COVERED CALIFORNIA

Job Description

Classification: Information Technology Specialist II

Position Title: Information Security Engineer II

Position Number: 801-130-1414-001

Division/Branch: Information Technology Division

Location: Sacramento County

Job Description Summary

Under general direction of the Information Technology Manager I (ITM I), the Information Technology Specialist II (ITS II), Information Security Engineer II is responsible for implementing, maintaining, monitoring, and managing the security of the Information Technology (IT) environment. Recommends, designs, 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. Duties may include access to information containing protected enrollee information, including federal tax information, protected health information, and personal identifiable information.

Job Description

35% (E) Security Architecture & Engineering

Develops and maintains procedures that address 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 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.

25% (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.

10% (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: This position generally receives guidance set forth in department policies. This position performs a wide variety of tasks requiring innovative problem-solving where guidance is not readily available. The ITS II is responsible for leading projects and ensuring federal artifacts are reviewed and submitted in a timely manner, participates in all activities related to the development, implementation, architecture, and maintenance of Covered California's security policies, standards, processes, and procedures to ensure adherence to state, federal and industry standards related to Information Security. The consequences of error, including lack of adherence to department procedures, may result in increased risk to PI and liability to the state.
b. Administrative Responsibility: This position does not have administrative responsibility.
c. Supervision Exercised: This position does not exercise supervision; however, acts as a lead.
d. Internal Personal Contacts: Chief Information Security Officer, Chief Information Officer, IT Technical staff, and Covered California leadership.
e. External Personal Contacts: CALHEERS staff, contractors/subcontractors, vendors, state and federal government security staff and the California Highway Patrol.

Physical and Environmental Demands
Work in a climate-controlled, open office environment, under artificial lighting; exposure to computer screens and other basic office equipment; open office environment; 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. Need to be able to lift 35 pounds or more, and have the flexibility to crawl under and behind

computer/network equipment, and must travel to satellite offices and partner department sites throughout California.
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; using headsets to talk with internal and external customers for extended periods (up to 60%); 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.

Working Conditions and Requirements
a. Schedule: Core business hours are Monday through Friday, 8am - 5pm.
b. Travel: Travels statewide to attend meetings and training, and between other Covered California locations up to 5% of the time.
c. Other: May require rotating 24x7 on-call support responsibility as well as weekend and holiday support. Incumbent is required to carry a cell phone.