



☐ PROPOSED ☒ CURRENT

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

General Statement: Under the general direction of the Career Executive Assignment-B (CEA-B) of the Information Technology Services Division (Division), within the Department of Cannabis Control (Department), the Information Technology Manager I (ITM I) in the Information Security Office (Office) will serve as the Chief Information Security Officer (CISO) and Privacy Officer (PO) for the Department. The incumbent will direct all areas and responsibilities of the Office. The incumbent will be responsible for implementing State of California (State) policies and standards regarding the confidentiality and security of information pertaining to the Department and the development, implementation, maintenance of, and adherence to State and Department 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) Direct the Information Security Program

Advise the CEA-B, Chief Deputy Director, and Director on all matters related to the security of Department information assets. Develop information security plans, policies, procedures, and standards to ensure confidentiality, integrity, availability, and appropriate use of Department information assets. Conduct security risk assessments to identify threats and vulnerabilities to Department information and advise Executive Officers and DCC Department management on measures that can be taken to eliminate or mitigate identified risks through formal recommendations. Oversee the email quarantine process and authorize the release of any quarantined emails that contain confidential information. Investigate and resolve the authenticity of reported security incidents and violations. Coordinate all external reporting and file Information Security Incident Reports with the State's Office of Information Security and Privacy Protection as well as the California Highway Patrol Emergency Notification and Tactical Alert Center. Protect Department 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.

Serve on the Executive Steering Committee for critical interdepartmental Information Technology (IT) projects to ensure the integration of appropriate information security protocols and controls. Coordinate with Division staff to provide for the integrity and security of the Department's information assets and IT facilities, software, and equipment. Review Feasibility Study Reports to ensure appropriate security protocols are being addressed. Oversee the Department information security awareness program.

25% (E) Direct the Information Privacy Program

Develop 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. Conduct 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.). Review and approve all privacy considerations for the automated and manual environment containing confidential or sensitive data. Oversee, direct, and ensure delivery of annual privacy education and awareness training to all Department staff to be compliant with Department policies. Respond to inquiries from consumers and licensees related to the Department's Privacy Policy.

15% (E) Oversees Operational Recovery Plan

Establish policies and procedures and coordinate with Division staff maintaining cost-effective risk management processes intended to preserve the Department's ability to meet State program objectives in the event of the unavailability, loss, or misuse of information assets. Ensure the recoverability of Department systems and assets by overseeing the development, implementation, testing, and maintenance of the Department's Operational Recovery Plan to assure continuity of computing operations in support of critical applications during a man-made or natural disaster. Establish and maintain processes that analyze the security risks associated with Department information assets.

15% (E) Department Representation

Serve 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. Meet and confer with high-level information security personnel from other state departments, governmental officials, and private sector businesses regarding matters affecting security policy and procedures.

5% (E) Analyzes Legislation

Analyze legislation and Federal and State mandates for their effect on Department security policies.

5% (E) Professional Development

Participate in professional development training, as well as tasks, meetings, and activities that support programmatic and workplace diversity, equity, and inclusion

B. Headquarters Designation

Department Headquarters Office, Rancho Cordova, CA 95670

C. Supervision Received

The incumbent will receive assignments and directions from the CEA B; however, assignments and directions may come from the Chief Deputy Director, and/or Director

D. Supervision Exercised

The incumbent will directly supervise IT Specialists.

E. Administrative Responsibility

The incumbent has complete responsibility for managing the Office and staff.

F. Personal Contacts

The incumbent has contact with all levels of Department staff, consultants, vendors, California Department of Technology staff, Control Agency staff, and other government agencies. Contacts may be initiated with other departments, governmental agencies, and private companies concerning information system and data center technologies as they relate to the performance of this position.

G. Actions and Consequences

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

H. Functional Requirements

The incumbent is a Work Week Group E employee and is expected to work an average of 40 hours per week, Monday through Friday, 8:00AM-5:00PM; however, may be required to work specified hours based on the business needs of the Division and/or the Department. 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 the Department's statewide field sites as scheduled in advance.

I. Other Information

The incumbent shall possess the general qualifications, as described in California Code of Regulations Title 2, Section 172, which include integrity, honesty, dependability, thoroughness, accuracy, good judgment, initiative, resourcefulness, and the ability to work cooperatively with others. The incumbent will maintain consistent and regular attendance, communicate effectively (both orally and in writing) when dealing with the general public and/or other employees, develop and maintain knowledge and skill related to specific tasks, methodologies, materials, tools, and equipment, and adhere to departmental policies and procedures.

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, the incumbent must have the ability to communicate and resolve business related issues/problems that require a technology solution. The incumbent must be able to develop and evaluate alternatives as well as research and present ideas and information effectively orally and in writing. The 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 while maintaining flexibility. The incumbent shall operate to protect the cyber security of individual departmental staff, the Department's network and infrastructure, and all data assets.

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 8/2026