Job Description

Classification: Information Technology Manager I

Position Title: Information Security Architecture and Engineering Manager

Position Number:

Division/Branch: Information Technology Division

Location: Sacramento County

Job Description Summary

Under general direction of the Chief Information Security Officer (CISO), Information Technology Manager I (ITM I), Information Security Architecture and Engineering Manager, provides oversight and is responsible for implementing, maintaining, monitoring, and managing the security of the Information Technology (IT) environment. Recommends, implements, and monitors IT security controls to effectively protect the confidentiality, integrity, and availability of Covered California's information assets and to ensure compliance with applicable federal, state, local, industry, and contractual security requirements. This position serves under the Information Security Engineering domain. Duties may include access to information containing protected enrollee information, including federal tax information, protected health information, and personal identifiable information.

Job Description

25% (E) Security Architecture & Engineering
Supports the CISO in developing and maintaining an Information Security program that addresses best practices, emerging threats, and compliance with applicable laws and regulations to ensure Covered California maintains its Authority to Connect (ATC) issued by the Centers for Medicare & Medicaid Services (CMS). Partners with IT on technical projects and provides information security oversight; reviews system architecture and provides guidance, identifies deficiencies, and makes recommendations to facilitate security by design and adherence to policies, procedures, and standards. Ensures implemented solutions and controls adhere to the security program framework based on CMS MARS-E and Internal Revenue Service (IRS) Publication 1075. Develops baseline security configuration standards for organizational systems and business applications; reviews configurations to ensure systems are consistently deployed based on the required standards. Handles day-to-day implementation, monitoring, and operation of security related hardware, software, applications, managed solutions, and service provider relationships. Leads technical security projects and regularly participates in project and change management meetings. Stays current with new threats; attacker tactics, techniques, and procedures (TTPs); and mitigations. Researches and recommends new security solutions to address emerging threats and to reduce the attack surface. Represents the Information Security Office in a courteous and professional manner; partners and collaborates with IT and other business divisions on technology and risk decisions. Provides excellent internal customer service by monitoring and responding to security service tickets and email.

25% (E) Security Incident Monitoring & Response
Implements, maintains, and monitors security solutions to detect and investigate unusual activity; updates the system configurations and rules based on emerging threats and published indicators of compromise (IOCs).Security solutions include but are not limited to security information and event monitoring (SIEM), intrusion detection and prevention (IDS/IPS), identity threat protection (ITP), endpoint detection and response (EDR), secure web gateway (SWG), data loss prevention (DLP) and file activity monitoring (FAM). Partners with contracted SOC for 24/7 threat monitoring. Creates timely dashboards and reports to convey the status of the security program.

Manages security event investigations and invokes the security incident response team for adverse events that can potentially be escalated to a security incident. Actively participates in the incident response (IR) activities throughout the security incident life cycle, partnering with other IR team members. IR may include involvement outside of regular work hours and responsiveness is expected.

20% (E) Risk Management
Develops and conducts threat modeling processes to analyze the organization's ability to mitigate a cyber-attack across the technology environments. Performs regularly scheduled authenticated internal and external vulnerability scans of the systems and networks; discusses the results with impacted teams ensuring mitigation plans are scheduled and completed. Participates in the development and tracking of measurable benchmarks to demonstrate status of the security program. Interface with internal and external auditors and assessors for testing, audits, and risk assessments. Conducts routine assessments of infrastructure devices (e.g., firewalls), for both on-premise and cloud environments. Participates in third-party risk assessments for identified vendors, software, and solutions.

20%(E) Management
Provides management guidance to staff within the Security Engineering team, ensuring team responsibilities are successfully performed. Maintains a high-performing team through effective recruiting, training, coaching, and mentoring. Measures staff performance with timely delivered performance reviews. Meets regularly with direct reports to discuss individual developmental needs and career aspirations. Assigns work and communicates priorities, monitors progress, seeks priority adjustments, redistributes workload and/or secures extensions as needed to meet established deadlines. Provides regular reports to leadership on status of assignments both verbally and in writing. Prepares and participates in the on-call rotation.

5% (E) Continuous Improvement
Evaluates current processes and makes recommendations to improve efficiencies and finds opportunities to eliminate repetitive and unproductive work. Continually improves knowledge and skills within information security and IT risk management. Sets an annual educational goal to include self-study, training classes, and/or conferences.

5% (M)
Assists with other duties as assigned which may include travel to meetings, training, and seminars.

Scope and Impact
a. Consequences of Error: The incumbent reports to the ITM II and the responsibility for decisions and consequence of error is significant as lack of adherence to department procedures, may result in the increased risk to PI and liability to the state.
b. Administrative Responsibility: This position does not have administrative responsibilities.
c. Supervision Exercised: Responsible for direct supervision of Information Technology Specialists I and Information Technology Specialist II.
d. Internal Personal Contacts: Privacy Officer, and other Covered California employees.
e. External Personal Contacts: CalHEERS, external assessors, vendors, other contractors/consultants.

Physical and Environmental Demands
Work Environment
Work in a climate-controlled office under artificial lighting; exposure to computer screens and other basic office equipment; office space is open and thus noisy; work in a high-pressure fast-paced environment, under time critical deadlines; work long hours; must be flexible to work days/nights, weekends and select holidays as needed; during peak periods, may be required to work overtime; appropriate dress for the office environment.

Essential Physical Characteristics

The physical characteristics described here represent those that must be met by an employee to successfully perform the essential functions of this classification. Reasonable accommodations may be made to enable an individual with a qualified disability to perform the essential functions of the job, on a case-by-case basis. Ability to attend work as scheduled and on a regular basis and be available to work outside the normal workday when required. Continuous: Upward and downward flexion of the neck. Frequent: sitting for long periods of time (up to 70%); repetitive use of hands, forearms, and fingers to operate computers, mouse, and dual computer monitors, printers, and copiers (up to 70%); long periods of time at desk using a keyboard, manual dexterity and sustained periods of mental activity are need; frequent: walking, standing, bending and twisting of neck, bending and twisting of waist, squatting, simple grasping, reaching above and below shoulder level, and lifting and carrying of files, and binders. Note: Some of the above requirements may be accommodated for otherwise qualified individuals requiring and requesting such accommodations.

Working Conditions and Requirements

a. Schedule: Core Business Hours are Monday through Friday, 8:00am - 5:00pm. Flexible with arrival and departure times based on unit schedules.

b. Other: Will require rotating 24x7 on-call support responsibility as well as weekend and holiday support. Incumbent will be required to carry a cell phone.