CCHCS Security Incident Reporting Procedures

1. According to SIMM 5340-A, a security incident is defined as follows:

a. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, procedures, or acceptable use policies.

i. **State Data** (includes electronic, paper, or any other medium).

1. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal.
2. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
3. Deliberate or accidental distribution or release of personal information by a state entity, or its personnel in a manner not in accordance with law or policy.
4. Intentional non compliance by the custodian of information with his/her responsibilities.

ii. **Criminal Activity** Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

1. **Unauthorized Access** This includes actions of state entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. Involving tampering, interference or damage to state data.
2. **Attacks** This includes, but is not limited to, successful virus attacks or exploited vulnerability, web site defacements, and denial of service attacks.

iii. **Equipment** This includes theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.

iv. **Inappropriate Use** This includes the circumventing of information security controls or misuse of a state information asset by state entity personnel and/or any unauthorized individuals for personal gain, or to engage in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal or other inappropriate activity

v. **Outages and Disruptions** This includes any outage or disruption to a state entity's mission critical systems or public-facing web applications lasting more than 2-hours, or in which the incident triggers the state entity's emergency response or technology recovery.

vi. **Any other incidents that violate state entity policy**.

2. If the incident meets the above criteria, the Program Unit must **immediately** take action and follow steps 3 – 5.

3. Complete the CCHCS Information Security Incident Form collecting the details and relevant information as required. "**CCHCS Information Security Incident Form,**"

4. The Program Unit or the person discovering the incident must immediately contact and report the incident to the CCHCS Information Security Office (ISO) using the following steps:

i. Email the ISO directly at CCHCS-ISO@cdcr.ca.gov or call **(916) 691-3243** with preliminary notice and summary of the events ***(e.g.: a description of the sequence of incident events, dates, location of the incident, people affected and full names, any lost data (personal or not,) any lost equipment and type of equipment … etc.)***

ii. **Supervisor or Hiring Authority Role:** In most cases, it is the supervisor or the hiring authority that must complete the Information Security Incident Report since the report involves collecting information on the incident that only supervisors or hiring authorities may be in a position to request from the employee who committed the incident.

iii. **The Local IT Role:** The Local IT is responsible for providing guidance and the technical substance to further enhance the completeness of the report.

iv. **Employee Relations Office:** If the incident involves possible employee disciplinary or internal investigation action, complete the Information Security Incident Report as accurately as possible, and contact the Employee Relations Officer (ERO) (916) 691-5857. The ERO will be responsible to contact the Office of Internal Affairs (OIA) and to coordinate the investigative activities

5. Within three **(3) business days** the Program Unit must complete the "**CCHCS Information Security Incident Form,**" and provide a **signed** copy of this form to the CCHCS ISO. **** Due to Regulatory and Legal obligations, the CCHCS Information Incident Form must be complete, must include ALL the requested information pertaining to the incident and be submitted within the timeframe outlined in this step.***