**Department of Health Care Access and Information**

**Information Services Division**

**Information Security Office**

**Duty Statement**

EMPLOYEE: Vacant

POSITION NUMBER: 441-175-1401-930

TITLE/CLASS: Information Technology Associate

WORKING TITLE: Information Security Analyst

LOCATION: Sacramento

**SECTION A: General Description**

Under general supervision of the Information Technology Supervisor II, the Information Technology Associate (ITA) supports the department Information Security Office (ISO). The Department of Health Care Access (HCAI) and Information (Department) must comply with federal and state security regulations including California State Administration Manual Information Security Sections and compliance with NIST Security requirements.

The ITA will be committed to adopting the best practices of information security industry as promulgated by the private, state and federal entities in order to secure confidential and sensitive information, to counteract hacker attacks, and to protect against malware infection throughout the organization. The mission is to ensure a secure computing environment that will provide availability, confidentiality, and integrity of information for HCAI and the Health Care Payments Data Program (HPD). The ITA works within the ISO unit which is comprised of security analysts and technologists to support the performance of a wide array of security related tasks.

The Information Security Office program elements include the following:

1. Promote awareness through Information Technology (IT) security training / education, and adherence to IT security policies and best practices.
2. Coordinate the IT security incident response team to respond to and resolve incidents.
3. Perform IT security monitoring and event correlation of systems and networks.
4. Perform periodic IT security assessments of systems and network components.
5. Assist customers with IT security related compliance with State and Federal requirements to ensure a secure environment for networks, servers, applications, interfaces and user data requirements.
6. Develop and implement governance and ensure compliance standards are met.

**Supervision Received:** Under general supervision, reports to the Information Technology Supervisor II, Chief Information Security Officer.

**Physical Demands:** Must possess and maintain sufficient strength, agility, endurance, and sensory ability to perform the duties contained in this duty statement with or without reasonable accommodation.

**Typical Working Conditions:** Requires use of computing devices and phones, frequent face-to-face contact with management, staff, consultants and the public, verbal, written and digital (e-mail) communication, extensive review, analysis and preparation of electronic and written documents, assessment of practical demonstrations, mobility to various areas of the Department, occasional travel and overnight stays to training / conferences or the Los Angeles field office may also be required, and work hours may deviate from core business hours based on the service requirements of the Department. Remote work may be assigned as needed and approved.

**SECTION B: Essential Functions**

**30% Monitoring and Analysis**

Perform periodic security analysis of the Information Technology (IT) environment including vulnerability scans on internal and external applications. Coordinate remediation efforts with IT managers and staff. Track security vulnerabilities and assist with the Department’s response to them. Review network and host intrusion prevention systems, anti-malware suite, data loss prevention, and device control appliances. Monitor systems and applications for unauthorized activities. Assist with vulnerability scans in installed hardware and software to detect malicious activity or unapproved configurations. Validate both internal and external information asset vulnerabilities are identified and documented. Monitor alerts from the security event manager and respond based upon approved processes and procedures. Track all changes to Health Payer Data (HPD) program and record changes in the system security plan. Monitor data moving to and from HPD.

**20% Compliance and Audit**

Review policy administration and management for the information security tools suite used to protect the Department network and its assets. Perform routine audits of hardware and software to identify security gaps and risks. Perform audits of HPD account access within HCAI and audits of outside accounts with enclave access. Review and respond to advisory notifications to determine appropriate actions. Report and document findings to report to ISO.

**15% Governance**

Assist with the development and maintenance of security policies, procedures, and standards to ensure compliance with State regulations and security best practices. Participate in formulating IT strategies, while complying with department, agency, and state IT policies. Process and coordinate access control documents and databases for local and remote network accounts, user accounts and access rights to physical and electronic assets. Assist the ISO with the strategic planning of the security program, identifying security goals and objectives consistent with the department’s strategic plan and ensure compliance with State regulations and security best practices.

**10% Training and Awareness**

Assist in the update of the annual Security Awareness Education and Training materials. Keep current with industry security standards, practices, and security methodologies, State guidelines, legislation, policies, and regulations. Monitor completion of security training for existing and new employees. Conduct unannounced phishing training targeting employee groups and roles.

**10% Incident Response**

Participate as an active member of the Cyber Incident Response Team (CIRT) by providing technical assistance and identifying potential remediation procedures. Assist with detection and analysis to understand attack targets and methods and impacts of events. Assist with post-incident reviews and action plans to reduce exposures to similar incidents.

**10% Threat Intel and Research**

Proactively protect Department computing assets by researching emerging threats, reviewing firewall log files, intrusion detection, prevention logs, and system event logs.

**SECTION C: Marginal Functions**

**5%** Perform other related duties as required.

**SECTION D: Other Expectations**

* Demonstrate a commitment to performing duties in a service-oriented manner.
* Demonstrate a commitment to maintaining a work environment free from workplace violence, discrimination, and sexual harassment.
* Demonstrate a commitment to following best practices and applying office-wide standards throughout the organization.
* Demonstrate the ability to establish and maintain priorities, successfully complete work assignments and meet deadlines as required.
* Show initiative in making work improvements, identifying and correcting errors, and initiate work activities.
* Demonstrate the ability to gain and maintain the confidence and cooperation of others.
* Maintain good work habits and adhere to all HCAI policies and procedures.
* Demonstrate a commitment to HCAI’s mission, vision, and goals.
* Demonstrate a commitment to HCAI’s Core Values.

|  |  |  |
| --- | --- | --- |
| **To Be Signed by the Employee and Immediate Supervisor** | | |
| I have read and understand the duties and expectations of this position.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | I have discussed the duties and expectations of this position with the employee.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Employee Signature/Date |  | Supervisor Signature/Date |
|  |  |  |