Security Architect

Job Code	20001128	**Job Family**	Technology	**Professional / Knowledge Worker**	
Department	ITS Information Security	**Reports to**	Sr Mgr ITS Information Security	**Union Status**	Non-Represented
FLSA Status	Exempt	**Pay Grade**	2061	**This Job is a Lead**	No
Last Updated	05/19/2026				

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 Security Architect is responsible for designing, implementing, and maintaining the District's security architecture and technology to protect information systems, data, and networks from threats and vulnerabilities. This role provides technical leadership for security programs, ensures compliance with regulatory and industry standards, and drives the adoption of best practices across infrastructure, applications, and cloud environments. The Security Architect collaborates with their ITS peers, business units, and external partners to integrate security into projects and operations, leads incident response and risk assessments, and fosters a culture of innovation, continuous improvement, and security awareness throughout the organization.

Accountabilities

Accountability #1

Strategic Security Architecture & Fiscal Stewardship

Lead the development, alignment, and ongoing maintenance of the District's security architecture and associated technology portfolio, ensuring initiatives support enterprise business strategy and maximize value. Set the strategic roadmap for security technology and services, orchestrate planning and prioritization, and participate in infrastructure, software, and vendor selections. Provide expert input to solutions that enhance operational efficiency and cost-effectiveness and ensure prudent management of technology investments and resources.

Accountability #2

Innovation, Change Management & Continuous Improvement

Drive continual improvement and innovation by leading and supporting the implementation of system changes, adoption of new technologies, and process enhancements. Apply deep technical expertise to deliver robust, scalable, and sustainable solutions. Oversee configuration, development, testing, and documentation, estimate and manage project scope and resources, and proactively consult across business and technical areas to define and influence future direction. Monitor industry trends and best practices to ensure the organization remains at the forefront of security and technology advancements.

Accountability #3

Cybersecurity, Compliance & Risk Management

Lead the development of secure systems architectures to ensure confidentiality, integrity, availability, and compliance of systems, data, and processes. Apply information security best practices, conduct risk assessments, and enforce regulatory and organizational standards (e.g., PII, PCI, HIPAA, NERC-CIP). Monitor systems for compliance with District standards and best practices. Oversee access controls for

protected data, develop and test disaster recovery and business continuity plans, and monitor emerging threats and trends. Lead or support incident response activities, including investigation, containment, and reporting, and ensure continuous improvement of security and privacy controls.

Accountability #4

Operational Support & Service Excellence

Lead the configuration, administration, support, and maintenance of security technology systems to ensure high availability, reliability, and readiness for business operations. Troubleshoot and resolve technical issues, implement and monitor improvements, and provide responsive customer support using recognized best practices and methodologies (e.g. ITIL). Maintain a thorough understanding of the organization's products, processes, and services, and ensure operational support aligns with business needs and service level expectations.

Accountability #5

Collaboration, Stakeholder Engagement & Governance

Build and maintain effective partnerships with internal and external stakeholders, integrating security requirements into projects, operations, and organizational initiatives. Participate in, and/or lead, governance boards (e.g., Architecture Review Board, Change Advisory Board), represent the organization to external forums and industry groups, peer utilities, and regulatory bodies. Communicate complex security concepts clearly, deliver training and post-implementation support, and ensure alignment with organizational goals, enterprise risk, and customer needs.

Accountability #6

Leadership, Mentorship & Talent Development

Provide leadership, coaching, and mentorship to Information Security, ITS, and technical staff from business units in information security, security architecture, and related topics - promoting a collaborative, inclusive, and high-performing environment. Develop and deliver training and awareness programs to promote security best practices, support career growth and professional development, and model behaviors that create a culture of mutual respect, trust, and continuous learning. Guide and assist team members in technical and professional matters to ensure the team is equipped to meet current and future security challenges.

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 Information (Cyber) Security, Computer/Information Sciences, or related field AND
Six (6) years progressively more responsible information technology/security experience

OR

Ten (10) years progressively more responsible information technology/security experience

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 of the following and/or equivalent: ISC2 Certified Information Systems Security Professional (CISSP); CompTIA Security+; CompTIA Advanced Security Practitioner (CASP+); ISC2 Systems Security Certified Practitioner (SSCP); GIAC Security Essentials (GSEC); ISACA Certified Information Systems Auditor (CISA); ISACA Certified Information Security Manager (CISM)

Qualifications – Skills and Abilities

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

Deep knowledge of information and cyber security principles, frameworks, and best practices.

Strong understanding of identity and access management (IAM), network security methods, and cloud security architecture.

Ability to design secure network communications aligned with utility industry best practices and regulatory requirements.

Experience designing, implementing, and supporting SaaS, cloud, and on-premises architectures.

Experience with regulatory compliance (e.g., NERC-CIP, HIPAA) and defining compliance processes and strategies.

Skilled in defining system and infrastructure specifications, interfaces, hardware capacity, and performance standards.

Experience with high availability, backup, and disaster recovery strategies.

Ability to develop infrastructure standards, processes, and procedures, and recommend emerging technologies.

Experience with IT architecture principles and integration strategies for enterprise systems.

Familiarity with secure software engineering/development principles and their impact on applications security.

Ability to lead cross-functional teams and manage multiple priorities.

Strong collaborative skills with commitment to team success.

Experience managing vendor deliverables and expectations.

Skilled in influencing IT policies, principles, standards, and design patterns.

Supports strategic priorities, digital innovation, and continual improvement initiatives.

Strong analytical, critical thinking, and risk assessment skills.

Expertise in root cause analysis and troubleshooting complex, multi-system issues.

Ability to apply structured approaches to problem identification and solution development.

Independent judgment with risk and impact analysis in decision-making.

Excellent communication and interpersonal skills; able to convey complex concepts to technical and non-technical audiences.

Experience communicating with diverse audiences using exceptional oral, written, and presentation skills.

Familiarity with ITIL, Agile, and project management methodologies.

Experience with/understanding of OSI layers, TCP/IP stack, and common internet protocols/services

Experience assessing and planning transformational technologies.

Ability to analyze marketplace, industry, and technology trends to inform business and IT strategy.

Ability to define KPIs to measure performance, availability, and benefit realization of enterprise solutions.

Preferred **Skills and Abilities:**

Competencies

The following competencies describe the cluster of behaviors associated with job success in the job group identified as “Professional / Knowledge Worker”.

- Adaptability
- Building Customer Loyalty
- Building Partnerships
- Communication
- Continuous Improvement
- Continuous Learning
- Courage
- Decision Making
- Earning Trust
- Emotional Intelligence Essentials
- Facilitating Change
- Influencing
- Initiating Action
- Innovation
- Leveraging Feedback
- Mentoring
- Planning and Organizing

- Positive Approach
- Professional Knowledge and Aptitude
- Stress Tolerance
- Technology Savvy
- Valuing Differences
- Work Standards

Physical Demands

Physical Demands List	Frequency
Sit	Frequent (34-66%)
Walk	Seldom (1-10%)
Stand	Seldom (1-10%)
Drive	Never
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)	Constant (67-100%)
Grasp (forceful)	Constant (67-100%)
Fine finger manipulation	Constant (67-100%)
Operate foot controls	Never
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)	Never
Work rapidly for long periods	Occasional (11-33%)
Use close vision	Constant (67-100%)
Use distance vision	Seldom (1-10%)
Use color vision	Never
Use peripheral depth perception	Never
Speak	Occassional (11-33%)
Hear	Frequent (34-66%)

Additional Physical Demands not listed above and associated frequency below.
Lift/Carry: 10lbs.

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	Constant (67-100%)
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	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.