Chief Information Security Officer (CISO)

FLSA: Exempt	**Bargaining Unit/Contract**: AT-Will	**Reports to**: Director of Information Technology
Location: Bridgeport/Mammoth Lakes	**Salary/Level**: 116	**Position Type**: Full-Time
EEO Category: 1	**BOS approval Date**: 07/2024	**Last Revision**: 11/2024

About the role

As a Chief Information Security officer (CISO) under the administration direction of the Director of Information Technology, the Chief Information Security Officer plans, organizes, implements and directs the County-wide information security program; and performs related duties as required.

DISTINGUISHING CHARACTERISTICS

The incumbent in this single position class reports directly to the Information Technology Director and is responsible for advising and training County departments on the proper management of security risks to their information systems and assets, directing and overseeing the County's defensive architecture systems and efforts, monitoring County information/computer assets for compromise, assisting in the recovery of compromised assets, overseeing the investigation of suspicious computer-related activities, developing County-wide policies and procedures, and overseeing end-user security awareness efforts. This position will focus executive and management attention on the secure and uninterrupted operation of County information systems through minimization of exposure and vulnerability to risk and loss factors.

The Chief Information Security Officer is distinguished from the next higher class of Information Technology Director in that the latter is responsible for the overall development and successful implementation of the policies, goals, and mission of the Information Technology Department and satisfying the information technology requirements and needs of the entire County.

CLASSIFICATIONS SUPERVISED:

n/a

EESSENTIAL DUTIES AND RESPONISBILITIES

Nothing in this specification restricts management's right to assign or reassign duties and responsibilities to this job at any time.

1. Develops, establishes, implements, and directs the County's information technology security program across all departmental divisions and units
2. Develops, coordinates, and maintains policies pertaining to information technology security
3. Works with County-wide task forces, committees, and departmental liaisons to implement security policies, procedures, and infrastructure modifications
4. Acts as the central point of contact related to violations of information technology security policies and investigates or assists in the investigation of violations
5. Writes and maintains appropriate reports and records
6. Upon request, conducts security risk assessments, and business impact analysis of all County departments, in coordination with departmental security assessment teams/staff
7. Acts as a consultant to all County information technology functions in the review of security policies, computer operations, access controls, system security, computer applications, and network and data security
8. Develops, promotes, and presents security awareness education to all levels of the County organization
9. Reviews all system-related information security plans throughout the County's network to ensure alignment between security practices
10. Maintains current knowledge of applicable federal and state laws, accreditation standards, and monitors information security technologies to ensure organizational adoption and compliance; maintains up-to-date knowledge of general threats to local government and methods of attack
11. Plans, prioritizes, delegates, and reviews of the work of assigned staff
12. Develops and leads and trains the Information Security Response Team; coordinates all incident preparedness activities
13. Consults with the County Counsel's Office to provide legal investigative services related to information technology
14. Coordinates with the Network Infrastructure Team on the monitoring of County systems and networks for malicious or unusual activity that may allow unauthorized access and/or attacks, such as the presence of malware, viruses, worms, botnets, backdoors, and runaway services
15. May be assigned as a Disaster Service Worker as required
16. Performs other related duties as required

QUALIFICATIONS

A combination of experience, education, and/or training which substantially demonstrates the following knowledge, skills, and abilities:

Knowledge and Skills:

Thorough knowledge of:

1. Principles and methods used in the analysis and development of information security systems and procedures
2. Principles of management and supervision
3. Currently accepted information security standards, guidelines and theories
4. Knowledge of computer networking protocols, infrastructure principles and practices
5. Information technology equipment operation, capacity and capability
6. Analytical techniques relating to the assessment of business needs and the generation of management decision making information
7. Information technology security practices

8. Current information security regulations, including Federal Information Security Management Act, Federal Risk and Authorization Management Program, Federal Information Processing Standard, National Institute of Standards and Technology, Health Insurance Portability and Accountability Act, Personally Identifiable Information, and Protected Health Information, and various other laws, regulations and statutes
9. Hacker tools and techniques used to gain unauthorized access to computer systems
10. Currently accepted information security standards, guidelines, and theories
11. Knowledge of risk management processes

Skills and Ability to:

1. Analyze, assess, and interpret complex data, policies, procedures, regulations, and legislation
2. Understand and apply the technologies used to collect, access, store, and transmit information in all forms
3. Identify information security needs for the County
4. Skill in evaluating laws and regulations
5. Skill in performing risk assessments
6. Effectively motivate, supervise, and direct the work of others
7. Prepare and present effective, clear, and concise reports and correspondence
8. Analyze problems, identify solutions, and make recommendations
9. Prioritize and meet project timelines
10. Establish and maintain effective working relationships
11. Exercise good judgment, decisiveness, and creativity

Required condition of Employment

As a condition of employment, the incumbent will be required to:

Successfully pass a background investigation including but not limited to a fingerprint clearance from the Department of Justice

Possess a valid California License Class “C” driver’s license with a satisfactory driving record or be able to provide suitable transportation that is approved by the appointing authority

Be available to work outside of normal business hours as needed, including evenings, weekends, holidays

and during times of emergency and/or disaster.

Examples of Experience/Education/Training

Any combination of training, education and/or experience which provides the knowledge, skills and abilities and required conditions of employment listed above is qualifying. An example of a way these requirements might be acquired is:

Education:

Possession of a bachelor’s degree in information security, Computer Science, or a closely related field from an accredited, four-year college or university.

AND

Experience:

At least six (6) years of increasingly responsible professional experience performing varied and complex work in the areas of information security administration, network systems, and/or desktop systems, including at least two

(2) years of experience supervising or managing technical staff, and/or serving as a technical expert.

Licenses/Certifications:

Certification in an information security discipline (i.e., GIAC, ISACA or ISC2 certifications) is desirable.

Typical Physical Requirements

Sit for extended periods, frequently stand, and walk; normal manual dexterity and eye-hand coordination; lift and move objects weighing up to 25 pounds; corrected hearing and vision to normal range; verbal communication; use of office equipment, including computer, telephone, copiers, and FAX.

Typical Working Conditions

Work is usually performed in an office environment, with frequent contact with staff and the public.