California Office of Digital Innovation

Duty Statement

☐ Current ☒ Proposed

IT Domain: Information Security Engineering

Classification	**Office/Department**
Information Technology Specialist II	Office of Digital innovation
Working Title	**Unit/Section**
Information Security Officer	Operations
Position Number	**Effective Date**
374-100-1414-XXX	
Name	**Date Prepared**
Vacant	5/3/2022

General Statement

Under the general direction of the Chief Information Officer (IT Manager II), the Information Technology Specialist II (IT Specialist II) acts as the Information Security Officer (ISO) for the Office of Digital Innovation (ODI). The ISO directs all areas and responsibilities of the Information Security Office. The incumbent acts as a technical lead on the most complex IT security projects and systems that impact the Department. The ISO is responsible for implementing policies and standards regarding the confidentiality and security of information pertaining to ODI and development, implementation, maintenance of, and adherence to ODI and state privacy policies and procedures. The incumbent works collaboratively with the ODI management team and staff, briefs and advises leadership, exercises a high degree of initiative, independence of action, and originality, and must demonstrate tact and good judgment. The incumbent must be able to communicate effectively in order to develop and maintain effective and cooperative working relationships. The incumbent must be able to adapt easily to changing priorities. Duties include, but are not limited to, the following:

Essential Functions

%	Description
45%	• Develop and maintain ODI's information security program standards, plans, guidelines, practices, and procedures to align and comply with statewide requirements and goals as outlined in the State Administrative Manual (SAM), the

	Statewide Information Management Manual (SIMM), IT Technology Letters, and other published and required materials as appropriate. ● Develop, document, implement, and follow assigned procedures and components of ODI's information security program, including but not limited to Risk Management, Audit and Compliance Management, Information Security Governance, Incident Management and Reporting, Policy Management, and Security Awareness, Education, and Training. ● Evaluate, identify, configure, implement, optimize, maintain, troubleshoot, and remediate issues with information security related equipment, software, and services, including but not limited to: Endpoint Detection and Response (EDR), Intrusion Detection/Prevention Platforms (IDP/IPP); anti-phishing; disk encryption; security awareness and training; risk, threat, and vulnerability assessment; and Security Information and Event Management (SIEM) products and components. ● Conducts regular reviews of key systems including intrusion detection, data loss prevention, firewalls, routers, and system logs, and investigates anomalies, as needed. ● Respond and mitigate, remediate, or resolve information security incidents using approved procedures and tools, ensuring proper documentation of activities performed and final results. ● Conduct information security related confidential investigations as required and serve as the central point of contact to internal and external security investigatory entities.
30%	● Develop and document a risk assessment methodology that includes the recommendation, selection, and application of vulnerability identification and corrective tools. ● 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). ● Perform and report on complex risk assessments, including monthly evaluation and tracking of threats and vulnerabilities, for ODI IT assets and systems, including network designs, server and network service configuration, and application design and functionality. ● Evaluate, recommend, and document existing and/or needed IT security policies or policy improvements based on analysis of existing requirements and/or trends in information security incidents or security industry developments. ● Assist in the evaluation of non-standard IT products for recommended approval or denial based on risk and compliance evaluation criteria. ● Research, identify, and document IT project security requirements, including system and application development, upgrade, and migration projects, to ensure inclusion of and compliance with all applicable state and federal regulatory requirements. ● Track and assist program customers and IT peers in filling out SIMM 5305 Classification and Categorization worksheets and use that information to further develop and document required System Security Plans for all ODI systems. ● Perform information security gap analyses to identify as-is and to-be designs and/or processes as required. ● Research, document, and file state-mandated compliance reports to the California Department of Technology according to predefined reporting schedules, including but not limited to SIMM 55, SIMM 5305, SIMM 5320, SIMM 5325, and SIMM 5330 reports. ● Research technologies and make appropriate recommendations to leadership about existing and future information security service improvements and efficiencies.

20%	• Participate in the contingency planning for the ODI by assisting in the development of the Department's Emergency Operations Plan and Business Continuity Plan. • Develop, document, improve, and implement the Department's Technology Recovery Plan (TRP), including coordination and documentation of Business Impact Assessments, and annualized evaluation and testing of recoverability standards against service level agreements and/or objectives. • Ensure that the TRP is maintained and tested periodically to validate its effectiveness in recovering critical information assets in the event of a disaster. • Plan, design, develop, and execute customized phishing test campaigns for the Department using approved procedures and tools, following established approval processes, and providing test results and remediation recommendations to leadership. Identify, develop, and/or maintain information security awareness outreach, training, and service materials to support ongoing security awareness initiatives, abilities, and requirements. • Develop and document information security marketing materials, including guides, standards, procedures, and knowledge articles for distribution to ODI customers. • Analyze legislation and Federal and State mandates for their effect on ODIs security policies.

Marginal Functions

5%	• Perform other assignments as appropriate and required

Supervision Received
The Information Security Officer will report to the Chief Information Officer.

Supervision Exercised
None, however, may lead teams to carry out information security related projects.

Working Conditions
The employee regularly works in an indoor and climate-controlled office setting under artificial light. The employee's workstation is located in Sacramento, CA, and is equipped with standard or ergonomic office equipment, as appropriate. Based on departmental or operational needs, work can be performed remotely. Occasional travel may be required to attend offsite meetings, conferences, and training classes. May sit for an extended period using a keyboard and video display terminal. On occasion, may require flexible work schedules, including some evening hours to complete assignments, meet deadlines, and provide support to the Directorate.

Attendance
Must maintain regular and acceptable attendance at such a level as is determined ODI's sole discretion. Must be regularly available and willing to work the hours the department determines are necessary or desirable to meet its business needs.

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. *(If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor.)

A Reasonable Accommodation is any modification or adjustment made to a job, work environment, or employment practice or process that enables an individual with a disability or medical condition to perform the essential functions of their job or to enjoy an equal employment opportunity.

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

Employee Signature	**Employee Printed Name**	**Date**

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

Supervisor Signature	**Supervisor Printed Name**	**Date**