Talent
Stress Tolerance
Technology Savvy

Physical Demands

Physical Demands List	Frequency
Sit	Frequent (34-66%)
Walk	Seldom (1-10%)
Stand	Frequent (34-66%)
Drive	Seldom (1-10%)
Work on ladders	Seldom (1-10%)
Climb poles or trees	Never
Work at excessive heights (note heights in open text box below)	Never
Twist	Seldom (1-10%)
Bend/Stoop	Seldom (1-10%)
Squat/Kneel	Seldom (1-10%)
Crawl	Never
Reach	Seldom (1-10%)
Work above shoulders (note specific activity in open text box below)	Seldom (1-10%)
Use Keyboard /mouse	Constant (67-100%)
Use wrist (flexion/extension)	Constant (67-100%)
Grasp (forceful)	Constant (67-100%)

Fine finger manipulation	Constant (67-100%)
Operate foot controls	Seldom (1-10%)
Lift (note weight in open text box below)	Seldom (1-10%)
Carry (note weight in open text box below)	Seldom (1-10%)
Push/Pull (note specifics in open text box below)	Seldom (1-10%)
Work rapidly for long periods	Occasional (11-33%)
Use close vision	Constant (67-100%)
Use distance vision	Seldom (1-10%)
Use color vision	Constant (67-100%)
Use peripheral depth perception	Never
Speak	Constant (67-100%)
Hear	Constant (67-100%)

Additional Physical Demands not listed above and associated frequency below.

Mental Demands

Communication	**Frequency**
Understand and carry out simple oral instructions	Frequent (34-66%)
Understand and carry out complicated oral instructions	Frequent (34-66%)
Train other workers	Frequent (34-66%)
Work alone	Frequent (34-66%)
Work as a member of a team	Frequent (34-66%)
Follow standards for work interactions	Constant (67-100%)
Write communications for clarity and understanding	Constant (67-100%)
Speak with clarity with others	Constant (67-100%)
Comprehension	**Frequency**
Read and carry out simple instructions	Constant (67-100%)
Read and carry out complicated instructions	Constant (67-100%)
Retain relevant job information	Constant (67-100%)
Reasoning	**Frequency**
Read and interpret data	Constant (67-100%)
Count and make simple arithmetic additions and subtractions	Occasional (11-33%)
Use intermediate and/or advanced math	Occasional (11-33%)
Organization	**Frequency**
Plan own work activities	Constant (67-100%)
Plan work activities of others	Frequent (34-66%)

Direct work activities of others	Frequent (34-66%)

Resilience	**Frequency**
Work under pressure	Frequent (34-66%)
Work for long periods of time	Frequent (34-66%)
Work on several tasks at the same time	Frequent (34-66%)

Additional Mental Demands not listed above and associated frequency below.

Work Environment

Environmental Conditions List	**Frequency**
Exposure to weather	Never
Wet and/or humidity	Never
Atmospheric conditions	Never
Confined/restricted working environment	Never
Vibratory Tasks – High	Never
Vibratory Tasks – Low	Never

Additional Environmental Conditions in this job not listed above and the associated frequency below.

Risk Conditions List	**Frequency**
Exposure to Heights	Seldom (1-10%)
Exposure to Electricity	Seldom (1-10%)
Exposure to Toxic or Caustic Chemicals	Never
Working with Explosives	Never
Exposure to Radiant Energy	Never
Extreme Cold	Never
Extreme Hot	Never
Proximity to Moving Mechanical Parts	Never
Noise Intensity	Never
Exposure to animals	Never
Working with angry customers	Seldom (1-10%)

Additional Risk Conditions present in this job not listed above and the associated frequency below.

On-Call Status and Frequency

On-Call is required.

○ Yes
⊙ No

On-call activities and frequency.

Work Location

The primary assignment for this position is:

○ Remote
⊙ Office Hybrid
○ On-Site
○ Field/Job Site

While this description has provided an accurate overview of responsibilities, it does not restrict management's right to assign or reassign duties and responsibilities to this job at any time. This position description is designed to outline primary duties, qualifications, and job scope, but not limit our employees or the organization to complete the work identified. In order to serve our customers best, each employee will offer their services wherever and whenever necessary to ensure the success of the District in serving our customers, to further the safety, health, and inclusivity of employees and the public, and achieve expectations of the District overall, while also remaining flexible in recognition of the employee's wellbeing.