Office of
Technology &
Solutions
Integration
CALIFORNIA HEALTH &
HUMAN SERVICES AGENCY

☒ Current
☐ Proposed

DUTY STATEMENT

1. POSITION INFORMATION

Civil Service Classification	Working Title
Information Technology Specialist I (ITS I)	Information Security Analyst

Employee Name	Position Number
Vacant	791-753-1402-036

Project/Division Name	Supervisor's Name
Child Welfare Digital Services (CWDS)	Vijay Vemuri

Unit	Supervisor's Classification
Information Security	Information Technology Manager I (ITM I)

Physical Work Location	Duties Based on:
2870 Gateway Oaks Dr. Sacramento, 95833	☒ Full Time ☐ Part Time - Fraction Click here to enter text.

Effective Date
TBD

2. REQUIREMENTS OF POSITION

Check all that apply:

☒ Conflict of Interest Filing (Form 700) Required   ☒ Requires Fingerprinting & Background Check

☐ May be Required to Work in Multiple Locations   ☒ Other *(specify below in Description)*

Description of Position Requirements *(e.g., the position may move from project to project upon business need, managing staff at an alternate location, graveyard/swing shift, frequent travel, etc.)*:

Remote Centered. Hybrid workplace environment. Telework available based on business need.

The incumbent will participate in an on-call rotation for Security Incidents. While on-call, the incumbent will carry a state issued cell phone and be available for duty 24x7.

3. DUTIES AND RESPONSIBILITIES OF POSITION

IT Domains used:

☐ Business Technology Management   ☐ Information Technology Project Management

☐ Client Services   ☒ Software Engineering

☒ Information Security Engineering   ☒ System Engineering

Summary Statement (Briefly describe the position's organizational setting and major functions):

Under the direction of the Information Security Chief (Information Technology Manager I), the Information Technology Specialist I (Information Security Analyst) will develop, maintain, and formulate a secure posture for CWDS projects. Duties include:

- Execution of Penetration and Vulnerability Scans.
- Review and perform risk analysis, of security events.
- Perform appropriate follow-up tasks with partner teams and CWDS leadership to report and help mitigate vulnerabilities.
- Define and drive implementation of security policies, standards, and procedures as necessary in adherence of state and federal compliance requirements.
- Act in accordance with Code of Ethics and demonstrate professionalism and respectful interactions with internal and external partners.

Percentage of Duties	Essential Functions
45%	**Develop and support maintain a secure posture by:** • Executing Penetration tests and Vulnerability scans using various industry standard security tools. • Identifying, analyzing, and reporting any potential security risks, threats or vulnerabilities observed in the various environments the projects operate in.

	• Ensuring that any reported security issues in tools used by the project are addressed in collaboration with the vendors and stakeholders. • Reviewing and analyzing network and system events using security tools such as Tenable, Splunk, and other on-prem or cloud-based security tools. • Using tools such as Jira and ServiceNow to coordinate reporting activities and corrective actions for mitigation of identified security threats or vulnerabilities through appropriate Risk Management, Incident Management, Bug reporting tools. • Collecting evidentiary artifacts and creating reports/metrics using approved security tools to document potential threats and vulnerabilities from various cloud and on-prem operating environments; and • Developing and/or reviewing data sharing agreements to ensure compliance with appropriate state and federal regulations. • Collaborating with all project stakeholders to ensure effective exchange of all appropriate security information Leading the utilization of data loss prevention tools and triaging the issues identified. Subscribing to state's security information communication forums to be appraised of latest security risks and threats, understanding impact on the project environments, and recommending appropriate mitigations. • Conducting analysis of any reported threats and risks to determine impact to CWDS programs and perform risk assessments for potentially impacted instances. • Perform security audits of project assets as directed. • Developing and presenting Information Security Training material to the project staff in collaboration with other team members and help spread awareness on common security topics.
25%	**Define, design, document and recommend security solutions using industry standards and methodologies and in compliance with state and federal policies by:** • Identifying and documenting security risks and vulnerabilities in the software development process. • Reviewing and performing Attack Surface Analysis and Privacy Reviews. • Developing necessary security controls to protect the program assets and working collaboratively with team members including subject matter experts from all stakeholder domains. This includes, but is not limited to Infrastructure, Technology, Service Desk, Product Management, QA Teams, etc. to provide expert guidance on information security related aspects.
15%	**Troubleshoot, analyze, and conduct root cause analysis of security issues by:** • Ensuring that all tasks are performed in compliance with policies, standards and procedures as described in State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) Section 5300 et. seq. • Reviewing all relevant service level agreements for compliance with legal and regulatory requirements; and Participating and leading the problem management and root cause analysis with team members and Subject Matter Experts to identify and recommend corrective actions.
Percentage of Duties	Marginal Functions
10%	**Develop, update, and recommend standards, procedures including related security controls to ensure:** • Compliance with applicable security, policies, frameworks, and standards, • The secure by design paradigm is well understood and champion its incorporation into the project lifecycle.
5%	Perform other duties as assigned.

4. WORK ENVIRONMENT *(Choose all that apply from the drop-down menus)*

Standing:	Rarely (1-6%)	Sitting:	Frequent (51-75%)
Walking:	Infrequent (7-12%)	Temperature:	Temperature Controlled Office Environment

Lighting:	Artificial Lighting	Pushing/Pulling:	1-25% of the time
Lifting:	1-25% of the time	Bending/Stooping:	1-25%

Other:	Remote centered hybrid workplace environment. Telework based on business need.

Type of Environment:	a. Cubicle b. High Rise

Interaction with Public:	a. Required to assist customers on the phone and in person. b. N/A c. N/A.

5. SUPERVISION

Supervision Exercised *(e.g., Directly – 1 Information Technology Supervisor II; Indirectly – 5 Information Technology Associates)*

None.

6. SIGNATURES

Employee's Statement:
I have reviewed and discussed the duties and responsibilities of this position with my supervisor and have received a copy of the Duty Statement and can perform the duties outlined above without a Reasonable Accommodation.

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

Supervisor's Statement:
I have reviewed the duties and responsibilities of this position and have provided a copy of the Duty Statement to the Employee.

Supervisor's Name (Print) Vijay Vemuri	
Supervisor's Signature	Date

7. HRD USE ONLY

Human Resources Division Approval

☐ Duties meet class specification and allocation guidelines. ☐ Exceptional allocation, 625 on file.	HR Analyst initials	Date approved
	NM	10/19/2020

Reasonable Accommodation Unit use ONLY *(completed after appointment, if needed)*

* If a Reasonable Accommodation is necessary, please complete a Request for Reasonable Accommodation form and submit to Human Resource Division (HRD), Reasonable Accommodation Coordinator.

List any Reasonable Accommodations Made:
Click here to enter text.

** AFTER SIGNATURES ARE OBTAINED:
- **SEND THE ORIGINAL DUTY STATEMENT TO HRD TO FILE IN THE EMPLOYEE'S OFFICIAL PERSONNEL FILE (OPF)**
- **PROVIDE A COPY TO THE EMPLOYEE**
- **FILE A COPY IN THE SUPERVISOR'S DROP FILE**