CLASSIFICATION SPECIFICATION

CLASSIFICATION: Information Security Officer
ALLOCATION: Administrative Services
FLSA STATUS: Exempt **ESTABLISHED:** June 2011
UNION AFFILIATION: Non-Represented – Management **REVISED:** February 2023

JOB SUMMARY:
Under administrative direction and in collaboration with the Chief Information Officer (CIO), plans, organizes, evaluates, implements, and directs the appropriate operational security posture for County information systems; manages the day-to-day security operations; oversees the development and implementation of County-wide security policies, procedures, and standards to protect the County from internal and external threats and vulnerabilities; serves as subject matter expert to County management on cybersecurity operations and activities; provides security training and awareness; and performs related work as assigned.

CLASS CHARACTERISTICS:
This is a mid-management position that reports directly to the Chief Information Officer. This class is distinguished from the Chief Information Officer in that the latter has overall management responsibility for all Information Technology Division activities and functions. This class is further distinguished from Information Technology Manager in that the ISO is focused on the security of all County information systems.

EXAMPLES OF DUTIES:
Essential:
- Plan, develop, implement and maintain the County's information security program to ensure the security of the County's most complex and strategic operations related to information systems which includes, but is not limited to: security awareness, risk assessment and mitigation, compliance monitoring, and disaster recovery.
- Understand business needs of County departments and outside customer agencies and facilitate security recommendations to meet those needs.
- Collaboratively develop and implement policies and procedures designed to mitigate the County's exposure to cybersecurity threats; conduct research to identify best management practices in cybersecurity program management; assist in recommending and selecting security solutions and enhancements; modify and update policies according to regulatory requirements and best practices; oversee the enforcement of County-wide information security policies.
- Direct and participate in the identification of security risks, development and implementation of security management practices, and the measurement and monitoring of security protection measures.
- Conduct information security threat/risk assessments and analysis; monitor and review intrusion detection systems and firewall logs; evaluate and identify risks and threats to system security; present security issues and countermeasure recommendations to the CIO and other department heads; and advise management of risks and best security practices.
- Direct the development and promotion of cybersecurity awareness training for all levels of the County organization structure; as appropriate, issue County-wide virus and threat warnings as well as information regarding the identification, avoidance, and mitigation of such threats.
- Participate in the development and implementation of disaster recovery and business continuity plans to ensure that appropriate information systems security measures are addressed.
- Act as the central point of contact for information technology related security incidents and violations; lead security architecture project reviews, audits and discovery efforts; lead county operations incident response teams; as appropriate, assist County departments in the investigation of security threats, incidents, or violations.
- Participate in the preparation and administration of assigned program and project budgets; submit budget recommendation; coordinate vendor activities, write and evaluate proposals, and negotiate contracts for information technology security related equipment and services; monitor expenditures.
- Perform County-wide information cybersecurity audits; create, implement, maintain, and test emergency and disaster recovery measures; monitor system recover processes to ensure security features and procedures are properly restored and functioning correctly working with the entire IT team.
- Lead the design and development of the County's cybersecurity infrastructure and applications; coordinate any changes or modifications to hardware, software, or firmware of a system with other IT Managers and CIO prior to the change; participate in systems design to ensure implementation of appropriate security policies; monitor software is implemented fully utilizing best practices.
- Chair County-wide security committees or work groups; plan, organize, and coordinate committees, task forces and meetings to identify, resolve and administer cybersecurity.
- Interact and communicate with other government agencies and external organizations to stay aware of security issues;

represent the County in inter-county and state matters; work in conjunction with agency compliance and security staff to maintain policies and audits in accordance with current regulations.
- Conduct periodic reviews of information systems to ensure compliance with cybersecurity policies and procedures; conduct continuous monitoring activities for authorization boundaries.
- Ensure all security related documentation is current and accessible to properly authorized individuals; ensure audit records are collected, reviewed, and documented (and include any anomalies).
- Attend required technical and security training (e.g. operating systems, networking, security management) relative to assigned duties.
- Analyze, recommend and report on solutions to departmental and enterprise security issues, concerns, questions, incidents and events; evaluate vendor process and services.
- Conduct research on information technology cybersecurity directions, emerging technologies and information technology management approaches.
- Prepare reports, correspondence and other documents on the status of security safeguards; participate on committees and task forces; attend meetings, conferences and training sessions.
- Create and document procedures and processes to support security policy; maintain cybersecurity policy and procedures, updating as necessary due to changes in standards, regulations and laws.

Important:
- Comply with all County equipment and safety policies and procedures, and California Occupational Safety and Health Administration (CalOSHA) rules and regulations.
- Use standard office equipment, including a computer, in the course of the work; drive a personal or county motor vehicle in the course of the work.

EMPLOYMENT STANDARDS:

Knowledge of:
- Advanced information technology cybersecurity management theory, principles, and practices and their application to a wide variety of services and programs.
- Advanced principles and practices of system security design, development, analysis and testing.
- 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.
- Advanced project management principles and techniques including project budgeting and execution, quality assessment and control and resource management.
- Advanced concepts, principles and practices of WAN design, development, protocols, security and administration.
- Operational relationships between information technology security program, application development, database management, and components of technology infrastructure.
- Principles of disaster recovery and business continuity planning.
- Methods and techniques of developing technology cybersecurity related training programs and educational materials.
- Principles and practices of developing and maintaining technical documentation, files, and records.
- Applicable federal, state, and local laws, codes, and ordinances relevant to information technology cybersecurity management.
- New developments in information technology and their relevance to current business needs and technology cybersecurity strategies.
- Modern equipment and communications tools used for business operations including computers and software programs relevant to work performed.
- County and departmental operations, terminology, rules, policy and procedure.
- Techniques for dealing successfully with a variety of individuals from various socio-economic, ethnic and cultural backgrounds.
- The structure and content of the English language including the meaning and spelling of words, rules of composition and grammar.
- Principles and processes for providing customer and personal services. This includes customer needs assessment, meeting quality standards for services, and evaluation of customer satisfaction.

Skill in:
- Planning, managing, and overseeing a County-wide cybersecurity vision, strategy, and program to ensure information assets and resources are appropriately protected.
- Conducting risk assessments of County information technology infrastructure, systems, and devices and make recommendations on needed changes.

- Developing and implementing cybersecurity related goals, objectives, policies, procedures, and work standards.
- Coordinating, overseeing and performing complex information systems cybersecurity work.
- Responding to and investigating security threats, incidents, and violations.
- Planning, organizing, supervising, reviewing and evaluating the work of others.
- Conducting tests and inspections of products, services, or processes to evaluate quality or performance.
- Providing advanced-level technical support and troubleshooting for the analysis of cybersecurity system problems.
- Understanding legal requirements for data security and implement policy and procedure to limit County risk.
- Evaluating and recommending improvements in operations, procedures, policies, or methods.
- Integrating information technology security needs of diverse departments with County-wide information technology systems and infrastructure.
- Working collaboratively with County staff to identify and implement security solutions for business process improvements and efficiencies.
- Understanding, interpreting, and applying all pertinent laws, codes, regulations, policies, procedures, and standard relevant to work performed.
- Considering the relative costs and benefits of potential actions to choose the most appropriate one.
- Effectively using tact, patience, courtesy, discretion and prudence in dealing with those contacted in the course of the work.

Ability to:

- Plan, develop, establish, monitor and maintain information systems cybersecurity and business continuity strategies.
- Analyze department procedures and data to develop logical security solutions for complex systems.
- Recommend, evaluate, design, develop, test and install complex cybersecurity systems, including specialized applications and supporting hardware and software.
- Plan and oversee quality assurance and security procedures for database and network systems.
- Coordinate and manage highly complex information systems projects.
- Serve as a County-wide technical adviser regarding information technology security and business continuity.
- Listen carefully to what other people are saying, take time to understand the points being made, and ask questions as appropriate for clarification.
- Exercise initiative, ingenuity, sound, and independent judgment within general policy guidelines.
- Collaborate on topics that are sensitive in nature, involving many stakeholders with competing interests.
- Communicate information effectively in writing and verbally as appropriate for the needs of the audience.
- Make rational judgments and decisions in a timely manner particularly in situation involving potential risks.
- Work within a team framework, both as a leader and a member.
- Interact with others and demonstrate sensitivity to their needs in order to establish and maintain a supportive and professional working relationship.
- Adapt quickly and maintain composure in difficult and high stress situations.
- Organize own work, manage multiple projects/programs and meet critical deadlines.
- Pay attention to detail and be thorough in completing work tasks; concentrate on a task over a period of time without being distracted.
- Prepare clear, concise and organized written reports, correspondence and other materials by compiling various sources of information into a professional document.

Physical Demands: The physical demands and work environment described here are representative of those that must be met by an employee to successfully perform the essential function of the job, with or without accommodation. Prospective employees must complete a pre-employment medical exam (Occupational Group IV) which will measure the ability to:

- See well enough to read fine print and view a computer screen; speak and hear well enough to understand, respond, and communicate clearly in person and on the telephone; independent body mobility sufficient to stand, sit, walk, stoop, and bend to access the work environment and a standard office environment; manual dexterity and sufficient use of hands, arms, and shoulders to repetitively operate a keyboard and to write; and the ability to sit or walk for prolonged periods of time.
- Properly handle equipment and supplies weighing up the 25 pounds on an occasional basis.
- Mobility to drive motor vehicle to visit work sites throughout community and attend meetings.

Accommodation may be made for some of these physical demands for otherwise qualified individuals who require and request such accommodation.

Work Environment:
- Typical office environment, with multiple work locations.
- Generally, noise levels are typically quite. May at times be exposed to loud noise levels. However, noise levels are typically quiet.

QUALIFICATIONS:
The minimum and preferred requirements are listed below. While the following requirements outline the minimum qualifications, Human Resources reserves the right to select applicants for further consideration who demonstrate the best qualifications match for the job. Meeting the minimum qualifications does not guarantee further participation in selection procedures.

Licenses and Certification:
- The ability to obtain a valid California Class C driver's license within ten (10) days of employment; maintain throughout employment.
- Maintain professional development and continue education activities as required.

Special Requirements:
- May be required to work evenings, weekends and/or holidays and in response to system security emergencies and priorities.
- Must successfully complete an extensive and thorough background investigation which includes Live Scan fingerprinting prior to hire.
- DMV printout prior to hire.
- Must file statements of economic interest with the Yuba County Clerk/Recorder.
- Will be required to perform disaster service activities pursuant to Government Code 3100-3109.

Education and Experience:

MINIMUM: Bachelor's degree from an accredited college or university in Computer Science, Information Systems or related field and six years of experience configuring, installing, upgrading, maintaining, diagnosing, analyzing and resolving problems related to software and hardware systems which has included at least four years of experience in information and communications security and/or information security operations.

PREFERRED: In addition to the minimum, a Master's Degree in a related field, Certification as a Certified Information Systems Security Professional (CISSP) or Certified in Risk and Information Systems Control (CRISC) or equivalent and additional years of experience as a Network Administrator or Information Security Officer in a public agency setting.

This class specification lists the major duties and requirements of the job. Incumbent may be expected to perform job-related duties other than those contained in this document.

Administrative Services Approval:
Date:

Signature: _____

Human Resources Approval:
Date:

Signature: _____

EEOC: A
WC: 9410

Established: June 2011
Revised: Feb 2023