DUTY STATEMENT

Department of Finance
Human Resources Office

The Department of Finance's mission is to serve as the Governor's chief fiscal policy advisor and to promote long-term economic sustainability and responsible resource allocation.

NAME		**EFFECTIVE DATE**	MM DD, 2024
UNIT	Information Services	**POSITION NUMBER**	300-XXX-1405-XXX
CLASSIFICATION	Information Technology Manager I		

SCOPE

Under the general direction of the Chief Information Officer (CIO), the Incumbent is designated as Finance's Information Security Officer (ISO) and functions as the Privacy Officer. This is the managerial level, which may manage the work of lower-level information technology and support staff and may manage work in any domain or combination of domains thereof.

The ISO has significant responsibilities for formulating or administering organizational information technology policies and programs for planning, organizing, and directing the work of one or more information technology programs; provides input and participates in the planning, developing, and managing efforts of Information Security Incident responsibilities; oversees data privacy practices; develops and implements policies and operational standards addressing Information security; analyzes security-related budget change proposals for the Information Technology Consulting Unit (ITCU); provides advice and technical assistance to management on information security-related issues; co-leads projects to determine the potential risk of exposure of all information assets; serves as a consultant on the implementation of laws, policies and standards regarding current information security and relevant privacy laws and regulations; serves as the liaison to all control agencies in communicating the Department's security policies, incident responses and action plans; and ensures all Government Code and State Administrative Manual (SAM) requirements are met.

The ISO investigates, resolves, and reports through appropriate channels all information security incidents; monitors vulnerabilities, threats and incidents; performs departmental risk assessments; conducts and documents information security awareness and privacy training for all employees on an annual basis and consults with the Enterprise Architecture/Client Services unit on IT-related security issues.

ESSENTIAL FUNCTIONS

The incumbent Is required to have knowledge of principles of data processing systems design; exercise initiative, independence of action and originality; demonstrate tact, and exercise sound judgment that recognizes the best Interests of the State and Department of Finance; work under pressure to meet deadlines; communicate effectively; develop and maintain effective and cooperative working relationships; easily adapt to changing priorities; demonstrate an understanding of enterprise security-related policy, procedures, standards and guidelines, and their effect on the business environment; and maintain consistent, predictable attendance In the performance of these specific functions:

	SPECIFIC DUTIES:
30%	**Information Security Program and Policy Management:** • Develop, implement, and maintain all necessary security policies, standards and procedures required for a comprehensive Information Security Program in compliance with SAM 5300 (Information Security), SIMM 5300 (Information Security), Cal-Secure and Finance's Administrative Policy Manual (APM). • Ensure security and privacy policies and procedures, provide operational guidelines to ensure the confidentiality, integrity and availability of information assets. • Manage the design, development, implementation and operation of the information security and privacy program for the collection, use, storage and destruction of information assets. • Provide security and privacy awareness training to all employees with attention to relevant departmental and statewide security policies, regulations, and practices. • Conduct periodic email phishing exercises. • Disseminate quarterly security awareness notices to departmental employees. • Ensure all departmental employees participate in the required training and adhere to established policies and procedures. • Monitor the implementation and compliance of State information security policies and coordinate annual compliance reporting with control agencies. • Represent the department on security policy and standards workgroups and at statewide meetings. • Serve as departmental representative at technology forums and conferences.

20%	**Compliance, Governance and Risk Management:** • Conduct ongoing risk assessments to identify potential vulnerabilities of all system applications and business processes that could threaten the security, confidentiality and integrity of departmental information assets and privacy data. • Identify, evaluate, and mitigate cybersecurity and privacy risks. Ensure regular third-party security assessments and audits are conducted through the California Department of Technology (CDT) and California Military Department. • Assess the probable loss or consequences of identified threats and assess the likelihood of such occurrences. • Identify and estimate the cost of protective measures which would eliminate or reduce vulnerabilities to an acceptable level. • Select cost effective security management measures to mitigate security threats. • Review the security components of the Project Approval Life Cycle (PAL) containing an information technology component. • Assist in the preparation of the security plan. • Verify the security requirements identified in the PAL or other more detailed system requirements documents that have been met during user acceptance testing for new applications. • Prepare confidential reports to appropriate management and control agencies documenting identified risks and propose security management measures and resources necessary for security management and residual risks.
20%	**Security Incident Management:** • Develop and implement policies and procedures for monitoring and reporting incidents involving intentional, unintentional or unauthorized access, disclosure, use, modification, or destruction of information assets. • Develop and manage the Department's cybersecurity incident response plans. • Direct regular tabletop exercises to ensure organization cybersecurity incident response readiness. • Ensure tabletop lessons learned, and findings are addressed and remediated. • Oversee efforts in cybersecurity incident investigation, digital forensics and system recovery. • Ensure digital forensics capabilities are legally defensible preservation of data adhering to industry standard digital forensics best practices. • Serve as the Department's "person most qualified" in legal depositions and testimony to describe and defend digital forensics preservation of evidence and digital forensic investigations and findings. • Report security incidents to executives, California Information Security Office (CISO); California Highway Patrol (CHP), and Emergency Notification and Tactical Alert Center (ENTAC) per SIMM 5340-A. • Conduct post-incident reviews, develop action plans to reduce further exposure, and evaluate and report on trends and weaknesses in the security program.

15%	**Strategic Planning and Security Architecture:** • Collaborate with the State CISO to ensure alignment with statewide information security initiatives. • Lead and participate in security planning sessions; collaborate with the Stale CISO and Finance's CIO to manage the design and implementation of technical controls or threat counter measures of projects, systems, and applications. • Conduct maturity assessment to identify gaps and research and develop alternatives for investment recommendations to improve departmental security in system and technical architecture and business processes. • Provide input regarding the implementation of new security controls to more effectively monitor the department's enterprise network infrastructure. • Provide input regarding the change management process to ensure that all changes to the enterprise systems or services are conducted in a controlled manner and properly documented. • Provide input to the CIO on updates and changes to the Department's Administrative Policy Manual regarding security and privacy policies; partner with the Information Services unit to conduct vulnerability testing of the Department's network, hardware, software, and servers.
10%	**Security and Privacy Policy Review, Development, and Training:** • Analyze Information Technology Consulting Unit (ITCU) budget change proposals that have security related components and make recommendations. • Develop, review, and implement statewide and departmental security and privacy policies. • Create and disseminate departmental security bulletins to all staff. • Develop CDT approved phishing security campaigns and training for departmental staff using the KnowB4 Phishing Scam and Training Tool, and KnowBe4 PhishER. • Review, update, and disseminate the department's Technology Recovery Plan (TRP) to key stakeholders and privacy policy laws and regulations for training awareness.
5%	**Administrative Duties:** • As needed and when appropriate, and requested by Finance's CIO, Enterprise Architect, and Information Security Governance Committee; research and evaluate current and new information security technology and trends to develop departmental information security architecture roadmap. • Review and prepare written analysis on draft IT policies, standards, plans, reports, budget change proposals, and legislative bills which contain a security component for departmental or statewide security implications. • Provide regular reports on the status and posture of information security and privacy within the department to executive management, the Finance Director's Office, and State oversight agencies including the CDT.

SPECIAL REQUIREMENTS

- Willingness and ability to accept increasing responsibility.
- Stays abreast of theoretical developments and analytical techniques and updates.
- Provides consultative advice to the Department's administration, state and local government agencies.
- Works with private agencies as requested through telephone conversations, virtual conversations, written reports, or oral presentations on a wide variety of information technology issues
- Confers with executive management as needed.

KNOWLEDGE, SKILLS, AND ABILITIES

The incumbent is required to possess all knowledge and abilities of the Information Technology Specialist II and Information Technology Supervisor II classifications and the following knowledge:

- A manager's responsibility for promoting equal opportunity in hiring and employee development and promotion and maintaining a work environment which is free of discrimination and harassment.
- The department's Equal Employment Opportunity objectives.
- A manager's role in Equal Employment Opportunity and the processes available to meet equal employment objectives.

SIGNATURES

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 assigned HR analyst.) I also acknowledge, under certain circumstances, I may be required to physically come into the office at any time within a reasonable amount of time.

EMPLOYEE SIGNATURE		**DATE**	

I certify this duty statement represents a current and accurate description of the essential functions of this position. I have discussed the duties of this position and have provided a copy of this duty statement to the employee named above.

SUPERVISOR NAME			
SUPERVISOR SIGNATURE		**DATE**	
PROGRAM BUDGET MANAGER (PBM) NAME			
PBM SIGNATURE		**DATE**	