CLASS SPECIFICATION

Class Code: 60019857
Date Established: 07/2026
Last Reviewed:
Last Revised:
Last Title Change:
FLSA: Exempt
Probation: 12 months

CHIEF INFORMATION SECURITY OFFICER

DEFINITION

Under administrative direction, responsible for the strategy, governance, and operational management of information and cyber security to protect the confidentiality, integrity, and availability of Washoe County services and data; provides direct oversight for Washoe County's enterprise-wide information security program; and performs related work as required.

EXPERIENCE AND TRAINING REQUIREMENTS

Eight years of full-time experience in information security and technology infrastructure AND a bachelor's degree in information security, computer science, information systems, or a closely related field; OR an equivalent combination of training and experience.

LICENSE OR CERTIFICATE

A valid driver's license is required at the time of appointment and must be maintained for continued employment in this classification.

SUPERVISION EXERCISED

May exercise direct supervision.

EXAMPLES OF DUTIES *(The following is used as a partial description and is not restrictive as to duties required.)*

Develop, implement, and maintain a comprehensive County-wide cybersecurity strategy aligned with organizational objectives and best practices; establish and maintain cybersecurity governance, policies, standards, and procedures in accordance with applicable laws, regulations, and recognized frameworks.

Develop departmental assessment and provide awareness of cybersecurity risks with departments to ensure departments comply with data privacy and governance policies; establish and maintain County-wide security awareness and training programs for employees and contractors, including role-based training where needed.

Serve as the primary cybersecurity advisor to executive leadership, department heads, and elected officials; provide clear and concise briefings on cybersecurity posture, risk analysis, and funding priorities; define and maintain clear security ownership across disciplines including governance/risk/compliance (GRC), security operations (SecOps), identity and access management (IAM), application security (AppSec), data security, and third-party risk management.

Supervise assigned staff, which includes staff selection; assigning, scheduling, and reviewing work; providing training in proper work methods and procedures; providing professional development, coaching, and mentoring; writing performance evaluations; and implementing discipline and conflict resolution procedures when necessary.

Lead the County's cybersecurity risk management program, including maintaining an enterprise risk register, conducting risk assessments, and implementing prioritized mitigation plans; oversee security operations including threat detection and response, vulnerability management, security monitoring, and incident response coordination across County environments.

Serve as the senior technical escalation point during cybersecurity incidents; lead investigation, containment, eradication, recovery, and post-incident reporting; define incident response service level expectations and ensure timely closure of remediation actions and lessons learned.

Develop, test, and maintain incident response protocols and lead regular tabletop exercises with technical teams and executive stakeholders; ensure ransomware resilience practices are implemented and tested, including secure backups, recovery objectives, and segmentation where appropriate.

Oversee security monitoring and detection capabilities and ensure timely investigation and response to alerts; establish and enforce security architecture standards across County systems and departments; coordinate security aspects of business continuity and disaster recovery (BC/DR), ensuring cyber scenarios are incorporated into continuity planning.

Define security requirements in requests for proposals (RFPs) and contracts, and conduct third-party/vendor risk assessments before onboarding; lead third-party/vendor risk management including security assessments, contract security requirements, and ongoing oversight of vendor performance.

Review and approve security designs, configurations, and technical standards for County systems and third-party integrations; lead implementation of modern defensive strategies such as Zero Trust principles, MFA/conditional access, network segmentation, secure remote access, and least privilege.

JOB RELATED AND ESSENTIAL QUALIFICATIONS

Full Performance Level *(These may be acquired on the job and are needed to perform the work assigned.)*

Knowledge of:
Department/division policies and procedures.

Organizational structure, systems, and functions of Washoe County and local governments.

Local, state, and federal laws and regulations relevant to cybersecurity.

Various hardware, software and network equipment and systems; voice/data network and transmission technology; functions and operational requirements specific to Washoe County.

Emerging cybersecurity trends, threats, modern attack techniques and defensive strategies.

Washoe County purchasing and contract administration practices and procedures.

Countywide personnel policies such as sexual harassment, discrimination, ADA, and EEO.

Principles and practices of effective supervision including leadership, motivation, development, team building, conflict resolution, employee training, performance evaluation, and discipline.

Ability to:
Plan, coordinate, and direct the operations of the information security program to accomplish established goals and maximize efficiency.

Supervise personnel, including training, assigning and reviewing work, administering discipline and conducting performance evaluations.

Effectively represent the County in cybersecurity collaborations with state, regional, and federal partners, including information-sharing initiatives and incident coordination.

Interpret and negotiate terms and conditions within RFPs and contracts.

Interpret and adhere to Washoe County's technology plan and provide strategic recommendations and input to the plan.

Establish and maintain data classification, encryption, and data handling standards aligned to the County's risk and regulatory requirements.

Entry Level *(Applicants will be screened for possession of these through written, oral, performance, or other evaluation methods.)*

Knowledge of:
Principles and practices of information security technology, cybersecurity frameworks, cybersecurity threats, vulnerabilities, and mitigation strategies.

Complex information technology and telecommunications networks, including IP-based networks and RF/wireless architectures.

Security monitoring tools and practices (e.g., SIEM, EDR/XDR), IAM, and data protection technologies.

Methods and techniques for enterprise risk management, audits, and risk assessments.

Principles and practices of strategic planning and effective collaboration across departments, divisions, and cross functional teams.

Principles of program planning, implementation, and administration.

Ability to:
Analyze information, project consequences of proposed actions, formulate alternative solutions and make appropriate responses or recommendations.

Evaluate programs or projects to determine their effectiveness in meeting goals and objectives and develop and implement program or project modifications.

Interpret and apply pertinent laws, regulations and standards including organizational policies and procedures.

Communicate cybersecurity risks, trends, and incidents in clear, non-technical terms.

Develop and deliver effective written and oral presentations, reports, correspondence, and other materials.

Communicate effectively, both orally and in writing.

Establish, maintain, and foster effective and positive working relationships with all those contacted in the course of work.

SPECIAL REQUIREMENTS *(Essential duties require the following physical skills and work environment.)*

Ability to work in a professional office environment. Ability to lift and move objects weighing up to 25 lbs.

Must be available to work during cybersecurity incidents, disaster, or emergency situations which occur outside of normal working hours.

Must be able to travel as necessary for conferences, trainings, and meetings with other agencies.

This class specification is used for classification, recruitment, and examination purposes. It is not to be considered a substitute for work performance standards.