STATE OF CALIFORNIA
DEPARTMENT OF COMMUNITY SERVICES AND DEVELOPMENT
DUTY STATEMENT

EMPLOYEE NAME	CLASSIFICATION	POSITION NUMBER
Vacant	Information Technology Specialist II	016-190-1414-XXX
DIVISION	**UNIT**	**EFFECTIVE DATE**
Administration	Information Technology Services – Information Security Officer	

SUMMARY OF RESPONSIBILITIES

Under the general direction of the Chief Information Officer (CIO), the Information Technology Specialist II (ITS II) is designated as the Community Services and Development (CSD) Information Security Officer (ISO). The ISO under the general direction of the CIO, plans, organizes, directs, and evaluates the activities of CSD'S Information Security Program. The ISO provides input and participates in the planning, developing, and managing efforts of Information Security incident responsibilities; develops and implements policies and operational standards that address information security breaches; provides advice and technical assistance to management on information security-related issues; co-leads projects to determine the potential risk of exposure of all information assets; serves as a consultant on the implementation of laws, policies and standards regarding current information security; serves as the liaison to all control agencies in communicating the Department's information security policies, incident responses and action plans; and ensures all Government Code and State Administrative Manual requirements are met.

The ISO investigates, resolves, and reports through appropriate channels all information security incidents; monitors vulnerabilities, threats, and incidents; performs departmental risk assessments; facilitates the online information security awareness training for all employees monthly.

Description of Essential Functions:

30% Directs the Information Security & Privacy Program. Advises the CIO and ITS Leadership Team on all matters related to the security of CSD information assets. Serves as team lead to ensure the effective and efficient delivery of Information Security Office program and that the ISO program and services that are consistently delivered are in alignment with the CIO's goals and priorities for information technology. Develops information security & privacy plans, policies, procedures, and standards to ensure the confidentiality, integrity, availability, and appropriate use of CSD information assets. Conducts security risk assessments to identify threats and vulnerabilities to CSD information assets. Advises Executive Officers and CSD management, through formal recommendations, on measures

that can be taken to eliminate or mitigate identified risks. Oversees the email quarantine process and authorizes the release of any quarantined emails that contain confidential information. Investigates and resolves the authenticity of reported security incidents and violations. Coordinates all external reporting and files Information Security Incident Reports with the State's Office of Information Security and Privacy Protection and the California Highway Patrol Emergency Notification and Tactical Alert Center. Protects CSD's sensitive resources against misuse, abuse, and unauthorized use by developing and enforcing strict controls that regulate an individual's access to and use of information assets. Serves on California Health and Human Services (CalHHS) Security related committees for critical interdepartmental IT projects to ensure the integration of appropriate information security protocols and controls. Coordinates efforts to provide for the integrity and security of CSD's information assets and provides for the security of IT facilities, software, and equipment. Reviews internal and external contract documents to ensure appropriate security protocols are being addressed. Oversees the CSD information security awareness program.

30% Responsible for the Information Privacy Program. Develops privacy policies and procedures to limit the collection of and safeguarding of the privacy of personal information collected or maintained by CSD and any of its local service providers (LSP) and constituent entities. Conducts periodic privacy assessments and ongoing compliance monitoring activities to ensure that personal information is handled in full compliance with all provisions of the Information Practices Act of 1977 (Civil Code 1798 et seq.). Reviews and approves all privacy considerations for the automated and manual environment containing confidential or sensitive data. Responds to inquiries from LSP's and other stakeholders related to the CSD Privacy Policy.

20% Coordinates the CSD Operational Recovery Plan. Leads and directs IT governance in support of business and technology strategy. Establishes policies and procedures and coordinates efforts that maintain cost-effective risk management processes intended to preserve CSD's ability to meet state program objectives in the event of the unavailability, loss, or misuse of information assets. Participates as a key member of CSD's enterprise governance and provides critical support and information to business leaders in support of governance decisions. Ensures the recoverability of CSD's systems and assets by overseeing the development, implementation, testing, and maintenance of CSD's Technology Recovery Plan (TRP), Business Continuity Plan (BCP), and ancillary system and services Operational Recovery Plans (ORP)to assure continuity of computing operations for the support of critical applications during a period of man-made or natural disaster. Establishes and maintains processes for the analysis of risk associated with CSD's information assets.

15% Supports all programs within CSD and the overall delivery of ITS strategy, goals, and objectives. Develops direction, policy, and culture that promotes the success of ITS as a key program area within CSD. Represents CSD ITS with customers and stakeholders on a variety of issues and activities. Coordinates various committees and boards and technology procurements to ensure CSD systems are aligned to the ITS strategic directions, maintain, and enhance appropriate and necessary security, developed, and built as part of an enterprise-focused design, and follow appropriate change management policies.

Marginal Functions

5% Represents CSD as a Member of National and State Security Organizations. Serves as a member of the State and CalHHS Agency Information Security Officer's Committee to ensure the protection of vital assets and the sustainability of operations. Meets and confers with high-level information security personnel from other state departments, governmental officials, and private sector businesses regarding matters affecting security policy and procedures. Attend professional conferences and training classes, as appropriate, to maintain and enhance the current level of service to CSD IT customers. Review high level technical documentation and discover emerging technologies and methodologies to educate CSD and ITS team members. Perform training to CSD Staff on system administration, account management, system backup and user training. Mentor and train subordinate staff. Other duties as assigned.

Domains:

This position is in the Information Security Engineering domain.

Supervision Received:

The incumbent works under the direction of the Chief Information Officer.

Supervision Exercised:

None.

Administrative Responsibility:

None.

Personal Contacts:

The incumbent has contact with all levels of the CSD staff, consultants, vendors, CalHHS staff, California Technology Agency staff, Control Agency staff, and other government agencies. This includes CSD's Programs, Local Service Providers (LSP), Front-End Vendors who support the LSP's, and executive management. Contacts may be initiated with other departments, governmental agencies, and private companies concerning

information system and data center technologies as they related to the performance of this position.

Actions and Consequences:

The incumbent will make decisions that impact the functionality of the CSD technology applications and solutions. Failure to properly administer duties using good judgment, logic, and discretion, may result in poor performance or unusable systems and/or applications, and prevent the CSD end users from effectively performing their duties. In addition, substantial workload backlogs may occur, online consumer services may be unavailable, and the CSD may be unable to carry out mandates designed to protect consumers, licensees, and applicants.

Performance Expectations*:*

The incumbent must be able to reason logically and creatively and utilize a wide variety of skills to resolve enterprise-wide technical issues, application development and multiple system interface issues. Additionally, this position must have ability to communicate and resolve business related issues/problems that require a technology solution. Incumbent must be able to develop and evaluate alternatives and research and present ideas and information effectively both orally and in writing. Incumbent must be able to consult with and advise interested parties on IT subjects, gain, and maintain the confidence and cooperation of those contacted, and accurately assign priorities to multiple projects at any given time and to remain flexible. The incumbent shall operate to protect the cyber security of individual departmental staff, the Department's network and infrastructure, and all data assets.

- Ability to work cooperatively with others.
- Ability to work efficiently and work under changing deadlines.
- Ability to maintain consistent, regular attendance and report to work on time.
- Ability to lead and collaborate with ITS stakeholders in a professional manner.
- Ability to get along with others.
- Ability to always exhibit courteous behavior towards others.
- Ability to meet deadlines and perform tasks with minimal amount of errors.
- Ability to do completed staff work.

Characteristics:

- **Leadership** – Possesses a natural ability and keen desire to manage projects and mentor and guide staff, as well as internal and external customers.
- **Innovation** – Demonstrates and encourages creativity and proactive problem-solving.
- **Credibility and Integrity** – Understands internal and external customers and has a true desire to build credibility. Demonstrates the highest professional and legal ethics.
- **Teamwork** – Cooperates to achieve the department's mission, vision, and goals by leading and actively contributing to intradepartmental project teams.
- **Vision** – Understands the context and mission of the Department both internal and external.
- **Accountability** – Makes decisions and remains accountable for those decisions.

- **Reliability** – Understands the importance of meeting timelines and work priorities.
- **Mentor and Coach** – Ability to instruct, direct, and prompt subordinates to help them perform to their full potential.

Job Requirements:

Ability to perform the essential functions of the job, with or without reasonable accommodations including communicate effectively, comprehend, evaluate, and follow written instructions, type, and use personal computers.

Conflict of Interest: This position is subject to Title 16, section 3830 of the California Code of Regulations. The incumbent is required to submit a Statement of Economic Interests (Form 700) within 30 days of assuming office, annually by April 1st, and within 30 days of leaving office.

I have read and understand the duties outlined in this document.

Can you perform the essential functions of the position, with or without reasonable accommodation?

_____ YES _____ NO

If reasonable accommodation is necessary, please complete a Reasonable Accommodation Request Form from the Human Resource Office, Reasonable Accommodation Coordinator.

_____ _____

EMPLOYEE SIGNATURE DATE

_____ _____

SUPERVISOR SIGNATURE DATE

JOB TITLE