County of Humboldt Job Specification
CHIEF INFORMATION SECURITY OFFICER
Classification 0290
FLSA: Exempt

DEFINITION

Under general direction, plans, organizes, manages, and provides oversight for Countywide information technology security related operations and activities; operational areas include, but are not limited to, security awareness, risk assessment, business impact analysis, disaster recovery, and business continuity; develops and implements information technology security policies, procedures, goals, and directives; coordinates assigned activities and fosters cooperative working relationships among County departments, officials, outside agencies, the public, and private groups; provides highly responsible and complex professional advice, guidance, and assistance to the County Administrative Officer and other staff in areas of responsibility; and performs related duties as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from the County Administrative Officer, Assistant County Administrative Officer, or designee. Exercises direct supervision over technical staff.

CLASS CHARACTERISTICS

This is a management classification responsible for developing, implementing, and managing a Countywide information technology security program and related activities. The incumbent is responsible for performing specialized, complex information technology security functions involving significant accountability and decision-making responsibilities, which include developing and implementing Countywide information assurance policies and guidelines. The incumbents is responsible for supervising the work of assigned staff; providing professional level support to the County Administrative Officer or designee in areas of assignment; and communicating and collaborating with the Information Technology Division Director and other internal and external County partners. Performance of the work requires the use of considerable independence, initiative, and discretion within broad guidelines.

This class is distinguished from the Information Technology Division Director in that the latter has management responsibilities for the Information Technology Division.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

Management reserves the right to add, modify, change, or rescind the work assignment of different positions.

- Plans, develops, and implements a Countywide information technology security program which includes, but is not limited to, information technology security awareness, systems risk assessment, business impact analysis, disaster recovery, and business continuity.

- Develops and oversees Countywide information assurance policy and guidelines in concert with County agencies and departments for executive management review and approval; upon approval, implements policy and guidelines.
- Advises County staff and departments in the review of information technology security policies, computer operations, server infrastructure, logical access controls, and network and data communication systems security; recommends the use of information technology and network security solutions and tools.
- Acts as the central point of contact for information technology related security incidents or violations; assists County departments (e.g., law enforcement, auditors, etc.) in the investigation of security threats, incidents, or violations.
- Plans, coordinates, and participates in conducting cyber security risk assessments and business impact analyses of County department processes and information technology infrastructure and systems to identify and address threats and vulnerabilities; facilitates the development of effective disaster recovery and business continuity plans.
- Evaluates and ensures the installation, management, operation, and maintenance of information technology infrastructure, systems, and support environments.
- Adheres to information assurance policy and guidelines; troubleshoots and resolves security-related issues.
- Develops, promotes, and presents information assurance security training and education to all levels of the County organization structure on an ongoing basis.
- Leads security research and development; conducts an extensive review of processes, regulatory changes, or business requirements with user focus groups; identifies options to develop new or modify existing applications and databases to respond to these needs.
- Analyzes work processes and flows and creates technical documentation; audits installation projects to ensure compliance; identifies need for integration of technology infrastructure or systems and creates specifications for same; ensures adherence to Countywide information technology policies, procedures, protocols, and standards.
- Collaborates with and coordinates the County information technology security program with state and federal agencies.
- Plans, prioritizes, assigns, supervises, reviews, and participates in the work of staff responsible for information technology security projects and activities.
- Participates in the development and implementation of information technology goals, objectives, policies, and priorities; monitors work activities to ensure compliance with established policies and procedures; makes recommendations for changes and improvements to existing standards and procedures.
- Selects, trains, motivates, and evaluates assigned staff; works with employees to correct deficiencies.
- Participates in the preparation and administration of assigned program and project budgets; submits budget recommendations; coordinate vendor activities, write and evaluate proposals, and negotiate contracts for information technology security related equipment and services; monitors expenditures.
- Writes and maintains County information technology security policies and procedures; maintains systems certification, authorization documentation, and related documents.
- Attends and participates in professional group meetings; stays abreast of new trends and innovations in the field of information technology security.
- Performs related duties as assigned.

Reasonable accommodations may be made to enable qualified individuals with disabilities to perform the essential functions.

QUALIFICATIONS

The requirements listed below are representative of the knowledge and ability required.

Knowledge of:

- Organization and management practices as applied to the development, analysis, and evaluation of information assurance program, policies, procedures, protocols, and standards.
- Advanced information technology security management theory, principles, and practices and their application to a wide variety of services and programs.
- Industry best practices of information technology security management and control.
- Methods and techniques of developing technology security related training programs and educational materials.
- Methods and techniques of identifying and assessing security threats and violations and developing response and mitigation strategies.
- Principles and practices of project management.
- Operational relationships between information technology security program, application development, database management, and components of technology infrastructure such as server and network systems.
- Principles and practices of developing and maintaining technical documentation, files, and records.
- Principles and practices of employee supervision, including work planning, assignment review and evaluation, discipline, and the training of staff in work procedures.
- Principles and practices of leadership.
- Applicable federal, state and local laws, regulatory codes, ordinances and procedures relevant to assigned areas of responsibility.
- Principles and techniques for working with groups and fostering effective team interaction to ensure teamwork is conducted smoothly.
- Techniques for providing a high level of customer service by effectively dealing with the public, vendors, contractors, and County staff.
- The structure and content of the English language, including the meaning and spelling of words, rules of composition, and grammar.
- Modern equipment and communication tools used for business functions and program, project, and task coordination, including computers and software programs relevant to work performed.

Ability to:

- Plan, manage, direct, and oversee a Countywide technology security program.
- Conduct risk assessments of County information technology infrastructure, systems, and devices and make recommendations on needed changes.
- Develop and implement IT security related goals, objectives, policies, and procedures.
- Establish an environment which promotes the criticality of technology system security.

- Serve as a technical advisor to departments on security matters.
- Respond to and investigate, security threats, incidents, and violations.
- Select and supervise staff, provide training and development opportunities, ensure work is performed effectively, and evaluate performance in an objective and positive manner.
- Assist in developing and implementing goals, objectives, practices, policies, procedures, and work standards.
- Evaluate and recommend improvements in operations, procedures, policies, or methods.
- Integrate information technology security needs of diverse departments with Countywide information technology systems, infrastructure, and policies, procedures, and standards.
- Work collaboratively with County staff to identify and implement security solutions for business process improvements and efficiencies.
- Recommend, design, develop, and implement new, enhanced, or modified information technology security systems and tools.
- Prepare clear and concise technical documentation, information technology procedures, staff reports, and other written materials related to IT security.
- Understand, interpret, and apply all pertinent laws, codes, regulations, policies and procedures, and standards relevant to work performed.
- Independently organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- Effectively use computer systems, software applications relevant to work performed, and modern business equipment to perform a variety of work tasks.
- Communicate clearly and concisely, both orally and in writing, using appropriate English grammar and syntax.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:
Any combination of training and experience that would provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the required qualifications would be:

Equivalent to a bachelor's degree from an accredited four-year college or university with major coursework in information technology, computer science, or a related field

and

Five (5) years of increasingly responsible experience in providing professional level support in the administration of an information technology security program, including two (2) years of lead, supervisory, and/or project management responsibility specific to the security operations center.

Licenses and Certifications:

- Must possess a current professional security management certification, such as a Global Information Assurance Certification (GIAC) Security Expert (GSE), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), or equivalent. A master's degree in cyber

security, technology management, or a closely related field may substitute for the certification requirement.
- Must possess a valid US driver's license upon date of application. Must obtain California driver's license following hire date per California DMV regulations.

PHYSICAL DEMANDS

- Mobility to work in a standard office and use standard office equipment, including a computer, and to operate a motor vehicle to visit various County and meeting sites; primarily a sedentary office classification although standing in and walking between work areas is may be required; occasionally bend, stoop, kneel, and reach to perform assigned duties, as well as push and pull drawers open and closed to retrieve and file information; possess the ability to lift, carry, push, and pull materials and objects up to 10 pounds with the use of proper equipment.
- Vision to read printed materials and a computer screen.
- Hearing and speech to communicate in person and over the telephone.
- Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment.

ENVIRONMENTAL CONDITIONS

- Office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances.
- Employees may interact with upset staff and/or public and private representatives in interpreting and enforcing departmental policies and procedures.

ADDITIONAL REQUIREMENTS

- Must be willing to work weekends and evenings as necessary to resolve security breaches.
- Some departments may require pre-employment screening measures before an offer of employment can be made (i.e., background screening, physical examination, etc.).