CENTRAL INFORMATION TECHNOLOGY ENTERPRISE SECURITY OFFICER
(Administrative Manager III)

DEFINITION

Performs expert-level professional duties in planning and overseeing the County's information technology security and business continuity programs; plans, develops, directs, establishes, maintains and ensures the security of highly complex and strategic County technology operations including mainframe, network, application and database systems; performs comprehensive and complex programmatic design, analysis and development duties in support of infrastructure services and business continuity planning and development; and performs other related duties as assigned.

DISTINGUISHING CHARACTERISTICS

Reporting to Executive Management, incumbents in this classification work under general direction, working from broad policies and towards general objectives and referring specific matters to a superior only when interpretation or clarification of organizational policies is necessary.

EXAMPLES OF DUTIES

- Plans, develops, directs, establishes and maintains the County's information security program, designed to ensure the security of the County's most complex and strategic operations related to mainframe, networked and database systems.
- Plans, develops, directs, establishes and maintains the County's business continuity program, designed to ensure the operation of critical technology functions in the event of an emergency or disaster.
- Develops, coordinates, establishes and maintains policies to provide guidance to County departments and staff regarding Local Area Network (LAN), Wide Area Network (WAN), mainframe, servers, applications, network services, desktop security and business continuity issues; researches and recommends centralized written manuals, guidelines, standards and procedures regarding security and business continuity controls.
- Plans, organizes and coordinates committees, task forces and meetings to identify, resolve and administer security and business continuity-related issues and activities; assists County departments with disaster recovery planning and testing.
- Researches, identifies and analyzes existing and potential security and business continuity threats that could harm or destroy County information assets; interacts and communicates with other government agencies and external organizations to stay aware of security issues; as appropriate, issues Countywide virus and threat warnings as well as information regarding the identification, avoidance and mitigation of such threats.
- Performs Countywide information security audits to identify weaknesses that could be used to gain access to confidential County information; creates, implements, maintains and tests emergency and disaster recovery measures.
- Serves as the central point of contact for the County regarding information technology-related incidents or violations; assists department information technology staff and others (e.g., law enforcement staff) in investigating security violations; performs formal investigations of County employees for misuse of County assets.

- Serves in conjunction with the County Privacy Officer as central points of contact for regulatory compliance, including but not limited to HIPAA. Works in conjunction with agency compliance and security staff to maintain policies, audit logs, and staff development in alignment with current regulations.
- Leads County operations incident response teams; collaboratively develops and enforces Countywide information technology security policies; chairs Countywide security working groups; leads security architecture project reviews, audits and e-discovery efforts.
- Leads the design and development of the County's security infrastructure; represents the County in inter-county and state matters.
- Determines and develops complex cost benefit analyses for project justifications; developing comprehensive and complex project budgets; identifying available resources needed to conduct the work; evaluating risk concerns and options; coordinating the development of specifications for "requests for proposals" pertaining to external services; reviewing vendor submissions and providing recommendations on vendor selection.
- Monitors vendor performance to ensure compliance with County standards and specifications; ensuring project compliance with external laws, County procedures or protocols, budgetary constraints and staff/resource utilization;
- Directs the resources of assigned projects, including subordinate project management staff, to ensure compliance with budget and project specifications;
- Conducts research on information technology security directions, emerging technologies and information technology management approaches.
- Prepares reports, correspondence and other documents; participates on committees and task forces; attends meetings, conferences and training sessions.
- Performs other related duties as assigned.

MINIMUM QUALIFICATIONS

Knowledge of:

- Operations, services and activities of comprehensive information systems security and business continuity programs.
- Advanced principles and practices of system security design, development, analysis and testing.
- Advanced methods and techniques of evaluating information security and business continuity requirements and developing appropriate solutions.
- Functional structures of various operating systems components, including system control programs and data access methods.
- Advanced concepts, principles and practices of WAN design, development, protocols, security and administration.
- Operations, services and activities of a comprehensive database administration program.
- Operational characteristics of database support tools, servers and communication devices.
- Principles and practices of administrative and operations management including budget development and execution.
- Information technology and systems management best practices.
- New developments in information technology and their relevance to current business needs and technology strategies.
- Process analysis, flow and documentation methodologies.
- Advanced project management principles and techniques including project budgeting, quality assessment and control and resource management.
- Computer operating systems, hardware, software and languages used in the County.

- The operations, services, concepts, terms and activities common to a comprehensive, state-of-the-art information systems program.
- Statewide and industry direction for public access to government information
- Principles and practices of customer service.
- Methods and techniques of developing and presenting technical documentation and training materials.

Ability to:

- Plan, develop, establish, monitor and maintain information technology security and business continuity strategies.
- Direct and coordinate technical information security operations and services.
- Serve as a Countywide technical advisor regarding information technology security and business continuity.
- Analyze department procedures and data to develop logical security solutions for complex systems.
- Recommend, evaluate, design, develop, test and install complex security systems including specialized applications and supporting hardware and software.
- Provide advanced-level technical support and troubleshooting for the analysis of security system problems.
- Plan and oversee quality assurance and security procedures for mainframe, database and network systems.
- Assign, direct, and monitor the work of others on a project basis.
- Coordinate and manage highly complex information technology projects.
- Gather and evaluate information in order to reason logically, draw valid conclusions, take appropriate actions and/or make appropriate recommendations.
- Develop information system designs, flow charts, report layouts and screen designs.
- Communicate technical information to a wide variety of users.
- Plan, organize, prioritize and process work to ensure that deadlines are met.
- Interpret and apply highly complex and technical information pertaining to computer and network systems.
- Adapt quickly to changes in policies, procedures, assignments and work locations.
- Communicate effectively, both orally and in writing.
- Establish and maintain effective working relationships with those encountered during the course of the work.

Education/Experience:

One year of experience as an Administrative Manager II with the County of Orange;

OR

Five (5) years of responsible information technology-related experience that provided the knowledge and abilities identified above;

A bachelor's degree from an accredited college or university with major coursework in computer science, information systems or a closely related field may substitute for two (2) of the required years of experience.

College level education or training directly related to the competencies and attributes required of the position may be substituted for up to one year of required experience at the rate of three semester

units or the equivalent, equaling one month of experience and one hour of training equaling one hour of experience.

College level education or training beyond a bachelor's degree, which is directly related to the competencies and attributes required of this position, may be substituted for up to an additional year of required experience at the rate noted above.

Special Requirements: Depending upon assignment, demonstrated professional level experience and/or certification pertaining related to the duties of the position may be required.

PREFERRED EXPERIENCE/EDUCATION

Experience: Two (2) years of information technology experience equivalent to a Central IT Domain Manager or Information Technology Manager II or 12 years experience that included substantial responsibility for planning, administering and ensuring large scale information security operations and disaster recovery for device, LAN/WAN, application, Internet and/or other systems.

Education: A bachelor's degree from an accredited college or university with major coursework in computer science, information systems or a closely related field. Post-graduate education beyond a bachelor's degree which directly enhances the knowledge required for this position is desirable.

Special Requirement: Security certifications pertaining to the information technologies used by the County may be required.

PHYSICAL REQUIREMENTS

All Positions:

Possess vision sufficient to read standard text and a computer monitor; speak and hear well enough to communicate clearly and understandably in person to individuals and groups and over the telephone; possess body mobility to stand, sit, walk, stoop and bend routinely to perform daily tasks and to access a standard office environment; possess manual dexterity sufficient to use hands, arms and shoulders repetitively to operate a keyboard, utilize office equipment and to write; use a County approved means of transportation.

Some Positions:

May be required to possess one or more of the following: the ability to climb, bend, stoop, twist and reach overhead in rugged conditions to review/evaluate work; manual dexterity and bodily movement sufficient to operate various types of equipment in extreme conditions; lift up to fifty pounds.

MENTAL REQUIREMENTS

All Positions:

Possess the ability to independently reason logically to analyze data, reach conclusions and make

recommendations; possess the ability to remain calm and appropriately focused in rapidly changing and difficult situations involving conflict, complex issues, controversy and diverse stakeholder groups and interests; possess the ability to deal calmly and effectively with emotional interactions.

Some Positions:

May be required to possess the ability to handle emotional client situations effectively.

ADDITIONAL REQUIREMENTS

Additional physical/mental requirements or frequencies may be required, depending upon assignment. Depending upon assignment, some positions in this class may require possession of a valid California driver's license, Class C or higher.

ENVIRONMENTAL CONDITIONS

Work is typically performed in an indoor office environment, but occasionally requires travel to other locations. Work environments may include high levels of noise, dust and/or unpleasant odors. Occasional early morning, evening, holiday and/or weekend work may be required.