County of Humboldt Job Specification
INFORMATION SECURITY OFFICER I/II
Classification 0289
FLSA: Exempt

DEFINITION

Under general supervision and direction, performs a diverse range of analytical duties in support of the implementation of the countywide information technology security program including, but are not limited to, security awareness, risk assessment, business impact analysis, disaster recovery, and business continuity; monitors and evaluates the County's information security posture daily; and performs related duties as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives general supervision (Information Security Officer I) or direction (Information Security Officer II) from the Chief Information Security Officer. Exercises no direct supervision over staff.

CLASS CHARACTERISTICS

Information Security Officer I: This is the entry-level classification in the Information Technology Security Officer series. Initially under close supervision, incumbents learn dimensions of the County's information technology security program, guidelines, support service needs. As experience is gained, assignments become more varied, complex, and difficult; close supervision and frequent review of work lessen as an incumbent demonstrates skill to perform the work independently. Positions at this level usually perform most of the duties required of the positions at the II-level but are not expected to function at the same skill level and usually exercise less independent discretion and judgment in matters related to work procedures and methods. Work is usually supervised while in progress and fits an established structure or pattern. Exceptions or changes in procedures are explained in detail as they arise.

Information Security Officer II: This is the journey-level classification in the Information Technology Security Officer series. Positions at this level are distinguished from the I-level by the performance of the full range of duties as assigned, working independently, and exercising judgment and initiative. Positions at this level receive only occasional instruction or assistance as new or unusual situations arise and are fully aware of the operating procedures and policies of the work unit.

This class is distinguished from the Chief Information Security Officer in that the latter oversees the development, implementation, and enforcement of the countywide information technology security program and supervises lower-level staff.

Positions in the Information Security Officer class series are flexibly staffed and positions at the II-level are normally filled by advancement from the I-level, after gaining the knowledge, skill, and experience which meet the qualifications for and after demonstrating the ability to perform the work of the higher-level class.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

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

- Participates in implementing a countywide information technology security program which includes, but is not limited to, security awareness, risk assessment, business impact analysis, disaster recovery, and business continuity.
- Analyzes and evaluates County technology and business processes for security related purposes with specific focus on countywide information technology security policies and guidelines governing and regulating data creation, access, retention, and destruction
- Applies technical standards, methods, and tools for the identification and investigation of information security threats and incidents; audits pertinent logs, analyzes the results from information security scans, and coordinates with Information Technology Security Officer to identify, investigate, respond, and resolve information security incidents; collaborates with compliance and privacy teams to develop and implement corrective action plans.
- Performs regular security assessment of critical information technology network, server, and data storage infrastructure, systems, and devices to mitigate immediate threats and report potential vulnerabilities; identifies strengths and gaps which require action.
- Conducts research to identify alternatives for resolving information security issues and collaborates with senior technical staff from all departments to develop specifications for hardware and software information security systems.
- Performs analysis and evaluation of County web applications to identify vulnerabilities present in application code; collaborates with web application development team to apply code fixes.
- Maintains and updates County employee intranet content dedicated to information security.
- Assists in developing and updating the County IT Incident Response Plan.
- Advises County staff and departments on 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.
- Promotes and presents information technology security training and education to all levels of the County organization structure on an ongoing basis.
- Coordinates with vendors to resolve implementation issues; utilizes application security checklist to assess vendor security posture for all hosted services.
- Assists in coordinating security audits with staff and departments.
- Provides consultation and reviews on project designs; identifies and recommends security design solutions that conform to the countywide Information Assurance policy and guidelines, as well as technology best practices to ensure technology infrastructure, systems, and devices function properly.
- Performs other 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.

Some duties, knowledge, skills, and abilities may be performed in a learning capacity for entry-level (I Level) positions.

Knowledge of:

- 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 identifying and assessing security threats and violations and developing response and mitigation strategies.
- 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.
- Information security forensic tools, rules of evidence, and chain of custody.
- Vulnerability management systems or services.
- 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:

- Conduct risk assessments of County information technology infrastructure, systems, and devices and make recommendations on needed changes.
- Respond to and investigate, security threats, incidents, and violations.
- Troubleshoot, diagnose, analyze, and resolve information security problems and identify and recommend alternative solutions.
- 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 and implement new, enhanced, or modified information technology security systems and tools.
- Prepare clear and concise technical documentation.
- 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 graduation from a four-year college or university with a degree in Computer Science, Management Information Systems, or related field

and

Level I: one (1) year of experience providing professional level support to an information technology security management program which included computing and information security, including security policy development, security education, network penetration testing, application vulnerability assessments, risk analysis and compliance testing.

Level II: three (3) years of experience providing professional level support to an information technology security management program, or two (2) years of experience in the County's classification of Level I.

Licenses and Certifications:

- 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.
- *Level I*: Must attain Global Information Assurance Certification (GIAC) in the Cyber Defense domain that qualify for GIAC Security Expert certification within one year of hire.
- *Level II:* Must possess and maintain two current GIAC certifications in the Cyber Defense domain that qualify for GIAC Security Expert certification.

PHYSICAL DEMANDS

- Mobility to work in a standard office.
- Use standard office equipment, including a computer, and to operate a motor vehicle to visit various County and meeting sites.
- Vision to read printed materials and a computer screen; and hearing and speech to communicate in person and over the telephone.
- This is primarily a sedentary office classification although standing in 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, and reach to perform assigned duties, as well as push and pull drawers open and closed to retrieve and file information.
- Employees must possess the ability to lift, carry, push, and pull materials and objects up to 10 pounds with the use of proper 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

- Some departments may require pre-employment screening measures before an offer of employment can be made (i.e., background screening, physical examination, etc.).