CHIEF INFORMATION SECURITY OFFICER

DEFINITION

Under general direction, plans, organizes, and provides general direction and oversight for County-wide technology systems security related operations and activities; operational areas include, but are not limited to, security awareness, risk assessment, business impact analysis, disaster recovery and business resumption; coordinates assigned activities and fosters cooperative working relationships among County departments, officials, outside agencies, the public, and private groups; provides expert professional assistance to County management staff in areas of responsibility; and performs related duties as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from the Director of Information Technologies and/or the Assistant Director of Information Technologies. Exercises supervision over professional and technical staff.

CLASS CHARACTERISTICS

This is a management classification with responsibility for developing, implementing, and directing a County-wide technology security program. Incumbents serve as an advisor and resource to County executives and departments on security related policies, procedures, risk assessments, threats, violations and incident investigations and response, and related matters. Incumbents serve as management-level resources for organizational and operational analyses and studies and as highly technical resources to County departments on their technology needs. Performance of the work requires the use of considerable independence, initiative, and discretion within established guidelines.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

- Plans, organizes, manages, and directs the operations and activities of a County-wide technology security program which includes, but is not limited to, security awareness, risk assessment, business impact analysis, disaster recovery, and business resumption.
- Develops and maintains a County-wide information technology security policy in concert with County agencies and departments for executive management review and approval; upon approval, implements direction from executive management.
- Designs or integrates appropriate data backup capabilities into overall system designs, and ensures appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.
- Conducts Privacy Impact Assessments of application security designs for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information.
- Selects, trains, motivates, and directs personnel; evaluates and reviews work for acceptability and conformance with department standards, including program and project priorities and performance evaluations; works with employees on performance issues; implements discipline and termination procedures; responds to staff questions and concerns; works with department management and staff to build and maintain a high performing team environment.
- Acts as the County-wide central point of contact for information technology related security threats, incidents, or violations; serves as a technical advisor to departments within the County under the Department of Technologies purview in the review of security policies, computer operations, logical

access controls, system development, and data communications security; assists other County departments (e.g., law enforcement, auditors, etc.) in the investigation of information technology related security threats, incidents, or violations.

- Designs to minimum security requirements to ensure requirements are met for all systems and/or applications.
- Develops, coordinates, and maintains policies and provides guidance in Local Area Network, Wide Area Network, mainframe, and desktop information security issues; conducts continuous analysis to identify network and system security vulnerabilities.
- Directs activities of all staff assigned to large-scale information technology security development and maintenance projects.
- Integrates and aligns information security and/or information assurance policies to ensure system analysis meets security requirements
- Researches and recommends centralized written manuals and procedures regarding security controls.
- Develops and directs security related risk analysis (e.g., threat, vulnerability, and probability of occurrence) assessment activities; conducts security risk assessments and business impact analyses of County departments to evaluate the effectiveness of the comprehensive County-wide business resumption plan; performs security reviews and identifies security gaps in security architecture; and assists in the coordination and testing of department information technology disaster recovery and business continuity plans; recommends needed changes.
- Develops an enterprise system security context, a preliminary system security concept of operations, and defines baseline system security requirements in accordance with applicable information assurance requirements.
- Develops, promotes, and presents security awareness training and education to all levels of the County organization on an ongoing basis.
- Plans, prioritizes, delegates, and reviews the work of assigned project staff; establishes schedules and methods for achieving project goals and objectives; reviews work products and makes corrections; and coordinates staff training and development efforts.
- Makes verbal and written presentations to the County Board of Supervisors, Chief Administrative Officer, Director of Information Technologies, and executive management in other County departments and outside agencies.
- Establishes and chairs a County-wide Information Security Advisory Committee for discussion and dissemination of information security and related programs.
- May assist in the preparation of departmental budgets, as well as strategic and tactical plans, so that adequate resources are made available to implement information security controls.
- May coordinate vendor activities, write and evaluate proposals, and negotiate contracts for information technology security related equipment and services.
- Performs related duties as assigned.

QUALIFICATIONS

Knowledge of:

- Organization and management practices as applied to the development, analysis, and evaluation of security related programs, policies, procedures, protocols, and standards.
- Principles and practices of employee supervision, including planning and assigning work, performance review and evaluation, discipline, and the training of staff in work procedures.
- Advanced information technology security management theory, principles, and practices and their application to a wide variety of services and programs.
- Information assurance principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation.

- Network protocols (e.g., Transmission Control Protocol and Internet Protocol, Dynamic Host Configuration Protocol, and directory services [e.g., Domain Name System]).
- Penetration testing principles, tools, and techniques.
- Industry best practices of information technology management and control.
- Methods and techniques of developing technology security related educational materials.
- Methods and techniques of developing response strategies for security threats and violations.
- Principles and practices of project management.
- Applicable federal, state, and local laws, regulatory codes, ordinances, and procedures relevant to information technology management programs.
- 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.
- Computers and software programs (e.g., Microsoft software packages) to conduct, compile, and/or generate documentation.

Ability to:

- Plan, manage, direct, and oversee a County-wide technology security program.
- Conduct risk assessments on County business processes and make recommendations on needed changes.
- Develop and implement security related goals, objectives, policies, and procedures.
- Establish an environment which promotes the criticality of technology system security.
- Serve as a technical advisor to County departments on security matters.
- Respond to, and investigate, security threats, incidents, and violations.
- Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.
- Understand, interpret, and apply all pertinent laws, codes, regulations, policies and procedures, and standards relevant to work performed.
- Conduct complex research projects, evaluate alternatives, make sound recommendations, and prepare effective technical staff reports.
- Plan, organize, assign, direct, review, and evaluate the work of assigned staff.
- Analyze, interpret, summarize, and present administrative and technical information and data in an effective manner.
- Prepare clear and concise technical reports, correspondence, and other written material.
- Effectively represent the department and the County in meetings with governmental agencies; community groups; various business, professional, and regulatory organizations; and in meetings with individuals.
- Independently organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- Coordination; and information technology supply chain security/risk management policies, requirements, and procedures.
- Effectively use computer systems, software applications, 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.

- Use tact, initiative, prudence, and independent judgment within general policy, procedural, and legal guidelines.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:
Any combination of the required experience, education, and training that would provide the essential knowledge, skills, and abilities is qualifying.

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

AND

Five (5) years of increasingly responsible experience providing professional-level support to an information technology security program, two (2) years of which must have been in a supervisory capacity in an information technology environment.

Licenses and Certifications:

- Possession of, or ability to obtain and maintain, a valid California or Nevada Driver's License and a satisfactory driving record.
- Possession of nationally recognized security certification is strongly desirable.

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; to operate a motor vehicle and to visit various County and meeting sites; vision to read printed materials and a computer screen; and hearing and speech to communicate in person, before groups, and over the telephone. This is primarily a sedentary office classification although standing and walking between work areas may be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Reasonable accommodations will be made for individuals on a case-by-case basis.

ENVIRONMENTAL CONDITIONS

Employees work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Employees may interact with members of the public or with staff under emotionally stressful conditions while interpreting and enforcing departmental policies and procedures.