DUTY STATEMENT

Employee Name: Vacant	Current Date: 02/03/2025
Classification: Information Technology Manager II	Position #: 637-860-1406-XXX
Division/Office: Office of Information Systems	CBID: M01
Section: Security Operations Center	
Supervisor Name: Kim Vu	Supervisor Classification: Career Executive Assignment

I certify that this duty statement represents an accurate description of the essential functions of this position.	
Supervisor:	Date:

I have read this duty statement and agree that it represents the duties I am assigned.	
Employee:	Date:

SPECIAL REQUIREMENTS OF POSITION (IF ANY):

☒ Designated under Conflict of Interest Code.
☐ Duties performed may require pre-employment physical.
☐ Duties performed may require drug testing.
☐ Duties require participation in the DMV Pull Notice Program.
☐ Requires the utilization of a 32-pound self-contained breathing apparatus.
☐ Operates heavy motorized vehicles.
☐ Requires repetitive movement of heavy objects.
☐ Works at elevated heights or near fast moving machinery or traffic.
☐ Performs other duties requiring high physical demand. (Explain below):
☐ Duties require use of hearing protection and annual hearing examinations.

SUPERVISION EXERCISED

☐ None	☐ Lead Person
☒ Supervisor	☐ Team Leader

FOR SUPERVISORY POSITIONS ONLY: Indicate the number of positions by classification that this position DIRECTLY supervises:

1 Information Technology Supervisor II
1 Information Technology Specialist III

Total number of positions in Section/Branch/Office for which this position is responsible: 9

FOR LEADPERSONS OR TEAM LEADERS ONLY:

Indicate the number of positions by classification that this position LEADS:

MISSION OF SECTION:
The mission of the California Air Resources Board's (CARB) Office of Information Services (OIS) is to be a cohesive, proactive, and disciplined team that delivers innovative technology solutions while demonstrating a strong customer-oriented mindset and unleashing the power of data. Our vision is to be a trusted advisor, strategic resource and partner in CARB's innovation, growth and secure use of data.

The OIS Information Technology Security Office (ITSOC) is responsible for managing and reporting security incidents; developing and maintaining information security and privacy plans, policies, processes, procedures and standards; developing CARB's technology recovery plan (TRP); risk management; security training and awareness; information security operations; and providing information security consulting services for implementing new information technology products, projects, and systems.

CONCEPT OF POSITION:
Under administrative direction of the Chief Information Officer (CIO), the Information Technology Manager II (ITM II), also known as the Information Security Officer (ISO), will head ITSOC and is responsible for developing, implementing, and maintaining a comprehensive information security program that includes policies, standards, procedures, and guidelines to protect the organization's information assets. The ISO will establish and maintain an information security program that is consistent with government and industry best practices and applicable regulations. The ISO will be the single point of contact for all security-related matters, security reporting, and security-related executive summaries to CARB's CIO and the Executive Office. The ISO works collaboratively with other Divisions within the CARB, and external partners, such as MS-ISAC, CDT, CAL OES, CISA, and California EPA, to ensure the organization's information assets' confidentiality, integrity, and availability.

The ITM II participates in executive-level decisions and execution of strategies to achieve the objectives and overall IT Strategic Plan for OIS. The ITM II must provide in-depth knowledge and guidance of IT Service Management (ITSM/ITIL) strategies, process, policies, project management, budget management, and best practices, and demonstrates customer centricity.

The ITM II conducts business activities in a professional manner that leads to superior customer satisfaction and delivers services that meet or exceed the customers' expectations. Further, the ITM II must communicate effectively, be well-organized, and be able to track and complete multiple assignments concurrently, while establishing and maintaining professional relationships with internal/external customers, including management, executives, CARB end users, peers, vendors, other government entities, etc.

The ITM II must maintain confidentiality while handling and processing any confidential personnel/business data.

INFORMATION TECHNOLOGY DOMAINS:
☐ Business Technology Management
☒ Information Security Engineering
☒ IT Project Management
☒ Software Engineering
☐ Client Services
☒ System Engineering

% OF TIME	RESPONSIBILITIES OF POSITION
25%-E	**Security Operations and Program Management** Directs, plans, organizes, and controls the Department's implementation of the information security program including practices and procedures required by the California Technology Agency's Office of Information Security (OIS), National Institute of Standards and Technology (NIST), and System Administration Networking and Security (SANS) to ensure that all deployments, enhancements, operations, and maintenance of CARB's network systems are documented and in compliance with control agency security standards. Protects CARB's information and information processing assets by ensuring that CARB is in compliance with all applicable legal, statutory, and regulatory requirements concerning information security management and best business practices. These activities include but are not limited to: coordination with the Technology Recovery Coordinator in the preparation of disaster and technology recovery plans; investigating, resolving, and reporting information security incidents; ensuring compliance with telework and remote access security standards and social media standards; developing security management plans consistent with State Administrative Manual (SAM) Chapter 5300; and ensuring IT security certifications are submitted according to control agency requirements. This work includes submitting certain security documents, including disaster recovery plans and incident reports, to the California Technology Agency and the California Highway Patrol on an annual basis and during security incidents. Directs the reporting of security metrics using methodologies developed by the State OIS. Participates in activities coordinated by the State OIS in order to better understand and address security incidents and critical cyber security threats to the State. Has full management responsibility for the IT Security Office functions. The incumbent is responsible for the planning, directing, organizing, and controlling of work activities related to ITSOC, including but not limited to: Risk Management; Information Security Governance; Incident Management; Security Awareness Program; Privacy; Oversight of Continuity of Operations and Continuity of Government Program (COOP/COG) Plans; and Security Audit and Compliance. Has full responsibility of CARB's shared information security technologies that includes but not limited to firewalls, intrusion prevention systems, advanced persistent threat systems, and web application firewalls. The incumbent will act as the Project Sponsor for the Zero Trust Architecture Project and program. This long-term project and program will bring CARB into compliance with Zero Trust Architecture requirements. Will develop, evaluate, and approve requirements,

	vendors, and solutions that will meet final requirements and will oversee contracted project staff. Once the project is implemented, the incumbent will manage the continued upkeep and compliance required as part of this program, and oversee any contracted staff required to maintain the program. Coordinate internal and external audits and assessments to evaluate the effectiveness of security controls and identify areas of improvement. Collaborate with legal, risk management, and incident response teams to respond to security incidents and breach notifications as relevant regulations requirements. Implementing an effective process for the report of security incidents. Monitor changes in the regulatory environment and update security policies and procedures accordingly. Provides technical consultation on all IT security-related issues and maintains technical expertise on emerging IT trends and strategic IT direction and their implications for information security. Researches, identifies and verifies new security threats and vulnerabilities and corresponding leading-edge, innovative best practices and technologies for defensive and preventive measures. Responds to written and verbal inquiries from ARB executives, managers, and internal or external parties on management issues pertaining to security, privacy, disclosure or resolution. Participates in project meetings and consults technical and business teams on information security best practices and technical architectures. Reviews project plans, feasibility studies, requirements specifications, and technical documents for information security issues, risks, and implications. Recommends security technologies and provides guidance to technical staff responsible for implementing these technologies in CARB's business applications and computing infrastructure, including network, hardware, software, internet and intranet connectivity, desktop and laptop configurations, server configurations, and physical asset security. Consults on cloud security settings for Azure, AWS, Salesforce, and OCI cloud environments. Reviews a variety of documents including, but not limited to, legislation, IT project initiatives, review and approval of FSRs, SPRs, PIERs, procurements for IT goods, and IT contracts to ensure the safeguarding of data and to reduce security risks on behalf of CARB. Provide technical IT support to CARB managers or designees regarding the Cal/EPA Network Computer Center. These activities include, but are not limited to, server and network performance, capacity planning, configuration management, change management, and information security. Ensures that Enterprise systems incorporate privacy principles and requirements in accordance with state and Federal mandates. Identifies privacy weaknesses and proposes solutions to appropriate legal, project, IT or program management. As a lead member of the CARB’s security incident response team, handles privacy incidents, manages the incident response, documents lessons learned, and identifies needed improvements in the design, implementation, and operation of CARB’s privacy program. Consults with the CIO on policies and procedures that pertain to the protection of all IT resources and information from unauthorized use, access, modification, loss or destruction, or disclosure to protect the confidentiality and security of information assets. Develops and delivers reports and presentations to executive management within CARB, providing guidance and recommendations with regard to applying privacy policies and guidelines.

20%-E	**Information Security Strategy and Governance:** Provides consultation and recommendations to resolve the most complex information and physical security issues. Directs the implementation of new security controls to be able to more effectively monitor CARB's IT infrastructure and information systems for inappropriate use or unauthorized activity. Demonstrates a broad understanding of enterprise policy, procedures, standards, and guidelines and their effect on the business environment and criticality to CARB's mission. Collaborates with the State CISO to ensure alignment with statewide information security initiatives, leads and participates in security planning sessions. Researches and evaluates current and new security technology and trends to develop an information security architectural roadmap. Conducts maturity assessments to identify gaps and develop alternatives for investment recommendations to improve CARB's security posture in workforce qualifications, system and technical architecture, and business processes. This work may involve comparing baseline information in certain subject areas such as technology, system users, or IT processes, against control agency requirements as mandated by State OIS, CalEPA AISO, SANS, NIST, and any other information security organizations. Establish and maintain a governance framework to consistently apply security policies and procedures throughout the organization. Establish and maintain security incident response to ensure the organization can respond to and recover from security incidents. This involves creating guidelines and standards that define how information should be protected, specifying acceptable use of technology resources, and outlining incident response protocols. Promote a security-conscious culture throughout the organization by raising awareness of security threats and best practices. Directs the education/training of CARB employees on their security and privacy protection responsibilities. Directs system administrators and application developers to develop installation and deployment plans for all software and hardware. This includes directing system administrators to ensure that critical patches are deployed in an acceptable time frame to avoid a security vulnerability. Directs staff in performing informal and formal security reviews, assessments and audits for CARB's local area network and wide area network (LAN/WAN) environments, as well as, other contract and regional partner networks and systems. Conducts and documents information security awareness training for all Departmental employees on an annual basis. Directs, prepares, and provides oversight and delivery of training, presentations, and briefings for Executive staff and various discrete audiences and venues on information security issues.
20%-E	**Risk Management** Develops, implements, and manages risk management plans consistent with State Administrative Manual (SAM) Chapter 5300, including but not limited to risk management, audit and compliance, information security governance, incident management program, and continuity of operations and government programs. Manages information security vulnerabilities within CARB's information processing infrastructure. Information security vulnerabilities could be discovered in CARB's IT applications, operating systems, and networks, potentially exposing sensitive information. Directs advanced oversight, system guidance, and technical security support for all enterprise infrastructure that supports business functions. This work includes directing the analysis of new releases of OS software to ensure they meet established baseline standards set forth by CARB, CalEPA,

	State OIS, SANS, and other recognized security organizations. Directs, monitors, and reviews central anti-virus reporting and virus incidents, as needed, to troubleshoot and refer actions associated with inappropriate use of computing systems and improving anti-virus mitigation and protections. Directs monitoring of CARB's network traffic on a regular and periodic investigative basis, including monitoring and analyzing web reporting systems for security threats, including unauthorized access and employee inappropriate activity. Responsible for intrusion detection and prevention system (IDPS) traffic for anomalies and responds to alerts including conducting ad-hoc computer security incident reviews and computer vulnerability assessments for the identification and detection of high-risk and/or suspect activities and/or vulnerabilities (i.e., potential of resident malware; un-patched desktop computers and servers). Directs and performs vulnerability assessments of new and existing systems to ensure vulnerabilities and deficiencies are remediated. The incumbent will serve as the backup lead for CARB in the CDT Artificial Intelligence Community. The incumbent will evaluate risk and threat levels to CARB on various requests for systems impacted by AI or derived from AI. The incumbent will guide standards and a framework on AI's responsible, secure, and ethical use at CARB in partnership with the AI Lead, OIS Chiefs of System Development & Support, Project Management, and Data Management (aka Science & Technology), Legal, and the Executive Office. The incumbent is responsible for evaluating and identifying vulnerabilities, risk, and threat levels to CARB's cloud infrastructure and cloud-based systems.
20%-E	**Managerial Duties:** Plans, organizes, directs, and provides managerial review of the work performed in the ITSOC. Provides regular and timely written performance appraisals to staff. Counsels staff and initiates disciplinary actions, as necessary. Recruits, hires, trains, develops and provides leadership to staff. Identifies appropriate long-range plans and goals to address succession planning and knowledge transfer. Manages and coordinates assignments of technical staff based on departmental priorities, staff experience and skill levels, complexity assessments of projects, specialized skills and experience requirements, and resource availability. Develops long and short-term staffing plans that meet workload needs within budgeted resources. Establishes performance standards and expectations by conducting probationary reviews, annual performance reviews, annual Individual Development Plans, constructive intervention, corrective and disciplinary actions, and training to enhance personnel growth. Establishes reasonable deadlines and monitors staff's workload to ensure work is completed accurately and timely. Provides advice and consultation to staff on the most difficult and sensitive work issues. Encourages team building across all service delivery teams. Facilitates cross-training and promotes continuous improvement of processes. Implements motivation techniques, promotes training, and creates a positive climate for change. Mentors staff and ensures training opportunities are available to assist in developing technically skilled staff. Sets and communicates standards of performance for all team members. Performs the full range of supervisory and management duties, including, but not limited to: interpret and adhere to state and federal laws, rules, regulations, bargaining unit contracts and policies in all personnel practices, including, but not limited to hiring, employee development, and management; provide direction and guidance regarding work assignments and daily work activities to ensure timely completion of assignments; review work and evaluate the performance of staff by providing regular feedback and completing

	timely probationary reports, annual performance appraisals, and individual development plans; monitor employee performance and, if necessary, utilize progressive discipline principles and procedures; complete personnel documentation and utilize competitive hiring process; approve or deny administrative requests including leave, overtime, travel, and training; adheres to Department policies, rules, and procedures; accurately submits and approves timesheets by the due date. In addition to the above duties: • Responsible for forming and documenting all IT metrics, goals, procedures, processes, and governance related to the domains in ITSOC. • Ensure cost-effective use of resources, and identify operational cost savings related to IT Security throughout the Department. • Collaborate with a variety of OIS managers/staff, CARB Executive Officers, program staff, and external control agencies (such as CalEPA, CDT, DGS, and DOF) in the analysis and decision-making on a variety of IT ideologies. Reports regularly to the CIO, Division Chiefs, Assistant Division Chiefs, and Executives on progress made with various IT security initiatives on a regular basis. • Oversees ITSOC's development of Requests for Proposals (RFPs), Requests for Offers (RFOs), Budget Change Proposals (BCPs), and/or IT Acquisitions in support of IT security, services, and/or systems. • Works on Legislative analysis for proposed law changes that may affect OIS from a risk, security, resource, and/or cost perspective. Identifies key elements and manages and presents analysis of security-related legislation affecting OIS. • Coordinates the development of issue papers, analyses, correspondence, and requests for action to the CIO. • Acting CIO in their absence (as needed). • Establishes schedules and priorities for all work efforts to ensure continuity and efficiency of customer services. • Ensures services are compliant with CARB's policies, following all state government codes, rules, and regulations; and, must be able to sustain any type of audits. • Measures and reports on the effectiveness of security services and systems through the use of Service Level Agreements (SLAs), metrics, data, and dashboards. • Manages and maintains compliance with established OIS SLAs • Responsible for participating in and consulting on OIS Change Advisory Board (CAB) meetings/processes and the IT Architecture Board. • Briefs the CIO on incident trends and inquiries. • Lead triage analysis to troubleshoot, assess risk, and resolve elevated incidents. • Establish and manage after-hours support model and processes as needed.
10%-E	**CARB Shared Services** Collaborates with the CIO, CalEPA's Information Security Officer (AISO), and Agency Chief Information Officer (AIO) to ensure alignment with Agency shared services and statewide information security initiatives. Provides input, and as needed, present to the Agency CIO and other technology leaders within the organization for the long-range information systems plans to broaden and strengthen shared services operations. Provides timely and useful management and investments. Ensures CARB's technology architecture and solutions align and integrate with Agency IT shared services. Provides information security updates to CalEPA's AISO for CARB systems to ensure information security policies and standards are being met.
5%-M	**Other:**

	Provide management backup support for other areas within OIS as needed. Complete special projects and other duties as assigned and/or required.
	SPECIAL REQUIREMENTS Occasional after-hour work and travel to various CARB regional offices and locations ay be required (travel not to exceed 5%). All employees are responsible for contributing to an inclusive, safe, and secure work environment that values diverse cultures, perspectives, and experiences, and is free from discrimination. **KNOWLEDGE, SKILLS and ABILITIES:** Knowledge and experience in information technology governance processes and procedures; procurement; contract negotiations; vendor management; and customer relationships management. Knowledge of State IT policies and direction. Strong communication, leadership, interpersonal, and problem-solving skills. Incumbent must have the ability to: • Analyze and Formulate policies, procedures, and practices; • Interface with business, technical, and policy-administrators personnel and management; • Plan, organize, and to provide oversight and leadership to the work of multi-disciplinary professional staff.