Department of Cannabis Control
CALIFORNIA

Position Duty Statement

DCC-2409

☐ **PROPOSED** ☒ **CURRENT**

Classification Title Information Technology Manager I	**Division** Information Technology (IT) Services
Working Title Information Security Officer	**Office/Section/Unit/Geographic Location** IT Operations Branch / Information Security Office / Sacramento
Position Number 592-640-1405-001	**Name and Effective Date**

General Statement: Under the general direction of the CEA-B (Chief Information Officer), the Information Technology Manager I (ITMI) serves as the Information Security Officer (ISO) and Chief Privacy Officer (CPO) for the Department of Cannabis Control (DCC). The ISO directs all areas and responsibilities of the Information Security Office. The ISO/CPO is responsible for implementing state policies and standards regarding the confidentiality and security of information pertaining to DCC and the development, implementation, maintenance of, and adherence to State and DCC privacy policies and procedures. This position is in the Information Security Engineering domain. Duties include, but are not limited, to the following:

A. Specific Assignments [w/Essential (E) and Marginal (M) Functions]

35% (E) Directs the Information Security Program

Advises the Director, Chief Deputy Director, and Chief Information Officer over all matters related to the security of DCC information assets. Develops information security plans, policies, procedures, and standards to ensure the confidentiality, integrity, availability, and appropriate use of DCC information assets. Conducts security risk assessments to identify threats and vulnerabilities to DCC information and advises Executive Officers and DCC management, through formal recommendations, on measures that can be taken to eliminate or mitigate identified risks. Oversees the email quarantine process and authorizes the release of any quarantined emails that contain confidential information. Investigates and resolves the authenticity of reported security incidents and violations. Coordinates all external reporting and files Information Security Incident Reports with the State's Office of Information Security and Privacy Protection and the California Highway Patrol Emergency Notification and Tactical Alert Center. Protects DCC's sensitive resources against misuse, abuse, and unauthorized use by developing and enforcing strict controls that regulate an individual's access to and use of information resources.

Serves on the Executive Steering Committee for critical interdepartmental IT projects to ensure the integration of appropriate information security protocols and controls. Coordinates efforts to provide for the integrity and security of DCC's information assets and provides for the security of IT facilities, software, and equipment. Reviews

Feasibility Study Reports to ensure appropriate security protocols are being addressed. Oversees the DCC information security awareness program.

25% (E) Directs the Information Privacy Program
Develops privacy policies and procedures to limit the collection of and safeguard the privacy of personal information collected or maintained by DCC and any of its constituent agencies. 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.). Reviews and approves all privacy considerations for the automated and manual environment containing confidential or sensitive data. Oversees, directs, and ensures delivery of annual privacy education and awareness training to all DCC employees. Responds to inquiries from consumers and licensees related to the DCC Privacy Policy.

15% (E) Oversees Operational Recovery Plan
Establishes policies and procedures and coordinates efforts that maintain cost-effective risk management processes intended to preserve DCC's ability to meet state program objectives in the event of the unavailability, loss, or misuse of information assets. Ensures the recoverability of DCC's systems and assets by overseeing the development, implementation, testing, and maintenance of DCC's Operational Recovery Plan to assure continuity of computing operations for the support of critical applications during a period of man-made or natural disaster. Establishes and maintains processes for the analysis of risk associated with DCC information assets.

15% (E) Represents DCA as a Member of National and State Security Organizations
Serves as a member of the State and Consumer Services Agency Information Security Officer's Committee to ensure the protection of vital assets and the sustainability of operations within the State and Consumer Services Agency. Meets and confers with high-level information security personnel from other state departments, governmental officials, and private sector businesses regarding matters affecting security policy and procedures.

10% (E) Analyzes Legislation
Analyzes legislation and Federal and State mandates for their effect on DCC security policies.

B. <u>Supervision Received</u>
The incumbent works under the general direction of the Chief Information Officer.

C. <u>Supervision Exercised</u>
The incumbent directly supervises IT Specialists.

D. <u>Administrative Responsibility</u>
The incumbent has complete responsibility for managing the Information Security Office and staff.

E. Personal Contacts

The incumbent has contact with all levels of the DCC staff, consultants, vendors, California Technology Agency staff, Control Agency staff, and other government agencies. This includes DCC's Divisions, Branches, Offices, and Units including executive management. Contacts may be initiated with other departments, governmental agencies, and private companies concerning information system and data center technologies as they related to the performance of this position.

F. Actions and Consequences

The incumbent will make decisions that impact the functionality of the DCC technology applications and solutions. Failure to properly administer duties using good judgment, logic, and discretion, may result in poor performance or unusable systems and/or applications, and prevent the DCC end users from effectively performing their duties. In addition, substantial workload backlogs may occur, online consumer services may be unavailable, and the DCC may be unable to carry out mandates designed to protect consumers, licensees, and applicants.

G. Functional Requirements

The incumbent is a Work Week Group E employee and is expected to work an average of 40 hours per week each year and may be required to work specified hours based on the business needs of the office. The incumbent must occasionally move about inside the office to access office machinery. The incumbent must constantly operate a computer and other office productivity machinery, such as a copy machine. The incumbent must be able to remain in a stationary position 50% of the time. The incumbent may be required to perform duties at local client sites as required and at any of DCC's statewide field sites as scheduled in advance.

H. Other Information

The incumbent must be able to reason logically and creatively and utilize a wide variety of skills to resolve enterprise-wide technical issues, application development and multiple system interface issues. Additionally, this position must have ability to communicate and resolve business related issues/problems that require a technology solution. Incumbent must be able to develop and evaluate alternatives and research and present ideas and information effectively both orally and in writing. Incumbent must be able to consult with and advise interested parties on IT subjects, gain and maintain the confidence and cooperation of those contacted, and accurately assign priorities to multiple projects at any given time and to remain flexible. The incumbent shall operate to protect the cyber security of individual departmental staff, the Department's network and infrastructure, and all data assets.

Additional Performance Expectations:

Ability to work cooperatively with others
Ability to work efficiently
Ability to report to work on time
Ability to maintain consistent, regular attendance
Ability to work under changing deadlines
Ability to look and act in a professional manner

Ability to get along with others
Ability to exhibit courteous behavior towards others at all times
Ability to meet deadlines
Ability to perform tasks with minimal amount of errors
Ability to do completed staff work

Criminal Offender Record Information (CORI): Title 11, section 703 (d) of the California Code of Regulations requires criminal record checks of all personnel who have access to Criminal Offender Record Information (CORI). Pursuant to this requirement, applicants for this position will be required to submit fingerprints to the Department of Justice and be cleared before hiring. In accordance with CORI procedures, clearance shall be maintained while employed in a CORI-designated position. Additionally, the position routinely works with sensitive and confidential issues and/or materials and is expected to maintain the privacy and confidentiality of documents and topics pertaining to individuals or to sensitive program matters at all times.

Conflict of Interest: This position is subject to Title 16, section 3830 of the California Code of Regulations. The incumbent is required to submit a Statement of Economic Interests (Form 700) within 30 days of assuming office, annually by April 1st, and within 30 days of leaving office.

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. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the Health & Safety analyst.)

_____
Employee Signature Date

_____
Employee's Printed Name – Classification

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 Date

_____
Supervisor's Printed Name – Classification

Rev 7/2022