|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| State of California  California department of technology **PROPOSED**  Duty Statement  Tech 052 (Rev. 02/2018) | | | | | | **RPA NUMBER (HR Use Only)** | | | |
| **23-120** | | | |
| **ALERT: This form is mandatory for all Requests for Personnel Action (RPA).**  **INSTRUCTIONS:** Before completing this form, read the instructions located on last page. | | | | | | | | | |
| Section A: Position Profile | | | | | | | | | |
| A. Date | | B. appointment effective date | | C. Incumbent Name | | | | | |
| November 28, 2023 | |  | |  | | | | | |
| d. CIVIL SERVICE CLASSIFICATION | | | | e. POSITION WORKING TITLE | | | | | |
| Information Technology Manager I) | | | | Statewide Information Security Policy Program Manager) | | | | | |
| F. Current Position Number | | | | G. proposed Position Number (Last three (3) digits assigned by HR) | | | | | |
| 695-401-1405-007 | | | |  | | | | | |
| H. office / section / unit / physical Location of Position | | | | I. supervisor Name and classification | | | | | |
| CA Department of Technology Office of Information Security/ Security Risk Governance/Policy & Standards Program | | | | Payam Hojjat, Information Technology Manager II ) | | | | | |
| J. Work Days / Work Hours / work shift (day, swing, grave) | | | | K. Position Requires: | fingerprint background check | | | | Yes  No |
| M-F/ 8AM – 5PM (Day) | | | | Driving an Automobile | | | | Yes  No |
| Section B: Position Functions and Duties  **Identify the major functions and associated duties, and the percentage of time spent annually on each (list higher percentages first).** | | | | | | | | | |
|  | **Information Technology Domains (Select all domains applicable to the incumbent’s duties/tasks.)** | | | | | | | | |
| Business Technology Management  Information Security Engineering | | | IT Project Management  Software Engineering | | | Client Services  System Engineering | | |
|  | Organizational Setting and Major Functions | | | | | | | | |
|  | Under the general direction of the Office of Information Security (OIS), Security Risk Governance, (SRG) Manager, the Information Technology Manager I (IT Mgr I) will manage the Statewide Policy Program team to update the State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) section 5300 policies to align to the National Institute of Standards and Technology (NIST) to meet the Assembly Bill (AB) 581 Legislative mandate. As the Subject Matter Expert (SME), the SME will assist in the statewide security solution for compliance per the updated SAM and SIMM sections. The incumbent will develop training materials and perform knowledge transfer to OIS staff, departmental executives, managers, and Career Executive Assignment (CEA) staff. | | | | | | | | |
|  | Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.) | | | | | | | | |
| % of time performing duties  45%  % of time performing duties  25%  15%  10% | **Development of Statewide Policy**:   * Developing and Updating SAM and SIMM policies to align with:   + CalSecure   + New and Existing Legislation   + Cybersecurity Frameworks for best practices. * Providing oversight and complete management of the lifecycle of statewide policies from development to publication of SAM and SIMM. * Providing oversight of compliance processes to ensure that we are meeting the new updated SAM and SIMM policies. * Updating State policy annually. * Ensuring compliance of state entities to SAM and SIMM. * Providing expertise in risk and security program management disciplines and processes, at the same time mentoring state staff according to industry best practices. * Develop and implement training plans for the new SAM and SIMM changes. Provide knowledge transfer/ training of risk management principles to staff, managers, and executives. * Work with a wide variety of teams and stakeholders to develop other wholistic SAM and SIMM statewide policies.   **Information Security Research and Statewide Technical Guidance:**   * Research, evaluate, and test new cyber security technologies. * Research, evaluate, and keep up to date with legislation affecting cybersecurity initiatives. * Develop schedules, project plans, and status reports, including verbal and written presentations; and attend staff meetings, technical training classes, conferences, and seminars, and participate in professional security and privacy organizations. * Assist Agency Information Officers, Department Information Security Officers, and State IT business managers with the development of policies and procedures to ensure the security of the assets and data they manage. * Provide subject matter expert security guidance on the development of procurement and contract policies, including statement of works. * Sit-in as the cyber security subject matter expert on a wide variety of OIS and CDT cyber security initiatives per guidance of the IT Manager II.   Instruction and Training:   * Coordinate and conduct policy management training and promote awareness of sound policy management practices by developing training materials, including presentations, articles, and flyers to promote awareness throughout the state and by conducting outreach, marketing, and surveys. * Instruct and train all employees under their supervision. * Hold meetings with external stakeholders reviewing and updating new legislation and policies coming down the pipeline.   **Supervise Statewide Policy & Standards ProgramTeam and perform day-to-day management activities.**   * Develop plans to accomplish Statewide Policy Program initiatives, goals and objectives in accordance with organizational mission and strategic goal; support and advocate management’s philosophy, policies, and procedures; * Evaluate staff on completion of their responsibilities; develop and update duty statements as needed, establish performance expectations, complete individual development plans annually, complete probationary reports on a timely basis, and other performance management activities including adherence to the State’s progressive discipline policy including taking corrective or disciplinary action as necessary; * Responsible for making informed and defensible administrative and personnel management decisions in accordance with department and state policies, personnel-related laws, rules, established OIS administrative processes and procedures and collective bargaining agreements; * Ensure staff comply with all OIS policies, office standard operating procedures, and protocols; * Encourage unit team building, facilitate cross training and promote continuous improvement of processes. Implement motivation techniques, promote training, and create a positive climate for change; and * Foster methods of creative decision-making and problem solving and provide continuous feedback to managers. | | | | | | | | |
|  | Marginal Functions | | | | | | | | |
| 5% | * Develop statements of work and manage contractors. * Provide general security guidance to state entities. * Manage the security mailbox. * Help drive various OIS security related initiatives. | | | | | | | | |
|  | Work Environment Requirements | | | | | | | | |
|  | * Work is conducted in a professional office environment. Business dress, according to current office policy, is required. This position requires the ability to effectively handle stress while working under pressure to meet deadlines, use of a computer to communicate and prepare written materials, and the ability to travel to meetings and conferences at various locations; and * Must pass a fingerprint background check completed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI), and obtain Secret- level Clearance.   May be eligible for telework and when permitted incumbent is:   * Required to adhere to CDT Telework and Hybrid Policy. * Required to support a work from home environment. * Expected to maintain a secure workspace within their home and support necessary logistical requirements to support remote video conferencing and remote work. * Maintain a secure work from home environment for all work materials to ensure they are not misused, lost, damaged, stolen or improperly disclosed. | | | | | | | | |
|  | Allocation Factors (Complete each of the following factors.) | | | | | | | | |
|  | **Supervision Received:**  The IT Manager I receives general direction and supervision from the IT Manager II.  **Actions and Consequences:**  It is critical that the IT Manager I manage the efforts timely to meet the Legislative mandate or CDT will not be in compliant. AB 581 addresses the need to update SAM and SIMM align to the NIST standards so California can be aligned Federally. Failure to update and maintain SAM and SIMM will lead to mistakes pertaining to confidentiality and security of public data would be extremely costly to the Office, from a business, public, and security relations perspective. The consequence of error (lack of appropriate handling and response, policy enforcement, and risk management) results in increased security risk exposure and liability to for the state.  **Personal Contacts:**  The IT Manager I will interact with all levels of staff including state agency and departmental Agency Directors, Agency Information Officers, Chief Information Officers, Information Security Officers, and Privacy and Disaster Recovery Coordinators.  **Administrative and Supervisory Responsibilities:**  The IT Manager I manages all aspects of the Policy & Standards Program team.  **Supervision Exercised:**  The position will directly supervise staff under the OIS Statewide Information Security Policy & Standards Program. The position will serve as a project and program leader over a statewide program, and projects and initiatives with significant statewide impact and lead and direct others on task forces and working groups. | | | | | | | | |
|  | **Other Information** | | | | | | | | |
|  | N/A | | | | | | | | |
|  | **Desirable Qualifications: (List in order of importance.)** | | | | | | | | |
|  | * Possess and maintain one or more of the following professional security industry recognized certifications: Certified Business Continuity Professional (CBCP), Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), or Certified Information Systems Auditor (CISA). * Extensive knowledge of information security policies, standards, principles, practices and frameworks. * Extensive knowledge of the approval process for information technology projects; data processing systems design. * The ability to exercise a high degree of initiative, independence of action, and originality. * Demonstrate professionalism and good independent judgment. * The ability to communicate effectively, both written and verbal. * Ability to develop and maintain effective and cooperative working relationships. * Adapt easily to changing priorities. * Ability to lead a team of employees and/or working groups. * Maintain consistent, predictable attendance in the performance of the essential functions. | | | | | | | | |
| **incumbent Statement: I have discussed the duties of this position with my supervisor and have received a copy of the duty statement.** | | | | | | | | | |
| Incumbent Name (Print) | | | Incumbent Signature | | | | | Date | |
|  | | |  | | | | |  | |
| **Supervisor Statement: I have discussed the duties of this position with the incumbent.** | | | | | | | | | |
| Supervisor Name (Print) | | | Supervisor Signature | | | | | Date | |
| Payam Hojjat | | |  | | | | |  | |