

State of California - Department of Social Services

DUTY STATEMENT

EMPLOYEE NAME:

VACANT

CLASSIFICATION:

INFORMATION TECHNOLOGY SPECIALIST I

POSITION NUMBER:

721-1402-008 (Information Security Training Specialist)

DIVISION/BRANCH/REGION: *(UNDERLINE ALL THAT APPLY)*

INFORMATION SYSTEM DIVISION

BUREAU/SECTION/UNIT: *(UNDERLINE ALL THAT APPLY)*

INFORMATION SECURITY AND PRIVACY OFFICE

SUPERVISOR'S NAME:

Celia Khamphanh

SUPERVISOR'S CLASS:

INFORMATION TECHNOLOGY SUPERVISOR II

SPECIAL REQUIREMENTS OF POSITION *(CHECK ALL THAT APPLY)*:

Designated under Conflict of Interest Code.

Duties require participation in the DMV Pull Notice Program.

Requires repetitive movement of heavy objects.

Performs other duties requiring high physical demand. *(Explain below)*

None

Other *(Explain below)*

Fingerprinting clearance required.

I certify that this duty statement represents an accurate description of the essential functions of this position.

I have read this duty statement and agree that it represents the duties I am assigned.

SUPERVISOR'S SIGNATURE

DATE

EMPLOYEE'S SIGNATURE

DATE

SUPERVISION EXERCISED *(Check one)*:

None

Supervisor

Lead Person

Team Leader

FOR SUPERVISORY POSITIONS ONLY: Indicate the number of positions by classification that this position DIRECTLY supervises.

Total number of positions for which this position is responsible:

FOR LEADPERSONS OR TEAM LEADERS ONLY: Indicate the number of positions by classification that this position LEADS.

MISSION OF ORGANIZATIONAL UNIT:

Information System Division's (ISD) mission is to develop, support and promote the business value of IT which comes from the ability to conduct business processes more reliably, faster and at lower cost. ISD creates value by continually improving customer service and providing access to information that enables better decision making by CDSS business units.

ISD accomplishes this by:

- effectively managing information systems and equipment;
- planning, communicating and implementing responsible information technology policies and solutions; and,
- sharing and transferring information technology knowledge and tools.

CONCEPT OF POSITION:

The Information Technology Specialist I (ITS1) reports directly to the Information Technology Supervisor II (IT Sup II), Risk & Governance Unit. The ITS1 is responsible for leading the department's Information Security Awareness Training (ISAT) program, ensuring training content is current, role-based, and integrated into both onboarding and annual training cycles. The incumbent monitors program effectiveness through phishing simulations and reports key performance metrics to management. This role is committed to fostering a security-conscious culture within CDSS through the development, implementation, and evaluation of comprehensive information security training initiatives. The ITS1 also supports project risk management efforts, contributes to IT security initiatives, and assists in resolving complex security issues. Position requires knowledge of information security training and awareness, third-party risk management, systems security, identity and access management, and IT security governance.

A. RESPONSIBILITIES OF POSITION:

30% - Act as the lead over the enterprise information security training and awareness program. Coordinates the development and implementation of the department's Information Security Awareness Training (ISAT) to educate CDSS employees, contractors and vendors regarding their data handling responsibilities and about CDSS information security and privacy policies while consistently maintaining the relevancy and currency of the training content. Develops role-based information security training, and ensures the integration of role-based training into on-boarding and annual information security training for newly hired employees or contractors. Continually monitors ISAT proficiencies through simulated phishing exercises. Monitors the effectiveness of the training and awareness program and reports key metrics to the ISPO leadership team.

20% - Represent the Information Security & Privacy Office on various initiatives and efforts—particularly with respect to third-party risk management. Support IT security initiatives, troubleshoot, problem solve and work with all levels of IT technical support staff. Support the development, review, and revision of IT security-related documentation, informational materials, publications, trainings, policy memos, contracts, etc. Support IT technical security specialists assisting users in resolving the most complex and difficult IT security issues that may be encountered. Provide analysis of the overall needs for Department IT solutions statewide. Research, compile, analyze, and evaluate the more complex data to continuously improve IT systems operations related to IT security practices. Utilize excellent organization and written and verbal communication skills while working with Executive Managers, internal team members, and customers.

20% - Provide tier 1 support for third-party monitoring and security event notification oversight. Oversee the intake, triage, and escalation of security event notifications from external partners, ensuring timely analysis and response in alignment with departmental incident response procedures. Maintain documentation of third-party security incidents and provides regular reporting to ISPO leadership to support risk management and compliance initiatives. Escalate elevated risks to tier 2 support analysts when needed.

10% - Manage the lifecycle of system accounts across the enterprise. Ensure account modification and deactivation align with organizational policies and federal security standards. Ensure prompt deactivation or modification of accounts when users separate from the organization or transfer to different roles or groups. Coordinate with Human Resources and system owners to receive timely notifications of personnel changes, and ensure that access is revoked or adjusted accordingly to prevent unauthorized access. Collaborate with system owners, business owners, and privacy officials to approve privileged access and maintain compliance with privacy and security requirements.

15% - Actively participate in team meetings, technology initiatives, or other assignments. Maintain up to date knowledge about state policies, processes, and industry best practices related to IT administration and information security. Invest in personal development through continuous education to maintain position-related knowledge.

5% - Support organizational change management and product publicity narratives. Encourage process innovation and support approaches emphasizing class-leading security and modular architectural and modern development and deployment approaches. Escalate at-risk tasks to Project and Program Leadership. Assist in developing and implementing a product governance plan.

B. SUPERVISION RECEIVED:

ITS1 is under the direction of the IT Supervisor II.

C. ADMINISTRATIVE RESPONSIBILITY:

None

D. PERSONAL CONTACTS:

ITS1 may have contact with CDSS executives, program management, rank and file staff, other State departments and various vendors and consultants. The ITS1 is required to maintain a professional working relationship with all customers.

E. ACTIONS AND CONSEQUENCES:

The ITS1 must ensure that CDSS is in compliance with applicable information security policies. Failure to enforce these policies can result in CDSS paying penalties and other costs.

F. OTHER INFORMATION:

Requires operating a computer terminal approximately 80% of the time, in addition to remote work. Subject to fingerprinting and criminal record clearance by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI). Travel may be required. Will attend meetings in person and remotely.

- CISSP, ISACA CISM, CompTIA Security + and (ISC)2 SSCP are desirable certifications.
- Knowledge of HIPAA, SAM 5300, NIST 800-53, NIST CSF, IRS Pub 1075
- A demonstrated interest in assuming increasing responsibility.
- Mature judgment, poise, tact, and discretions.
- Ability to take and follow directions from supervisors.
- Ability to effectively demonstrate exceptional writing and communication skills.