

POSITION DUTY STATEMENT

PM-0924 (REV 7/2014)

| | | |
|--|---|----------------|
| CLASSIFICATION TITLE Systems Software Specialist II (Technical) | OFFICE/BRANCH/SECTION D20/Security & Network Services Division/ISO | |
| WORKING TITLE Systems Security Architect | POSITION NUMBER 900-170-1373-xxx | EFFECTIVE DATE |

As a valued member of the Caltrans team, you make it possible for the Department to provide a safe, sustainable, integrated, and efficient transportation system to enhance California's economy and livability. Caltrans is a performance-driven, transparent, and accountable organization that values its people, resources and partners, and meets new challenges through leadership, innovation and teamwork.

GENERAL STATEMENT:

The security architect designs the structure of security mechanisms, requirements, and standards to protect the Information Technology (IT) infrastructure of the Department from potential hackers, security breaches, and other technological security incidents. Under the general direction of the Assistant Information Security Officer, the Security Architect will perform as the technical advisor for IT security designs and provide technical expertise in the development and implementation of enterprise-wide IT security architectures. This includes providing security standards and procedural guidance in the design of network, system, and application architectures for enterprise projects and initiatives.

The incumbent serves as the lead technical security specialist for staff and management within the Information Security Office. The organization depends on this person's experience with complex technical activities and projects. The incumbent must demonstrate the ability to achieve a common understanding of a security risk or problem and arrive at a satisfactory solution. The incumbent proposes technical solutions within their scope of expertise which take into account technical, departmental, and business needs and compliance controls.

The incumbent performs work requiring extensive probing and analysis to determine the nature and scope of problem situations and work that contributes to the solutions of complex problems, architecture reviews, or strategic and tactical plans. This incumbent collaborates directly with various stakeholders to develop, document, implement and monitor a holistic security architecture.

TYPICAL DUTIES:

| Percentage Essential (E)/Marginal (M) ¹ | Job Description |
|---|---|
| 40% E | <p>Incumbent will perform Security Architecture Development:</p> <ul style="list-style-type: none"> Propose Security Architecture including high-level frameworks, designs, and concepts upon which security architectures can be built and standardized. Evaluate business strategies and requirements supported by the proposed architecture. Provide technical support in the design, development and identification of architectural security guidelines, secure system access strategies, security standards, principles, and procedures. Develop evaluations, studies, and procurement documents utilizing proficiency in technical writing. Plan secure systems by evaluating security technologies and providing lifecycle information security support enterprise-wide. Recommend upgrades to security systems by identifying security gaps and working with the security team to evaluate enhancements. Develop and maintain security standards and processes that maintain compliance with SAM, NIST, FISMA (Federal Information Security Management Act), and FedRAMP. |
| 40% E | <p>Incumbent will perform Security Consultation and Review/Oversight:</p> <ul style="list-style-type: none"> Provide input into and review the design and development of enterprise level application and infrastructure security, security models, and storage methodologies. Consult with various program, business function, and technical staff to assist in the analysis, design, and development of systems to ensure architectural security strategies, requirements, and guidelines are met. This consultation at least includes: reviewing business and IT applications, automation and infrastructure proposals and project deliverables; providing and recommending information security requirements, security safeguards, and controls based on policy and industry best practices; identifying and assessing potential application security risks and vulnerabilities. Actively participate in new information systems project reviews, including participating in reviews of procurement documents and project specifications. Coordinate with and assist IT staff in applying and testing new applications, security systems, |

POSITION DUTY STATEMENT

PM-0924 (REV 7/2014)

| | | |
|-----|---|---|
| | | techniques and tools |
| 10% | E | <ul style="list-style-type: none">• Advising ISO management as appropriate. Incumbent will perform Security Architecture Research: <ul style="list-style-type: none">• Researches security standards and technologies; conducts security and vulnerability analyses; and studies architectures and platforms.• Research available sources to stay current on developing security and comprehensive techniques from both and offensive and defensive perspective.• Track technical advances in security systems and software development models and assessment tools relative to Caltran's complex and diverse IT product environment. |
| 5% | M | Incumbent will perform Security Monitoring: <ul style="list-style-type: none">• Develop security performance metrics and standards.• Collect, analyze, and summarize data to recognize trends and to track metrics. |
| 5% | M | Incumbent will participate in Department Cyber Incident Response Team. |

¹ESSENTIAL FUNCTIONS are the core duties of the position that cannot be reassigned.

MARGINAL FUNCTIONS are the minor tasks of the position that can be assigned to others.

SUPERVISION OR GUIDANCE EXERCISED OVER OTHERS

None. The employee will serve in a lead role, as a subject matter expert, and as a project leader to other staff and consultants assigned to the project under his/her span of control.

KNOWLEDGE, ABILITIES, AND ANALYTICAL REQUIREMENTS

Exceptional knowledge of security concepts, practices, methods, and principals

Global understanding of, and currency with respect to, evolving industry trends, practices, and standards

Ability to effectively apply knowledge and sensitivity to the business perspective of the organization in solving the most complex issues

Understanding of the roles and responsibilities of oversight and regulatory agencies in assuring quality control and system dependability

Must have the ability to network and interface effectively with other technical personnel and the organization's management in securing the support necessary to implement large scale information technology solutions

Ability to prepare clear and concise documentation

Understand the mindset and techniques to compromise systems

Understanding of both offensive and defensive security technology techniques

Knowledge of compliance frameworks such as NIST 800-53, HIPAA, IRS, FedRAMP

Understanding of: California State Administrative Manual (SAM) Sections 5300 - 5399 and security industry standards (e.g., International Organization for Standardization (ISO) 27002, National Institute of Standards and Technology (NIST), etc.).

Ability to train or mentor organization staff and customers in a complex technical area or process.

Knowledge of NIST, FISMA (Federal Information Security Management Act), and FedRAMP

RESPONSIBILITY FOR DECISIONS AND CONSEQUENCES OF ERROR

The Department will depend on the Security Architect's work products to effectively and successfully implement the Departments IT Security and Network Services strategic goals and objectives. Failure to implement these objectives properly will cause the Department of Transportation to be out of compliance with regards to data security.

The incumbent will make recommendations that will impact and affect the operations of the Department and its information technology infrastructure. Recommendations will influence Department policy, information security policy and practices.

PUBLIC AND INTERNAL CONTACTS

The incumbent will routinely be in contact with members of the Department's management, staff, and contractors. The incumbent will be in contact with Federal, State, and Local government agencies, control agencies, and vendors.

POSITION DUTY STATEMENT

PM-0924 (REV 7/2014)

PHYSICAL, MENTAL, AND EMOTIONAL REQUIREMENTS

The incumbent may be required to sit for long periods of time using a keyboard, video display terminal and telephone. Incumbent must be able to travel throughout the State of California by a variety of modes of transportation.

Mental requirements include: openness to change and new information; ability to adapt behavior and work methods in response to new information, changing conditions, or unexpected obstacles. Employee must have the ability to multi-task, to adapt to changes in priorities, and complete tasks or projects with short notice.

Emotional requirements include: ability to value cultural diversity and other individual differences in the workforce; ability to adjust rapidly to new situations warranting attention and resolution; ability to consider and respond appropriately to the needs, feelings, and capabilities of different people in different situations; ability to be tactful and treat others with respect.

WORK ENVIRONMENT

Employee will work in a climate-controlled office under artificial lighting. The incumbent will be required to work for limited amounts of time in high noise level computer rooms with lower than normal temperatures. Employee may also be required to travel to district and outlying offices to conduct analyses and/or training.

I have read, understand and can perform the duties listed above. If you believe you may require accommodation, please discuss this with the hiring supervisor.

I have read, understand and can perform the duties listed above. (If you believe you may require reasonable accommodation, please discuss this with your hiring supervisor. If you are unsure whether you require reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Reasonable Accommodation Coordinator.)

EMPLOYEE (Print)

EMPLOYEE (Signature)

DATE

I have discussed the duties with, and provided a copy of this duty statement to the employee named above.

SUPERVISOR (Print)

SUPERVISOR (Signature)

DATE
