DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH

DUTY STATEMENT

JOB TITLE: Information Technology Manager II **POSITION #:** 472-508-1406-917

WORKING TITLE: Chief Information Security Officer **EMPLOYEE:**

POSITION DESCRIPTION: Under administrative direction of the Department's Chief Information Officer, the Information Technology Manager II (ITM II) serves as the Department's Chief Information Security Officer (CISO) and Department AI Cybersecurity Officer. The CISO is the executive responsible for establishing and directing the Department's enterprise information security, cybersecurity, privacy coordination, data protection, risk and compliance, security architecture and engineering, security operations, technology recovery, and artificial intelligence security programs. The CISO is responsible for establishing and enforcing enterprise information security policies, driving long-range security strategies, and overseeing the Information Security Branch to ensure alignment with the Department's IT strategic direction. The position provides expert leadership in risk management, threat mitigation, vulnerability assessments, security incident investigation, security compliance, security architecture planning, disaster recovery, and security agreements with external partners supporting our programs in Headquarters, the 21 regional centers, and state-operated facilities. The CISO maintains enterprise accountability for safeguarding the Department's IT infrastructure, networks, devices, and data, ensuring the confidentiality, integrity, and availability of critical information assets. This includes developing and maintaining policies and controls necessary to protect Protected Health Information (PHI) and Personally Identifiable Information (PII) for more than five hundred thousand individuals served across highly complex applications, 21 regional centers, state-operated facilities, and over 29,000 community service providers.

SUPERVISION EXERCISED: Supervisory and Rank and File IT Staff.

SUPERVISION RECEIVED: Reports to and under administrative direction of the Department's Chief Information Officer.

DOMAINS:

Client Services:	critical skills
Business Technology Management:	critical skills
IT Project Management:	moderate skills
Software Engineering:	moderate skills
System Engineering:	critical skills
Information Security Engineering:	critical skills

EXAMPLES OF DUTIES:

Essential Job Functions:

25% Provide enterprise leadership in the development, implementation, and enforcement of information security policies, standards, and procedures that safeguard the confidentiality, integrity, and availability of Department data, including highly sensitive medical records for individuals served by regional centers, community service providers, and state-operated facilities. Direct and monitor the implementation of security policies, systems, and processes to ensure compliance with federal and state laws, regulations, and guidance such as California Civil Code, the State Administrative Manual (SAM), HIPAA, NIST standards, and directives issued by CMS and SSA. Serve as the Department AI Cybersecurity Officer and lead the secure, privacy-conscious, and responsible deployment of enterprise generative artificial intelligence, including Microsoft Copilot. Lead or participate in Department and statewide strategic security planning through collaboration with executive leadership, state committees, and the California Department of Technology. Oversee internal and external security assessments that validate compliance through automated tools, document reviews, and staff interviews. Develop and justify budget, staffing, contracts, tools, and service requirements necessary to address the Department's enterprise security, privacy, compliance, and recovery responsibilities.

25% Oversee all Department information security functions, including management of privacy and security incidents, detection and prevention of vulnerabilities and attacks, and mitigation of employee misuse of Department resources. Direct the operation and administration of complex security technologies such as intrusion detection, vulnerability assessment, penetration testing, web content filtering, security event management, and forensic analysis tools. Provide expert guidance on low-risk implementation of artificial intelligence solutions, secure file transfer, endpoint protection, identity management, data encryption, data loss prevention, secure application development, and enterprise security architecture. Direct enterprise data discovery, inventory, and classification across Microsoft 365 and SharePoint, cloud file services, Snowflake, Amazon RDS, and other repositories; oversee implementation of Varonis, Microsoft Purview, sensitivity labeling, and data loss prevention controls to protect PHI and other sensitive information. During suspected security or data breaches, direct response activities and advise the CIO and Chief Deputy Director on actions that may involve public notification, financial impacts, and potential legal consequences.

20% Plan, direct, and oversee all activities of the Information Security Office, providing clear guidance, direction, and support to staff. Develop management and supervisory personnel through coaching, timely performance feedback, and structured development plans. Mentor current and emerging IT leaders to ensure technical excellence, leadership readiness, and ongoing professional growth. Foster strong teamwork across all service delivery functions, promote cross-training, and drive continuous process improvement. Create a positive environment that supports change, staff motivation, and ongoing training opportunities to build and maintain a highly skilled security workforce. Establish and communicate performance expectations for all team members. Define long-term goals and objectives for the Information Security Office and allocate resources accordingly. Oversee the development and maintenance of all required policies, standards, procedures, and related governance materials necessary to achieve the Office’s mission and security objectives.

15% Provide executive oversight for cybersecurity assessments and advisory services offered to Regional Centers and other business associates to improve maturity and strengthen the broader Department security ecosystem. Partner with regional centers to ensure they are progressing toward a secure and resilient environment as the Department transitions to the centralized LOIS platform. Conduct bi-annual information security assessments to identify vulnerabilities, verify remediation efforts from prior assessments, and provide targeted recommendations to reduce risk. Ensure regional centers maintain compliance with HIPAA requirements, protect sensitive data, and work proactively with their vendors to secure Department information. Provide tailored security training to regional center staff, deliver guidance on emerging threats and best practices, and identify tools and solutions that strengthen their overall security posture. Support regional centers in adopting consistent security standards and improving their operational readiness as part of statewide modernization efforts.

10% Provide leadership and oversight for the planning, organization, and coordination of all Department technology recovery activities. Establish policies, strategies, and standards that ensure technology recovery plans meet all state and federal requirements, including the Statewide Information Management Manual (SIMM), CMS directives, and NIST best practices. Guide the assessment of the criticality of Department applications and determine appropriate levels of contingency planning, including the identification of alternate recovery sites, development of recovery strategies and detailed recovery procedures, and execution of regular recovery exercises. Ensure that recovery capabilities align with business needs and support continuity of operations during disruptive events. Ensure recovery tests, tabletop exercises, after-action reports, corrective actions, and lessons learned inform enterprise priorities, architecture, system plans, and investment decisions.

Marginal Job Functions:

5% Represent the Department on special committees, task forces, working groups, and professional forums related to information security, privacy, technology, resilience, and emerging risk. Complete other required duties within the scope of the classification.

DESIRABLE QUALIFICATIONS:

Knowledge of: Enterprise information security principles, frameworks, and practices, including security governance, risk management, incident response, vulnerability management, and security architecture; service-oriented and event-driven architecture, systems design, technology integration, and infrastructure platforms/protocols; IT project management methodologies, research and development approaches, IT service management, and organizational change management; regulatory and compliance requirements, including HIPAA, SOX, PCI, NIST, GLBA, CMS, and SSA directives, and how these requirements apply within large public-sector environments; data privacy laws, practices, and safeguards, including secure data acquisition, protection, transmission, retention, and disposal; organization and functions of California State Government, including its policies, principles, and governance structures; technical concepts across major IT domains such as networking, applications, databases, operating systems, cloud platforms, identity management, and endpoint protection; international, federal, state, and local laws governing data security and privacy; enterprise IT disciplines and how they interrelate (infrastructure, servers, networks, databases, applications, security operations, etc.) to support business missions.

Ability to: Lead and manage enterprise information security programs, including policy development, risk assessment, incident response, and compliance oversight; develop strategic plans, aligning security initiatives with organizational priorities, and translating complex security requirements into actionable operational activities; supervise, mentor, and develop technical and managerial staff, fostering teamwork, accountability, professional growth, and continuous improvement; analyze, problem-solve, and evaluate complex technical environments, identify risks, and recommend effective mitigation strategies; communicate clearly and effectively with executive leadership, program staff, and technical teams, including the ability to explain complex security concepts to non-technical audiences; evaluate, select, and implement security technologies, tools, and platforms to strengthen enterprise security posture; manage large-scale security projects and initiatives, including timelines, resources, dependencies, and change management; conduct and oversee security assessments, audits, and reviews using automated tools, documentation analysis, and stakeholder interviews; interpret and apply federal and state laws, regulations, and standards governing information security and privacy; build partnerships with program leaders, regional centers, external partners, and state oversight entities to align security expectations and drive compliance; develop and maintain disaster recovery and technology contingency plans, including conducting business impact analyses and coordinating recovery exercises; negotiate, coordinate, and manage vendor relationships related to security products, services, and third-party compliance requirements; oversee and ensure proper handling, protection, and transmission of sensitive and confidential data across complex distributed environments.

WORKING CONDITIONS: Open-spaced partitioned offices. Prolonged periods utilizing a computer most of the time. Occasional travel including overnight or day trips for covered California locations. May require 24/7 on-call support as well as weekend support responsibility. This position is a hybrid, in-office/telework position, and may be subject to change. Incumbent can be required to report to the office, or any designated location at any time. Telework agreements can be modified and/or cancelled at any time.

CERTIFICATION OR LICENSE: None.

Employee Name (Print)	Employee Signature	Date
Supervisor Name (Print)	Supervisor Signature	Date

Employee and Manager acknowledge that by signing this Duty Statement that they have discussed and agree to the expectations of the position.