STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF AGING
DUTY STATEMENT
CDA 9003 (REV 04/2021)

1. INCUMBENT	**2. EFFECTIVE DATE (MM/DD/YYYY)**
3. DIVISION Division of Information Technology	**4. UNIT NAME** Information Security Branch
5. CLASSIFICATION Information Technology Manager I	**6. POSITION NUMBER** 797-910-1405-001

7. SUPERVISOR'S STATEMENT: *I CERTIFY THAT THIS DUTY STATEMENT REPRESENTS AN ACCURATE DESCRIPTION OF THE ESSENTIAL FUNCTIONS OF THIS POSITION.*

SUPERVISOR'S NAME (Print)	**SUPERVISOR'S SIGNATURE**	**DATE**
Andrea Hoffman		

8. EMPLOYEE'S STATEMENT: *I HAVE READ THIS DUTY STATEMENT AND AGREE THAT IT ACCURATELY REPRESENTS THE DUTIES I AM ASSIGNED.*

EMPLOYEE'S NAME (Print)	**EMPLOYEE'S SIGNATURE**	**DATE**

You are a valued member of the department's team. All CDA employees are expected to work collaboratively with internal and external stakeholders to enable the department to provide the highest level of service possible. Your efforts to treat others fairly, honestly, and with respect are important to everyone who works with you. We value diversity at CDA and we strive to achieve equity and inclusion in the workplace for all employees. We believe that a diverse workforce and inclusive workplace culture enhances the performance of our organization and the quality of representation that we provide to a diverse client base.

9. DESCRIPTION

Under the direction of the Chief Information Officer (CIO), the Information Technology Manager I (ITM I) will lead the California Department of Aging (CDA) and the California Commission on Aging (CCoA) security program as the Information Security Officer (ISO). The ITM I oversees IT staff within the Information Security Branch and is responsible for ensuring the protection of information assets, including all data and systems, in compliance with state and federal security policies, standards, and requirements. The ITM I will develop security strategies and oversee operational plans to meet security goals and reinforce security policy. The ITM I will lead security initiatives to improve the security posture, remediate security risks and ensure the ongoing protection of information and systems, and provide exceptional customer services to CDA, CCoA and stakeholders by developing collaborative partnerships. The ITM I will provide guidance to diverse audience groups on the protection of confidential and sensitive information. The ITM I will implement practices to strengthen and improve the security program from a people, process, technology, and information perspective.

The duties are broadly defined as follows:

35% Information Security Leadership

- Develops and matures the security program to ensure the confidentiality, integrity, and availability of information assets. Ensures the security program meets compliance timeframes and adheres to state, federal, and other security requirements.
- Provides leadership related to security strategy, planning, compliance, policy, governance, operations, and monitoring. Facilitates resolution to the most complex security issues.
- Prioritizes workloads and direct staff responsible for security training, tools, reporting, risk and incident management, security architecture, vulnerability management, forensics and investigations, audits, technology recovery, and other security operational areas.
- Provides guidance to staff and stakeholders that balances the need for security compliance with business needs. Responds to security inquiries and communicates complex security information to technical and nontechnical audiences at various hierarchical levels.
- Reviews and approves security plans, procedures, procurement documents, as well as formal submissions and reports to state/federal entities.
- Guides planning and development the security architecture; evaluates and proposes security technologies. Oversees the deployment, configuration, and maintenance of security solutions.
- Formulates security recommendations related to legislation, purchase requests, projects, and policy that is consistent with state and federal requirements. Prepares and delivers presentations to various technical and non-technical audiences.
- Participates in strategic planning activities to define roadmaps, initiatives, and plans that align information security needs with CDA strategic goals.
- Participates in security workgroups and committees and represents CDA with stakeholders and government entities. Develops strong relationships with control agencies to effectively coordinate security policy, audits, reporting, incidents, and other areas impacting security.

30% Security Policy, Compliance, and Risk

- Leads security compliance for all requirements regulating information security and confidentiality such as the State Administrative Manual (SAM), State Information Management Manual (SIMM), Health Insurance Portability and Accountability Act (HIPPA), Personal Identifiable Information (PII), Protected Health Information (PHI), National Institute of Standards and Technology (NIST), and other requirements.
- Facilitates development of security reports and dashboards to present the level of controls, compliance, and current IT risk posture.
- Establishes Security Governance to address risk, priorities, policy, and compliance. Makes policy recommendations regarding sensitive and information security issues. Facilitates security policy development, updates, review, approval, and implementation consistent with security requirements and to protect confidential and sensitive information.
- Develops guidelines, standards, and practices to help communicate security policy information to stakeholders. Enforces policy through stakeholder education and monitoring.
- Collaborates with the CDA Privacy Officer on data privacy matters to limit departmental risk exposure and to ensure data privacy compliance with state and federal requirements.
- Collaborates with the Chief Data Officer on data classification and categorization related to protecting program data (storing, sharing), data masking, encryption, and data loss prevention.
- Oversees planning, coordination, and execution of security audits. Leads audit response, reporting, and remediation efforts. Participates in disaster recovery exercises.

- Develops proactive IT security risk and vulnerability management practices. Develops and manages frameworks, processes, tools, and consultancy necessary to properly manage risk, mitigate risk and make risk-based decisions. Leads security staff for ongoing compliance, risk assessments on systems and use of data, and vulnerability mitigation.

20% Information Security Operations

- Leads a culture of operational excellence by regularly evaluating the effectiveness of Branch services. Monitor ongoing changes that impact information security. Implements security measures to protect information assets from threat vectors. Incorporates best practices, requirements, and continuous improvement into security operations.
- Works with technical teams to optimize the technical environment to prevent, detect, and mitigate vulnerabilities and improve the overall security posture. Advises staff on controls, risk mitigation measures, tools, and configurations to enhance information and data security.
- Conducts security assessments to detect and mitigate cybersecurity threats and prohibit access to inappropriate content and unauthorized data.
- Implements practices and controls to secure the network, servers, storage, hardware, software, cloud, telecommunications, and other components within the IT environment.
- Oversees the security awareness training curriculum, platform, and compliance. Ensures training is current, updated, and timely and available for stakeholder consumption. Develops security campaigns and practices to increase security literacy, protect information assets, and minimize risks related to loss, theft, and misuse of IT assets and data.
- Keeps abreast of new/emerging security technologies, methods, and best practices through research and engagement with public, and private partners. Reviews procurement items to ensure acquisition of hardware, software, and services meet security requirements.

10% Incident Management and Response

- Develops, documents, implements, and optimizes incident management processes to effectively monitor, assess, and manage new and emerging threats.
- Directs incident response, reporting, and escalation activities for security events or exploited vulnerabilities such as unauthorized system or network access, denial of service, inappropriate data access, collection of confidential or sensitive information. Coordinates technology recovery activities and leads incident reporting.
- Maintains a current Technology Recovery Plan (TRP) that aligns with business priorities. Coordinates planning, testing, and reporting activities across multidisciplinary teams.
- Provides timely communications to stakeholder groups related to security incidents and recovery. Identifies, escalates, reports, mitigates, and resolves security incidents.
- Coordinates security incidents/events involving data privacy with the Privacy Officer for potential loss, theft, misuse of IT assets and/or confidential data.
- Oversees security forensics and investigations. Prepares and delivers written findings and recommendations. Ensures investigations include analysis, development, and execution of Corrective Action Plans (CAP). Develops CAP related to security vulnerabilities and audits.
- Oversees root cause analysis and remediation of security incidents. Collaborates with business partners to assess and mitigate impacts. Directs coordination across business, technical and/or external service providers to resolve security issues.

5% Marginal Duties

- Performs other related duties, as required.

Revised 10/27/2023