

☒ **PROPOSED**

☐ **CURRENT**

DUTY STATEMENT

Note: Shaded area is for Personnel Office use only.

PERSONNEL REQUEST NO.		EFFECTIVE DATE
DIVISION TECHNOLOGY SERVICES DIVISION		POSITION NUMBER (Agency – Unit – Class – Serial) 174-291-1414-009
UNIT INFORMATION SECURITY & PRIVACY OFFICE		POSITION CONTROL NO. 2406
INCUMBENT VACANT		CLASS TITLE INFORMATION TECHNOLOGY SPECIALIST II
Briefly (1 or 2 sentences) describe the position's organizational setting and major functions.		
<p>Under the administrative direction of the director of the Technology Services Division, the Information Technology Specialist II, as a member of the Information Security and Privacy Office (ISPO), is responsible for the enforcement of the California Department of Education's (CDE) and the State of California's information security and privacy policies and directives. The incumbent works on the development, oversight, administration, and technical implementation of the department's information security and privacy program standards, procedures, guidelines, safeguards, initiatives and processes.</p> <p>Regular travel to the State Special Schools and Services Division (SSSSD) schools and diagnostic centers will be required to oversee responsibilities related to this position. The majority of the duties for this position are in the Information Security Engineering domain.</p>		
% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. (Use additional sheet if necessary)	
30%	Information Security Compliance <ul style="list-style-type: none"> Ensures that the ISPO program follows California state security and privacy standards, policies, and procedures as documented in the State Administrative Manual (SAM 5300) and State Information Management Manual (SIMM 5300). Participates in security and privacy program audits and assessments conducted by California state oversight agencies and third-party contractors. Reviews findings and develops corrective action plans to address any non-compliance issues documented in the reports. Ensures timely communication with CDE executive and division management regarding information security and privacy issues, risks, and compliance. Directs the security and privacy training program for employees located at the Sacramento headquarters and SSSSD schools and diagnostic centers. Reviews pending IT contracts to ensure compliance with security and privacy policies and practices. 	
30%	Information Security Technical Monitoring and Consultation <ul style="list-style-type: none"> Proactively monitors CDE's information security-related products and services for signs of potential suspicious or malicious activity, and take appropriate remediation steps if necessary. Provides immediate response to high-priority alerts from information security-related products and services to ensure the potential problem is evaluated, and proper remediation steps are taken if necessary. Monitors the use of "shadow IT" products and services, and consult with CDE users on alternative solutions that minimize IT security risks. Reviews non-standard software requests which may cause an information security risk, and present possible options that meet CDE standards. Provides information security consultation for new IT projects, products, and services. Collaborates with the Executive Office and the Human Resources Division as a subject matter expert on IT security topics. Acts as CDE's Technology Recovery Plan coordinator. 	

30%	SSSSD Information Security Planning and Assessment <ul style="list-style-type: none"> Responsible for extending the CDE ISPO program to the SSSSD remote sites. These sites include two schools for the deaf (Fremont and Riverside), one school for the blind (Fremont), and three diagnostic centers (Fresno, Fremont and Los Angeles). Directs the efforts to conduct a comprehensive assessment of the SSSSD security and privacy issues, develops an IT asset inventory, and implements a security and privacy program correction and implementation plan. Investigates and assesses information security-related events (e.g., data breach) at SSSSD sites.
10%	Information Security Research <ul style="list-style-type: none"> Maintains an ongoing knowledge: (a) of State and Federal legislation, regulation, policies, and practices related to information security; (b) methodologies and best practices that are commonly used in the information security industry; (c) the status of State and Federal information security initiatives that offer opportunities for CDE or pose requirements to be met by the CDE; and, (d) the threats to and vulnerabilities of CDE assets to ensure the ISPO Program's efficiency and effectiveness.

To be reviewed and signed by the supervisor and employee:

Supervisor's statement:

- *I have discussed the duties and responsibilities of the position with the employee*
- *I have signed and received a copy of the duty statement.*

SUPERVISOR'S NAME (Print)

Rodney Okamoto

SUPERVISOR'S SIGNATURE



DATE

Employee's statement:

- *I have discussed the duties and responsibilities of the position with my supervisor*
- *I have signed and received a copy of the duty statement*

EMPLOYEE'S NAME (Print)

EMPLOYEE'S SIGNATURE



DATE

Distribution:

Original: Official Personnel File

Copy: Supervisor

Copy: Employee

Copy: Program File

☒ **PROPOSED**

☐ **CURRENT**

DUTY STATEMENT

Note: Shaded area is for Personnel Office use only.

PERSONNEL REQUEST NO.		EFFECTIVE DATE
DIVISION TECHNOLOGY SERVICES DIVISION		POSITION NUMBER (Agency – Unit – Class – Serial) 174-291-1402-XXX
UNIT INFORMATION SECURITY & PRIVACY OFFICE		POSITION CONTROL NO. 2406
INCUMBENT VACANT		CLASS TITLE INFORMATION TECHNOLOGY SPECIALIST I
Briefly (1 or 2 sentences) describe the position's organizational setting and major functions.		
<p>Under the administrative direction of the director of the Technology Services Division (TSD), the Information Technology Specialist I, as a member of the Information Security and Privacy Office (ISPO), helps to enforce the California Department of Education's (CDE) and the State of California's information security and privacy policies and directives. The incumbent works on the development, oversight, administration, and technical implementation of the department's information security and privacy program standards, procedures, guidelines, safeguards, initiatives and processes.</p> <p>Regular travel to the State Special Schools and Services Division (SSSSD) schools and diagnostic centers will be required to oversee responsibilities related to this position. The majority of the duties for this position are in the Information Security Engineering domain.</p>		
% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. (Use additional sheet if necessary)	
30%	Information Security Compliance <ul style="list-style-type: none"> • Works with CDE staff to ensure the ISPO program follows California state security and privacy standards, policies, and procedures as documented in the State Administrative Manual (SAM 5300) and State Information Management Manual (SIMM 5300). • Provides support with security and privacy program audits and assessments conducted by California state oversight agencies and third-party contractors. Reviews findings and helps to develop corrective action plans to address any non-compliance issues documented in the reports. • Drafts communication for CDE executive and division management regarding information security and privacy issues, risks, and compliance. • Assists with the security and privacy training program for employees located at the Sacramento headquarters and SSSSD schools and diagnostic centers. • Reviews pending IT contracts to ensure compliance with security and privacy policies and practices. 	
30%	Information Security Technical Monitoring and Consultation <ul style="list-style-type: none"> • Proactively monitors CDE's information security-related products and services for signs of potential suspicious or malicious activity, and take appropriate remediation steps if necessary. • Works with subject matter experts to provide immediate response to high-priority alerts from information security-related products and services to ensure the potential problem is evaluated, and proper remediation steps are taken if necessary. • Monitors the use of "shadow IT" products and services, and consult with CDE users on alternative solutions that minimize IT security risks. • Reviews non-standard software requests which may cause an information security risk, and present possible options that meet CDE standards. • Works with subject matter exports to provide information security consultation for new IT projects, products, and services. • Collaborates with the Executive Office and the Human Resources Division on IT security topics. • Assists in the development of CDE's Technology Recovery Plan. 	

30%	SSSSD Information Security Planning and Assessment <ul style="list-style-type: none"> Provides support for the CDE ISPO program at the SSSSD remote sites. These sites include two schools for the deaf (Fremont and Riverside), one school for the blind (Fremont), and three diagnostic centers (Fresno, Fremont and Los Angeles). Assists in the efforts to conduct a comprehensive assessment of the SSSSD security and privacy issues, including the development of an IT asset inventory, and implementation of a security and privacy program correction and implementation plan. Works with management to investigate and assess information security-related events (e.g., data breach) at SSSSD sites.
10%	Information Security Research <ul style="list-style-type: none"> Maintains an ongoing knowledge: (a) of State and Federal legislation, regulation, policies, and practices related to information security; (b) methodologies and best practices that are commonly used in the information security industry; (c) the status of State and Federal information security initiatives that offer opportunities for CDE or pose requirements to be met by the CDE; and, (d) the threats to and vulnerabilities of CDE assets to ensure the ISPO Program's efficiency and effectiveness.

To be reviewed and signed by the supervisor and employee:

Supervisor's statement:

- *I have discussed the duties and responsibilities of the position with the employee*
- *I have signed and received a copy of the duty statement.*

SUPERVISOR'S NAME (Print)

Rodney Okamoto

SUPERVISOR'S SIGNATURE



DATE

Employee's statement:

- *I have discussed the duties and responsibilities of the position with my supervisor*
- *I have signed and received a copy of the duty statement*

EMPLOYEE'S NAME (Print)

EMPLOYEE'S SIGNATURE



DATE

Distribution:

Original: Official Personnel File

Copy: Supervisor

Copy: Employee

Copy: Program File