Senior Manager, Information Security

Job Code	20000337	**Job Family**	Technology	**Leader**	
Department	Security Architecture	**Reports to**	Chief Information Officer	**Union Status**	Non-Represented
FLSA Status	Exempt	**Pay Grade**	2063		
Last Updated	12/1/2022				

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 Senior Manager, Information Security is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. Coordinates and leads employees and staff in planning, designing, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology (IT) risks, respond to incidents, establish appropriate standards and controls, manage security technologies, and leads the development and implementation of policies and procedures. Leads the District's enterprise cyber security program. Establishes an enterprise cyber security framework for all District technology through development of strategic plans and vision, policy, business processes, systems architecture, selection of security technologies, and training. Manages security compliance objectives and controls through evaluation, testing, remediation, vulnerability audits and assessments. Continually improves internal controls and processes for risk management and operational efficiency. Serves as the senior cyber security consultant to senior and executive leadership. Assesses the disruptive forces, economic, financial implications and risks of a cyber compromise and leads the District's cyber posture defense response planning and technology investment decisions to ensure Districts is protected. Promotes the business value of cyber security as an enabler of strategy formulation, and as support for technology innovation, which drives the organization's top and bottom lines.

Accountabilities

Accountability #1

Cyber Security and Information Protection:

Achieve the highest level of employee and community trust in how the District manages cyber security by ensuring the District-wide operations and strategic direction of technological systems, processes, and data that support District wide operations and all customer delivery are cyber secure. Provides leadership and support to all employees in the adherence to cyber and information security best practices, designs, and standards for protection of sensitive and/or confidential data; seeks the strongest possible cyber security and privacy data controls in vendor system solutions and processes, contract negotiations and project requests; provides vision and direction to strategic planning to prepare the District for future cyber security and confidentiality solutions architecture. Ensures the configuration, administration, support and maintenance of the District's cyber and information security systems. Leads the installation, development, configuration, and testing of hardware and software-based security technologies. Collaborates to troubleshoot and resolve technical issues as they arise. Provides customer support by responding to all technology requests. Generally, leads on development, change decisions and troubleshooting for high risk systems and enterprise wide business impacts or similar work. Leads cultural change in cyber security and information handling through active engagement across the District, and similar responsibilities.

Accountability #2

Business Innovation and Continual Improvement:

Deliver exceptional value to our customers through continual improvement and innovation by ensuring all aspects of implementation of enterprise system changes based on business needs. Develops cyber security technology strategies to support District strategic initiatives. Leads and manages cyber security and information protection aspects of implementation of enterprise system changes based on business needs, providing technical expertise to support the analysis, evaluation of options, and solutions. Leads research, assessment, and pilot projects to support future cyber security technology solutions and strategy. Oversees cyber security system configuration, administration, testing, and documentation of both emerging and legacy technologies to ensure delivery of quality technical solutions that reliably and sustainably meet the needs of the District. Provides mentorship to technology workers across the District. Generally, works on changes with high risk and business impact, and similar responsibilities.

Accountability #3

Fiscal Management:

Deliver exceptional value to our customers through fiscally responsible planning and management by ensuring development and delivery of cost effective and efficient technology systems and maintenance, adhering to cyber security best practices and standards on behalf of our customers and stakeholders. Ensures systems meet reliability and availability Key Performance Metrics. Designs solutions that provide value and continually enhance operational processes. Ensures vendor management complies with cyber security adherence to contract terms and service levels. Provides cyber security needs to strategic planning to gain the most value from vendor services in support of implementations and ongoing operations and similar responsibilities.

Accountability #4

Compliance:

Achieve the highest level of employee and community trust in how the District manages compliance by ensuring the regulatory compliance of corporate and operational technological systems and processes and data on behalf of our customers and stakeholders, providing leadership to staff in development, adherence to and the continual improvement of operational best practices and standards for compliance; seeks and maintains regulatory compliance vendor relationships, contract negotiations and project requests; and providing direction to strategic planning to prepare us for future compliance solutions; may be responsible for managing one or more regulatory requirements or sub-requirements, and similar responsibilities.

Accountability #5

Cross-Functional Collaboration and Customer Service:

Demonstrate powerful cross-Functional Collaboration and Customer Service (internal and external) that proactively anticipates and supports community and customer needs by effective communication and collaboration to ensure cyber security technology needs are met, supporting reliable and cost-effective service. Builds and maintains effective relationships with stakeholders inside and outside the organization (e.g., customers, peers, cross-functional partners, external vendors, alliance partners). Ensures the District is a valued partner in cyber and information security. Acts as the primary District representative to external organizations and agencies on matters of cyber and information security. Interacts with utility industry groups, state, and federal agencies to represent District needs, concerns, and efforts to ensure the District remains engaged with information security actions and trends. Scans the world for major disruptive technology and non-technology trends (trendspotting) that will affect the utility industry. Contributes to building and sustaining an inclusive and equitable working environment by supporting all District employees. Actively supports and encourages every team member to share their ideas in an open and inclusive manner and similar responsibilities.

Accountability #6

Policy Development:
Increase the public's confidence in the quality of governance by ensuring policy and directives are developed, distributed, and enforced to promote and reinforce cyber and information security. Constructs written policy to be easily understood by every employee. Composes, maintains, and clarifies the policies and procedures of the District governing information security, employee access, information handling, and use of information technology in a secure manner. Acts as a liaison between employees and District leadership to promote adherence to published policy and development of new policy to keep pace with evolving cyber security threats, and similar responsibilities.

Accountability #7

Management:
The Senior Manager, Information Security is accountable to achieve results for the cyber security. This is accomplished through clear ITS resource planning and skills need and alignment in support of business goals and objectives. Monitors and supports their team to determine opportunities for improvements. Responsible for talent acquisition to maintain and grow high performing teams. Coaches and develops managers and employees to increase performance while also identifying needs for new resources. Accountable for ensuring the ITS department performs at a high level of productivity, provide exceptional customer service, and respond effectively to issues as they arise. Leads by example in embracing a culture of continual improvement and service to the team, our customers, and the company. They establish standards for performance and employee interactions while ensuring accountability for alignment to goals. Proficient in and a champion for technology. Has a broad range of influence within ITS and across the District. They ensure systems are secure and help mitigate risks related to cyber security. Demonstrate capabilities to lead teams through demanding situations such as incident and change management. They must be resilient, calm, and professional in high stress and high workload situations. Fosters a diverse, equitable, and inclusive work environment. Supports the District safety programs. Responsible for effective communication to all levels of the organization. Demonstrates the ability to communicate technical concepts to business stakeholders in support of decision making and strategic planning. Capable of presenting to all levels of the organization and to various sizes of groups. Communicates effectively across all mediums (orally and written).

Accountability #8

Strategy and Planning:
The Senior Manager, Information Security establishes the strategic direction related to cyber security while ensuring alignment to District strategic goals to address new challenges, opportunities, and business

drivers. Leads several cross functional teams (direct reports and matrixed) to monitor, evaluate, and adjust the ITS strategic initiatives. Sets clear goals and defines KPIs to measure success. They determine roles, responsibilities and ensure appropriate collaboration within ITS and across the District. They ensure the plan is executed, monitored, and revised as needed. Must be knowledgeable about ITS and District goals, current technology portfolio, emerging technology trends (internal and external), and industry best practices (IT and utility). Must be able to coordinate and prioritize multiple high priority demands across several team to ensure success. Understands and optimizes resources (people, technology and processes) to deliver results in all areas (system support, projects, enhancements, and incidents as they arise). Responsible for working with managers and teams to develop and manage cyber security roadmaps for their domain.

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, Computer Engineering, Information Technology, Business or Public Administration, or related field, AND

Ten (10) years of directly related, progressively more responsible information technology services experience, including five (5) years of information security experience.

***Preferred* Education and Experience:**

Master’s Degree in Computer Science, Computer Engineering, Information Services, Business/Public Administration, or related field.

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

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

Must have one or more of the following certifications:
ISC2Certified Information System Security Professional (CISSP)
Systems Security Certified Practitioner (SCCP)
SANS GIAC Security Leadership
Security Essentials Certification

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

Qualifications – Skills and Abilities

***Minimum* Required Skills and Abilities:**

Knowledge of business ecosystems, SaaS, infrastructure as a service (IaaS), platform as a service (PaaS), SOA, APIs, open data, microservices, event-driven IT and predictive analytics
Familiarity with information management practices, system development life cycle management, IT services management, agile and lean methodologies, infrastructure and security operations, and national and international cyber security frameworks
Exceptional interpersonal skills, including team building, facilitation and negotiation
Strong leadership skills
Excellent analytical and technical skills
Excellent written, verbal, communication and presentation skills with the ability to articulate new ideas and concepts to technical and nontechnical audiences
Excellent planning and organizational skills
Knowledge of all components of holistic enterprise architecture
Knowledge of business engineering principles and processes
Familiarity with visual modeling approaches, tools, model libraries and standards
Knowledge of business models, operating models, financial models, cost-benefit analysis, budgeting and risk management
Understanding of agile principles, methodologies and frameworks, especially those designed to be scaled at the enterprise level
Understanding of existing, new and emerging technologies, processing environments, and cloud computing

Organizationally savvy and understanding of the political climate of the enterprise and how to navigate obstacles and politics
Balance the long-term (“big picture”) and short-term implications of individual decisions and organization goals
Translate business needs into cyber and information security requirements
Estimate the financial impact of cyber and information security alternatives
Apply multiple solutions to business problems
Rapidly comprehend the functions and capabilities of new technologies
Capable and comfortable with balancing time between foundational cyber security (Renovating the core of the IT state, ensuring efficiency and predictability) and future cyber security efforts (Concerned with business and operating model design, technology innovation, speed, agility and flexibility to achieve a unified and flexible cyber security posture that meets the organization’s needs)
Act in an innovative consulting manner to drive the organization’s digital business strategies

***Preferred* Skills and Abilities:**

Management ExperienceEnterprise security architecture
Enterprise security process and policy creationInformation management
Project management principles, practices, and methods
Problem identification, analysis, and troubleshooting
Business writing and presentation skills
Customer service marketing and engagement
Employee coaching and consulting
Budgeting and resource managementIdentity management
Network authentication
State and federal privacy laws and regulations
Utility systems and operations
North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards
Electricity - Information Sharing and Analysis Center (E-ISAC)
National Institute of Standards (NIST)
Federal Information Protection Standards (FIPS)
Business Continuity Planning and Disaster Recovery
Public Key EncryptionInternet Protocol (IP)-networking
Microsoft and Linux/UNIX operating environments
Governance and controls framework
Advanced Metering Infrastructure (AMI)
Wireless communications systems
Payment Card Industry Data Security Standard (PCI DSS)
Internet of Things (IoT) and peripheral devices
National and state-level intelligence gathering agencies
Multi-agency coordination and outreach efforts
Remote and teleworking technologies

Operational technology (OT) systems and architecture
Electric utility protection, control, and communication systems
Electric utility smart grid and automation systems
Physical security procedures and technologies
Understand and communicate in the language of the utility business

Competencies

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

Adaptability
Building Customer Relationships
Building Talent
Business Acumen
Coaching
Communication
Continuous Learning
Courage
Creating a Culture of Trust
Creating an Inclusive Environment
Cultivating Networks and Partnerships
Customer Focus
Delegation and Empowerment
Driving for Results
Driving Innovation
Emotional Intelligence Essentials
Facilitating Change
Financial Acumen
Guiding Team Success
Initiating Action
Inspiring Others
Leveraging Feedback
Planning and Organizing
Positive Approach
Professional Knowledge and Aptitude
Strategic Planning
Stress Tolerance

Physical Demands

Physical Demands List	Frequency
Sit	Constant (67-100%)
Walk	Occasional (11-33%)
Stand	Occasional (11-33%)
Drive	Seldom (1-10%)
Work on ladders	Never
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)	Never
Use Keyboard /mouse	Constant (67-100%)
Use wrist (flexion/extension)	Seldom (1-10%)
Grasp (forceful)	Seldom (1-10%)
Fine finger manipulation	Constant (67-100%)
Operate foot controls	Seldom (1-10%)
Lift (note weight in open text box below)	Never
Carry (note weight in open text box below)	Never
Push/Pull (note specifics in open text box below)	Never
Work rapidly for long periods	Occasional (11-33%)
Use close vision	Constant (67-100%)
Use distance vision	Occasional (11-33%)
Use color vision	Constant (67-100%)
Use peripheral depth perception	Occasional (11-33%)
Speak	Frequent (34-66%)
Hear	Frequent (34-66%)

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	Seldom (1-10%)
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	Frequent (34-66%)
Read and carry out complicated instructions	Frequent (34-66%)
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	Seldom (1-10%)
Organization	**Frequency**
Plan own work activities	Constant (67-100%)
Plan work activities of others	Occasional (11-33%)
Direct work activities of others	Occasional (11-33%)
Resilience	**Frequency**
Work under pressure	Constant (67-100%)
Work for long periods of time	Constant (67-100%)
Work on several tasks at the same time	Constant (67-100%)

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	Never
Exposure to Electricity	Never
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	Never

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.