Attachment 6

Auditing and Accountability Policy – ITAM-0612

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	AUDITING AND ACCOUNTABILITY POLICY	ITEM NUMBER:	ITAM-0612
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE **1** OF **7**

I. Purpose

To ensure that County Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors and third parties) whose responsibilities include managing, administering, and operating County networks or systems.

III. Scope

This policy applies to any Information System that electronically generates, receives, stores, processes, or transmits County-owned data, whether the system is hosted on the County network or by a third-party provider. Additionally, these provisions apply to anyone doing business as the County and/or in support of the County that is provisioned access to County Networks or systems. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, collectively referred to hereafter as “agents”.

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

It is the policy of the County Board of Supervisors that:

Audit trails maintain a record of system activity by system or application processes and by user activity and processes. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, means to reconstruct events, detect intrusions, and identify problems. System audit trails, or event logs, provide a record of events in support of activities to monitor and enforce the IT system security policy.

All audit logs are subject to recording and routine review by the CISO, security groups, and auditors for inappropriate or illegal activity. System owners must ensure the protection of system event logs with file-level permissions, separation of duties, and all other safeguards commensurate with the highest level of sensitivity of the information residing on the system for which the logs record data. The following outlines the minimum security control requirements which all County information systems must adhere to in order to operate in a production environment:

1. AUDIT EVENTS

The information systems owners, in cooperation with audits being performed and IT professionals, shall:

a. Determine that the information system is capable of auditing the following events: Log credentials, failures of login's and other 'events' determined by IT and/or the system capable of maintaining log data.

b. Coordinate the security audit function with other organizational entities requiring audit.

c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

d. Determine that the following events are to be audited within the information system:

i. Log credentials, failures of login's and other 'events' determined by IT and/or the system capable of maintaining log data.

2. REVIEWS AND UPDATES

a. The organization shall review and update the audited events as needed by a frequency determined by IT.

3. CONTENT OF AUDIT RECORDS

a. The information system shall generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

4. ADDITIONAL AUDIT INFORMATION

a. The information system shall generate audit records containing the following additional information: Logon data, failures, and other data fields as determined by IT.

5. AUDIT STORAGE CAPACITY

a. The information owner shall ensure audit record storage capacity is allocated in accordance with pre-described by IT requirements based on specific systems.

6. TRANSFER TO ALTERNATE STORAGE

   a. The information system shall off-load audit by IT, when appropriate, onto a different system or media than the system being audited.

7. RESPONSE TO AUDIT PROCESSING FAILURES

   The information system shall:

   a. Alert IT assigned staff in the event of an audit.

   b. Take the following additional actions: IT defined actions will be taken to prevent an event driven processing failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).

8. AUDIT STORAGE CAPACITY

   a. The information system shall provide a warning to IT Staff within enough time to allocate additional storage when audit record storage volume reaches 15% of repository maximum audit record storage capacity (if possible by specific systems).

9. REAL-TIME ALERTS

   a. The information system shall provide an alert as immediate as possible to IT and assigned departmental staff when the following audit failure events occur:

      i. Logon failures, hacking attempts, other cyber attacks.

10. CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

    a. The information system shall enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and apply appropriate action within network traffic above those thresholds.

11. SHUTDOWN ON FAILURE

    a. The information system or IT Staff shall invoke a full system shutdown, partial system shutdown, or degraded operational mode with limited mission/business functionality available or other appropriate responses in the event of audit failure, unless an alternate audit capability exists.

12. AUDIT REVIEW, ANALYSIS, AND REPORTING

    The information system owner shall:

a. Review and analyze information system audit records as determined by IT for indications of inappropriate or unusual activity.

b. Report findings to the CIO or CISO.

13. PROCESS INTEGRATION

a. The information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

14. AUDIT REPOSITORIES

a. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain County-wide situational awareness.

15. AUDIT REDUCTION AND REPORT GENERATION

a. The information system shall provide an audit reduction and report generation capability that:

i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.

ii. Does not alter the original content or time ordering of audit records.

16. AUTOMATIC PROCESSING

a. The information system shall provide the capability to process audit records for events of interest based on IT defined audit fields within audit records.

17. TIME STAMPS

The information system shall:

a. Use internal system clocks to generate time stamps for audit records.

b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets IT defined time periods.

18. SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

The information system shall:

a. Compare the internal information system clocks periodically to ensure all systems are date and time compliant.

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than acceptable best practices, generally within one second.

19. PROTECTION OF AUDIT INFORMATION

a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

20. ACCESS BY SUBSET OF PRIVILEGED USERS

a. The organization shall authorize access to management of audit functionality to only those fields that of non-protected data or information unless viewer already has appropriate access to such data and information.

21. AUDIT RECORD RETENTION

a. The information system owners shall retain audit records for a minimum of three months to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

22. LONG-TERM RETRIEVAL CAPABILITY

a. The information system owners shall employ appropriate policy to ensure that long-term audit records generated by the information system can be retrieved.

23. AUDIT GENERATION

The information system shall:

a. Provide audit record generation capability for the auditable events as defined at the system level of which containing protected or confidential or sensitive technology assets.

b. Allow appropriate IT staff to select which auditable events are to be audited by specific components of the information system.

c. Generate audit records for the events with the content as defined by IT.

24. TIME-CORRELATED AUDIT TRAIL

    a. The information system shall comply with audit records from all systems containing protected or confidential data and information and all sensitive technology assets into a system-wide (logical or physical) audit trail that is time-correlated to within recommended security best practices or as directed by law or organizational agreements.

25. STANDARDIZED FORMATS

    a. The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

26. CHANGES BY AUTHORIZED INDIVIDUALS

    a. The information system shall provide the capability for authorized IT Staff to change the auditing to be performed on systems audited based on industry acceptable best practices available.

VI. Exceptions

See ITAM-0600, IT Security Program

VII. Non-Compliance

See ITAM-0600, IT Security Program

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:
   a. National Institute of Standards and Technology (NIST) Special Publications (SP):
      i. NIST SP 800-53a – Auditing and Accountability (AU)
      ii. NIST SP 800-12
      iii. NIST SP 800-92
      iv. NIST SP 800-100
   b. State of California State Administrative Manual (SAM) 5300 et seq.
   c. Statewide Information Management Manual (SIMM) et seq.

2. Related Policies:

3. Referenced Documents:

4. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021