Information Security **AUDIT AND ACCOUNTABILITY POLICY**	**Issued by (Policy Owner): Chief Information Office, Information Security Office, and the Privacy Office**
Effective Date: May, 2019	**Last Reviewed: January 2022**

State Administrative Manual (SAM) References		National Institute of Standard and Technology (NIST) Cybersecurity Framework (CSF) Function and Category	
5335	Information Security Monitoring	DETECT	Anomalies and Events (DE.AE)
5335.1	Continuous Monitoring		Security Continuous Monitoring (DE.CM)
5335.2	Auditable Events		Detection Processes (DE.DP)

1. Audit and Accountability Policy

1.1. Introduction and Overview

In order to detect and respond to signs of attack, anomalies, and suspicious or inappropriate activities, CDPH requires an event logging and monitoring strategy to continuously monitor access and activities conducted using CDPH information assets.

Information assets owned by CDPH are strategic assets intended for official business use and are entrusted to State personnel and business partners to perform their job-related duties. Since inappropriate or unauthorized access and use of CDPH information assets could result in harm to the State and/or to CDPH, it is important to audit and monitor the system activities with sufficient regularity to detect and respond to signs of attack, anomalies, and suspicious or inappropriate activities in a timely manner.

1.2. Objectives

Objectives for this Audit and Accountability Policy are to:

1.2.1. Define the guidelines for the development and implementation of CDPH event logging and continuous monitoring strategy, and supporting processes to identify and respond to indicators of attack, anomalies, and suspicious or inappropriate activities; and

1.2.2. Establish accountability of users for their actions involving CDPH information assets and provide necessary evidence in the event of a security incident or breach.

2. Scope and Applicability

This policy applies to personnel and entities working at, for, or directly on behalf of CDPH.

3. Policy Directives

3.1. **[SAM 5335.1]:** CDPH information asset owners, in collaboration with information asset custodians and the CDPH Information Security Officer (ISO), shall develop and implement an event logging and continuous monitoring strategy for monitoring of access and activities conducted using CDPH information assets.

3.2. **[NIST 800-53 AU-2, AU-11;45 C.F.R. § 164.308(a)(5)(ii)(c)]:** CDPH systems that process, store and/or protect confidential, sensitive, and/or personal information shall have the capability to create audit logs for a variety of events. At a minimum, the CDPH information system shall be capable of auditing the following events:

3.2.1. Records of successful and rejected system access attempts;

3.2.2. Records of creation, modification and/or deletion of confidential or sensitive information;

3.2.3. Records of successful and rejected data and other resource access attempts;

3.2.4. Records of usage of administrative privileges; and

3.2.5. Other auditable events as required by CDPH.

3.3. **[NIST 800-53 AU-3]:** CDPH information systems shall generate audit logs that record details pertaining to an auditable event such as the description of event, time at which the event occurred, affected systems, and the outcome of the event. Each auditable event shall be associated with the identity of the user that caused the event (user accountability).

3.4. **[NIST 800-53 AU-6; 45 C.F.R.§ 164.308(a)(1)(ii)(D); SHIPM 3.3.1 III. B. (1)-(2)]:** The audit trails (application, system-level and user audit trails) and activity logs shall be reviewed periodically as defined in CDPH event logging and continuous monitoring standard by specified CDPH staff, including security, audit, and system administrators. The findings from review of audit logs shall be reported periodically to the CDPH ISO. The frequency of the review will depend on the risks involved. These risk factors include but are not limited to:

3.4.1. Criticality of the application processes;

3.4.2. Value, sensitivity, or criticality of the information involved;

3.4.3. Past experience of system infiltration and misuse; and

3.4.4. Extent of system interconnection, particularly to public networks.

3.5. **[NIST 800-53 AU-1; 45 C.F.R. § 164.312(b); SHIPM 3.3.1 III. A.]:** CDPH shall implement hardware, software, and/or procedural mechanisms that record, and examine activity in information systems that contain, or use, sensitive, confidential, and/or personal information.

3.6. **[NIST 800-53 AU-7, AU-9, AU-12]:** CDPH information systems shall support on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. Audit logs of system activity are classified as sensitive and should be secured from manipulation to maintain the integrity of the audit log information.

3.7. **[NIST 800-53 AU-8]:** The clocks of relevant information processing systems within CDPH shall be synchronized with an agreed accurate time source to generate time stamps for audit records.

3.8. **[NIST 800-53 AU-4, AU-5]:** CDPH information systems shall have adequate audit record storage capacity and the ability to alert personnel in the event of an audit processing failure.

3.9. **[SHIPM 3.3.1 III. D. 1.]:** Audit of CDPH's information security procedures shall be performed periodically. The security audits shall review systems that provide access to, or the collection or storage of sensitive, confidential, and/or personal information. The audit shall verify that security precautions required by the CDPH ISO as conditions for system approval are implemented and maintained.

3.10. **[SHIPM 3.3.1 III. C.; 45 C.F.R. § 164.308(b)(2) (i)-(ii)]:** CDPH shall retain the audit logs for as long as they are needed for operational, legal, and audit purposes and in adherence with established legal requirements. The Audit log retention period shall be revised regularly to reflect changes in the law and changes in CDPH policies and procedures. CDPH shall retain the policy and procedure documentation related to their technical audit controls, as well as action, activity or assessment for a minimum of six (6) years.

4. Roles and Responsibilities

CDPH Policy Owner

4.1. CDPH Policy Owner is responsible for determining the appropriate audience(s) for this policy.

4.2. CDPH Policy Owner shall create awareness about the policy and educate the identified audience(s) of their individual responsibilities and the associated sanctions.

4.3. CDPH Policy Owner is responsible for the periodic review and update of the policy.

4.4. CDPH Policy Owner is responsible for supporting the periodic auditing and assessment of compliance with the policy.

4.5. CDPH Policy Owner is responsible for seeking guidance from Information Security Officer (ISO), Chief Information Officer (CIO), Privacy Officer and Subject Matter Experts (SMEs) as appropriate to comply with security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs.

4.6. CDPH Policy Owner is responsible for supporting and coordinating the standards, procedures and guideline development activities required to align with the overarching policy.

4.7. CDPH Policy Owner is responsible for including the approved policy into the policy management system and the completeness of relevant metadata fields.

4.8. CDPH Policy Owner is responsible for responding to workflow notifications that may require review, impact analysis, policy changes and policy approval.

4.9. CDPH Policy Owner is responsible for managing the policy throughout its lifecycle from development to decommissioning or archiving.

4.10. CDPH Policy Owner is responsible for communicating key notifications regarding the policy such as decommissioning to linked policies, procedures, standards and guidelines to relevant stakeholders.

4.11. CDPH Policy Owner is responsible for participating in the security variance process and assessing the risks and compliance plan associated with variance requests.

4.12. CDPH Policy Owner supports the development of processes and metrics required to measure the effectiveness of the policy.

CDPH Owners of Information Asset

4.13. CDPH Owners of Information Asset are responsible for the protection of information assets under their purview.

4.14. CDPH Owners of Information Asset are responsible for defining the requirements for audit trails and auditability of events and transactions processed on information assets under their purview.

4.15. CDPH Owners of Information Asset are responsible for determining that the assets are continuously monitored based on the criticality of information assets.

4.16. CDPH Owners of Information Asset are responsible for participating in the development and implementation of the event logging and continuous monitoring strategy.

CDPH Information Security Officer (ISO)

4.17. CDPH Information Security Officer (ISO) is responsible for guiding the development and implementation of the CDPH event logging and continuous monitoring strategy.

Table 1 RACI Matrix

Activity	CIO	CISO	Privacy Team	Policy Owner	CDPH Users
Own Policy	C	Policy Owner	I	A	-
Policy awareness	R	Policy Owner	R	A	I
Develop and maintain Logging and Continuous Monitoring Strategy	C, I	Policy Owner	I	A	I
Report violations	R	Policy Owner	R	R	R
Review /Approve Security Variances	C, I	R	C, I	A	-

R	Responsible
A	Accountable
C	Consult
I	Inform

5. Enforcement

Non-compliance with this policy may result in disciplinary action in compliance with the escalating CDPH disciplinary process up to, and including, termination.

The consequences of CDPH negligence and non-compliance with state laws and policies may include loss of delegated authorities, negative audit findings, monetary penalties and legal actions.

As set forth in Government Code section 11549.3, CDPH shall comply with the information security and privacy policies, standards, procedures, and guidelines issued by the California Office of Information Security. In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the *[OIS]*, CDPH shall comply with security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, Information Security Officer (ISO), and Privacy Program Officer/Coordinator to identify security and privacy requirements applicable to their programs and implementation of the requisite controls.

6. Auditing

6.1. CDPH has the right to audit activities related to the use of State information assets.

7. Reporting

7.1. Violations of this policy shall be reported to the CDPH Information Security Officer.

8. Security Variance Process

8.1. If compliance is not feasible or is technically impossible, or if deviation from this policy is required to support a business function, the respective manager shall formally request a security variance as defined in the CDPH Security Variance policy.

9. Authoritative Sources

9.1 NIST Special Publication (SP) 800-53 Reference

Family	Control
Audit And Accountability (AU)	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12
Physical And Environmental Protection (PE)	PE-2, PE-6, PE-8

9.2 Statewide Health Information Policy Manual (SHIPM) Reference

Reference	Control
Audit Controls	SHIPM 3.3.1

9.3 Statewide Information Management Manual (SIMM) References and Implementation Guidance

Reference	Article
5305-A	Information Security Management Program Standard

10.Related Policies, Procedures and Standards

Reference	Article
Statewide Health Information Policy Manual (SHIPM)	Section: 3.1.2 – Incident Procedures
Statewide Health Information Policy Manual (SHIPM)	Section: 3.3.1 – Audit Controls
Statewide Health Information Policy Manual (SHIPM)	Section: 3.4.1 – Documentation
Statewide Health Information Policy Manual (SHIPM)	Section: 4.1.1 – Policies and Procedures
Statewide Health Information Policy Manual (SHIPM)	Section: 4.1.3 – Sanctions for Violation
CDPH Information Security Policy	Information Classification Policy

11.Revision History

Date	Revision	Description of Change
March, 2018	1.0	Initial Version

12.Definitions of Key Terms

CDPH uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and are on the California Department of Technology website at https://cdt.ca.gov/security/technical-definitions/.

Information Assets	Information Assets include (a) paper and automated information, including (but not limited to) records, files, and databases; and (b) information technology facilities and equipment (including telecommunications networks, personal computer systems, laptops, tablets and mobile devices), and software owned or leased by state entities.
Information Asset Custodian	Personnel or organizational unit (such as a data center or information processing facility) responsible as caretaker for the proper use and protection of information assets on behalf of the information asset

	owner.
Lifecycle	The anticipated length of time that the information technology system or application can be expected to be efficient, cost- effective and continue to meet the agency's programmatic requirements. Synonymous with operational life system.
Owner of Information Assets	An organizational unit having responsibility for making classification, categorization and control decisions regarding information assets.
Personnel	Employees, retired annuitants, student assistants, volunteers, contractors, sub-contractors commissioned, employed by or otherwise engaged in the performance of work associated with administration of a state entity program.
Audit log file retention period	Audit log file retention periods is the length of time a record needs to be maintained to satisfy the purpose for which it was created, and to fulfill operational, legal, fiscal, administrative, and prudent business requirements.
Audit log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit trails	A chronological set of logs and records used to provide evidence of a system's performance or personnel activity that took place on the system and used to detect and identify intruders.
Application audit trails	Application audit trails normally monitor and log user activities in the application. This includes the application data files opened and closed, and the creating, reading, editing, and deleting of applications records associated with health information.
System-level audit trails	System-level audit trails usually capture successful or unsuccessful log-on attempts, log-on ID/username, date and time of each log-on/off attempt, devices used to log-on, and the application the user successfully or unsuccessfully accessed.
User audit trails	User audit trails normally monitor and log user activity in an electronic health information system or application by recording events initiated by the user, such as commands directly initiated by the user, log-on attempts with identification and authentication, and access to electronic health information files and resources.
Integrity	The property that data or information has not been altered or destroyed in an unauthorized manner.

Protected Health Information (PHI)	"Protected Health Information" is defined as Individually Identifiable Health Information that is transmitted electronically, maintained electronically or transmitted or maintained in any other form or medium, concerning any CDPH patient or the patient of any of healthcare provider of CDPH.
Personal Information	The term "personal information" means any information that is maintained by CDPH that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

13. Policy Approval

Position	Name	Signature	Date
Information Security Officer	Charles Lano		