DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 046 (REV. 03/2024)

Type of Duty Statement:	Current & Proposed	**Revision Date:**	10/27/2026

1. Position Information

A. Employee Name:

B. Position Number:	**C. CBID:**	**D. WWG:**	**E. Effective Date:**
817-411-1402-002	R01	E	
F. Classification Title:		**G. Working Title:**	
Information Technology Specialist I		Information Technology Specialist I	
H. Division:	**I. Branch/Section/Unit:**		
Technology Services	Information Security Office, Risk and Privacy Office		

2. POSITION REQUIREMENTS

Special Requirement: *Check All that Apply*

- ☐ Bilingual Fluency (Non-English Language) - Specify Below
- ☑ Background Check Requirements
- ☐ Other - Specify Below

A. Special Requirements Description, as applicable:

N/A

B. Conflict of Interest Required (Gov. Code 87300, et seq.)? ☐ **Yes** ☑ **No**

This position is designated under the Conflict-of-Interest Code. This position is responsible for making or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete Form 700 within 30 days of appointment. Failure to comply with the Conflict-of-Interest Code requirements may void the appointment.

3. SUPERVISION

A. Supervision Received:

The incumbent reports directly to the Information Technology Manager I in the Risk & Privacy Office.

4. DUTIES AND RESPONSIBILITIES OF THE POSITION

CONDUCT, ATTENDANCE AND PERFORMANCE EXPECTATIONS

This position requires the incumbent conduct oneself in accordance with the Department of Child Support Services leadership practices and principles, maintain consistent and regular attendance; communicate effectively and professionally (both orally and in writing) in dealing with the public and/or other employees; develop and maintain knowledge and skills related to specific tasks, methodologies, materials, tools, and equipment; complete assignments in a timely and efficient manner; and adhere to all departmental policies and procedures.

GENERAL STATEMENT

Under the general direction of the Risk & Privacy Officer, Information Technology Manager I (ITM I) the Information Technology Specialist I (ITS I) serves as a specialist responsible for third-party and Supply Chain Risk Management (SCRM) programs, records and disclosure coordination, information governance, and business continuity facilitation. Collaborates with Enterprise Risk Management, Privacy, Insider Threat, Information Security, Legal, Human Resources, Procurement, and business and technical owners. Legal counsel, records custodians, authorized disclosure officials, and operational recovery owners retain their respective decision-making and execution responsibilities in the Risk & Privacy Office (RPO), Information Security Office (ISO), within the Technology Services Division (TSD).

A. Percentage of Time Performing Duties	**B. An itemized listing of the specific job duties and the percentage of time spent on each separate and distinct task, with essential and marginal functions identified. Percentages must be listed in descending order and must equal 100%. (No duties less than 5%.).**
ESSENTIAL FUNCTIONS	
IT Domain: *Check All That Apply*	**FOR INFORMATION TECHNOLOGY (IT) CLASSIFICATIONS ONLY** ☑ Business Technology Mgmt. ☐ Software Engineering ☑ IT Project Mgmt. ☐ System Engineering ☑ Information Security ☐ Client Services
30 %	Third-Party and Supply Chain Risk Management (SCRM): • Support the departmental SCRM framework, plan, procedures, assessment criteria, and standardized documentation, aligned with applicable departmental and government requirements. • Coordinate risk-based assessments of prospective and existing vendors, cloud services, technology products, hardware, software, external connections, and other third-party dependencies. • Gather and evaluate relevant evidence regarding third-party security, privacy, service continuity, data handling, and supply chain controls; obtain technical input from appropriate subject-matter experts. • Evaluates third-party and operational risks; coordinates authorized reviews involving personally identifiable information (PII), federal tax information (FTI), records requests, and information preservation; maintains program records and corrective action tracking; and supports management reporting. • Maintain the third-party risk register and related inventory, including assessment status, risk ratings, responsible owners, required actions, and reassessment schedules. • Provide documented findings and recommendations to business owners and appropriate decision-makers; coordinate risk acceptance or treatment through established departmental governance. • Coordinate risk-related input to vendor on boarding, renewal, change, and off

30 %	Records, Disclosure and Information Governance: • Provide SCRM, records/disclosure coordination, and continuity risk information to the ERM program for consolidated enterprise reporting and escalation; avoid maintaining a competing enterprise risk methodology. • Support California Public Records Act (PRA) requests by coordinating identification and collection of responsive records, documenting workflows, and referring exemption, redaction, and release decisions to authorized records and legal personnel. • Coordinate eDiscovery and litigation hold activities at the direction of Legal, including identifying relevant data custodians, facilitating preservation requests, documenting status, and supporting authorized retrieval of electronically stored information. • Coordinate intake, documentation, and referral of suspected data handling or disclosure policy violations, including requests from Human Resources and Legal; preserve confidentiality and avoid duplicating Insider Threat investigations or incident response. • Develop and maintain information governance procedures for request intake, classification and handling guidance, approvals, escalation, evidence tracking, and retention coordination, consistent with approved policies and records schedules. • Maintain logs and management metrics for disclosure and records coordination activities; identify recurring issues and recommend process or control improvements in collaboration with Privacy and other responsible owners.
25 %	Business Continuity Planning and Operational Resilience: • Facilitate the development, periodic review, maintenance, and submission of departmental Business Continuity Plans (BCPs) and Business Impact Analyses (BIAs) with designated business and technical owners. • Coordinate identification of critical business processes, dependencies, recovery priorities, and continuity-related risks; document assumptions, gaps, and ownership. • Plan and facilitate continuity tabletop exercises and other approved recovery exercises in coordination with responsible teams; capture observations and improvement actions. • Maintain continuity-related tracking and reporting, including plan currency, exercise participation, corrective actions, and escalation of unresolved risks. • Coordinate with disaster recovery and technical recovery owners while leaving execution of system restoration and operational recovery to designated teams.

10 %	Program Coordination, Reporting, and Continuous Improvement • The incumbent coordinates with staff on enterprise risk escalation; with Privacy staff on privacy assessments and sensitive-data requirements; with Insider Threat and ISO on suspected misuse or security incidents; and with Legal, HR, records custodians, Procurement, and program owners on authorized requests and third-party matters. The incumbent does not independently approve disclosures, make legal determinations, conduct personnel investigations, own procurement or contract approvals, operate security monitoring or DLP controls, or execute system recovery. • Support enterprise risk escalation, management reporting, and information sharing to ensure identified risks, findings, and remediation activities are appropriately documented, communicated, and tracked. • Apply knowledge of third-party risk management, information governance, sensitive-data handling, security and privacy controls, and supply chain dependencies to support assigned program responsibilities. • Facilitate BCP/BIA workshops and exercises, coordinate authorized records requests and preservation activities, and support timely resolution of corrective actions in collaboration with responsible stakeholders. • Identify opportunities to improve and standardize program workflows, documentation, intake, assessments, monitoring, reporting, and follow-up activities to enhance operational efficiency and effectiveness. • Support knowledge transfer, maintain program documentation, and promote sustainable processes and long-term state ownership of RPO functions.
0 %	N/A

MARGINAL FUNCTIONS	
5 %	Provides overall support to the Branch IT Manager II, Chief Information Officer, Chief Information Security Officer, and staff as the expert in various topics. Represents TSD on special teams, projects, and other duties as assigned. Performs special assignments, attend meetings, and serve as back-up for the Section Manager and peers as needed.
100 %	**TOTAL**

5. WORKING ENVIRONMENT AND PHYSICAL REQUIREMENTS

☐ **Office Centered**

Incumbent's workspace will be a two-story, office building environment with standard modular cubicle or office spaces, temperature control and artificial lighting. Requires sitting for long periods of time while using a personal computer for email communication, reviewing documents, and attending meetings. Incumbent must be able to sit for extended periods of time attending meetings or sit and/or stand while working. Incumbent may perform repetitive hand motions such as typing, push, pull, reach, or bend (neck and waist). The work environment is fast-paced and can be demanding. May require periodic work during non-standard hours and during weekends to meet workload needs. Travel may be required for meetings or to attend professional training and/or events.

☑ **Remote Centered**

Incumbent's workspace will be divided between an office-centered, two-story, professional office building environment and a remote-centered work location in accordance with an approved telework agreement. Dedicated remote-centered workspaces must comply with all departmental and state safety and security policies. Requires sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings remotely. The office-centered workspace consists of an office building environment with standard modular cubicle or hoteling office space, and artificial lighting. Requires sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings remotely or in designated areas. The work environment is fast-paced and can be demanding. May require periodic work during nonstandard hours and during weekends to meet workload needs. Travel may be required to attend professional training and/or events. Remote centered teleworkers must forgo telework when their physical presence is required in the office on a regularly scheduled telework day.

6. OTHER RESPONSIBILITIES

A. Independence of Action and Consequences:

Child Support Enforcement has critical timelines and political and financial ramifications. Poor participation, judgment, and decisions can adversely affect the success of the Child Support Program. Failure to identify risks and issues in a timely manner could result in slippages in schedule and increased costs. Poor communication and coordination can adversely affect the Child Support Program and the children of California. Incumbent is responsible for independent work within business constraints; recommendations to management and executives; decisions for projects and outputs; and program, project, and staff decisions and actions. Consequences may have statewide and enterprise-wide impacts, including lost funding, project failure, failed business strategy, poor customer service and performance, risk exposure, loss of business continuity, missed business opportunities, and budget implications.

B. Personal Contacts:
The incumbent has contact with departmental managers; supervisors; Department of Child Support Services, state, and Local Child Support Agency staff; governmental agencies; contractors; interface partners; and vendors.

7. Acknowledgements

A. Employee's Acknowledgement: I have read and understand the duties listed above and I certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others. I have received a copy of the duty statement.

I can perform these duties with or without reasonable accommodation: ☐ **Yes** ☐ **No**

If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will notify the Reasonable Accommodation Coordinator in the Equal Employment Opportunity and Diversity Office.

Duties of this position are subject to change and may be revised as needed or required.

Employee's Name (Print):	
Employee's Signature:	
Date:	

B. Supervisor's Acknowledgment: I certify this duty statement represents current and an accurate description of the essential functions of this position. I have discussed the duties of this position with and provided the above-named employee a copy of this duty statement.

Supervisor's Name (Print):	
Supervisor's Signature:	
Date:	