MAY 2021
FLSA: NON-EXEMPT
Bargaining Unit: PL
JCN: 3140

INFORMATION SECURITY ANALYST

DEFINITION

Under general direction, performs a variety of professional level information technology activities related to the coordination and implementation of County-wide cyber security compliance activities and operations, ensuring the confidentiality, integrity and availability of information technology systems; provides expertise in cyber security for the County; assesses information and facilitates remediation of identified vulnerabilities with the County enterprise network, systems and applications; report on findings and recommendations for corrective action; and performs other duties as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from assigned Chief Information Security Officer. Exercises no direct supervision over staff.

CLASS CHARACTERISTICS

This is an advanced journey-level classification characterized by the presence of complex analytical duties, including serving as a resource for County information security matters and leading various security-related activities that impact the County's systems, network and database operations. Incumbents at this level have a thorough knowledge of and demonstrated proficiency developing and deploying security related policies and procedures. Performance of the work requires the use of considerable independence, initiative, and discretion.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

- Participates in County-wide technology security program which includes, but is not limited to, security awareness, risk assessment, business impact analysis, disaster recovery, and business resumption.
- Monitors the integrity and security of County networks and all related components, including human element, physical and virtual servers, domain controllers, desktops, laptops, printers and other devices which utilize the County network.
- Scans and monitors network activity, filters malicious activity and virus probability.
- Conducts continuous analysis to identify network and system security vulnerabilities.
- Assists in development, coordination, and maintenance of policies related to Local Area Network, Wide Area Network, mainframe, and desktop information security issues.
- Makes recommendations of solutions to ensure requirements are met for systems and/or applications.
- 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.
- Conducts security risk assessments (e.g., threat, vulnerability, and probability of occurrence) and business impact analyses of County departments
- Assists in the coordination and testing of department information technology disaster recovery and business continuity plans; recommends needed changes.

- Stays abreast of new trends and innovations within information security, security threats and methods of mitigation.
- Performs security incident response activities, including containment, eradication, and recovery of affected systems.
- Performs compliance audits on County-wide security policies, procedures, and industry best practices.
- Facilitates information technology security/risk training curriculum.
- Researches and prepares technical, administrative and statistical reports.
- Attends and participates in professional group meetings.
- Builds and maintains positive working relationships with co-workers, other County employees and the public using principles of good customer service.
- Performs related duties as assigned.

QUALIFICATIONS

Knowledge of:

- Principles and practices as applied to the development, analysis of security related programs, policies, procedures, protocols, and standards.
- Methods and techniques of evaluating information security requirements and developing security solutions.
- Methods and techniques of investigating security violations.
- Methods and techniques of developing response strategies for security threats and violations.
- Applicable federal, state, and local laws, regulatory codes, ordinances, and procedures relevant to information technology management programs.
- Methods and techniques of developing data security, integrity, backup and recovery processes.
- Industry best practices of information technology management and control.
- 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.
- Standards and methods related to computerized data systems analysis and use.
- Methods and techniques of developing technology security related educational materials.
- 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, develop, establish, monitor and maintain system security strategies.
- Interpret and explain pertinent security related goals, objectives, policies, and procedures.
- Serve as technical advisor regarding information security.
- Respond to, and investigate, security threats, incidents, and violations.
- 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.
- 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.
- Develop and recommend policies and procedures related to system security.
- Prepare a variety of reports and maintain accurate records and files.
- Identify and assess alternative problem solving methods/techniques.
- Analyze complex problems, evaluate alternatives, and make sound judgments and recommendations within established guidelines.
- Organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- 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:

A combination of the required experience, education, and training that would provide the essential knowledge, skills, and abilities is qualifying; however, education may not solely substitute for the required experience.

Equivalent to a 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

Four (4) years of professional experience providing analytical support that included substantial responsibility for planning, administering and ensuring network and other systems security.

Licenses and Certifications:

- Possession of, or ability to obtain and maintain a valid California or Nevada Driver’s License and a satisfactory driving record.

PHYSICAL DEMANDS

Must possess mobility to work in an office setting; use standard office equipment, including a computer; some positions may be required to operate a motor vehicle; vision to read printed materials and a computer screen; and hearing and speech to communicate in person and over the telephone. Standing in and walking between work areas is frequently 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 frequently 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 25 pounds. Reasonable accommodations will be made for individuals on a case-by-case basis.

ENVIRONMENTAL CONDITIONS

Employees work in an office environment with loud to 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.

WORKING CONDITIONS

Must be willing to work after hours, weekends, and holidays as needed. Must be able to pass a thorough background investigation.