	COUNTY OF SAN BERNARDINO POLICY	No. 2-365 Effective: January 3, 2006 By: Bea Valdez, Interim Chief of Administrative Services	Issue No. 1 Page 1 of 2
	PUBLIC HEALTH	Approved: James A. Felten Public Health Director	
Subject: AUDIT CONTROLS FOR INFORMATION SYSTEMS			

I. POLICY:

It is the policy of the Department of Public Health (DPH) to audit its information systems to ensure that systems and data are protected from unauthorized access in accordance with San Bernardino County (SBC), DPH, state, and/or or federal requirements.

II. PURPOSE:

The purpose of this policy is to establish the guidelines for the implementation and use of audit controls on all systems (workstations, data systems, etc. – see Policy 2-350, Information Security for system definition) within DPH.

III. GENERAL INFORMATION:

DPH has the authority to conduct security audits on any automated systems available for workforce use. Audits provide indications as to the effectiveness of safeguards. Users should be aware that audit controls are in place and may be reviewed at any time to verify compliance.

Audits will be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources, especially sensitive information.
- Investigate possible security incidents to ensure conformance to security policies.
- Monitor user or system activity where appropriate.
- Verify that software is updated and working correctly.

Information Technology (IT) has the authority to monitor system access and the activity of all DPH workforce members.

IV. PROCEDURES:

A. Systems with sensitive information must have sufficient auditing capabilities to allow examination of system activity. Furthermore, to ensure that access to servers, workstations, and other computer systems is appropriately secured, IT must perform the following measures:

1. Monitor logins for the following purposes:
   a. Multiple attempts
   b. Lockouts
   c. Suspicious patterns, etc.
2. Monitor System Activity
   a. Suspicious activity may be monitored more closely.
   b. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

3. Review System Activity

    a. Each system will be reviewed on a periodic basis to ensure that proper audit controls are in place.

    b. All of the audit mechanisms on each system will be inspected to verify data security and look for any anomalies.

    c. Indications of improper use or suspicious activity will be reported to management for further review or investigation.

4. Audit Tool Security

    - Audit tools and audit information data shall be protected from unauthorized access, modification, and deletion.

V. VIOLATIONS:

Failure to comply with this policy may result in disciplinary action up to and including termination of employment/contract.

VI. REFERENCES:

A. Reference

- Health Insurance Portability and Accountability Act Code of Federal Regulations (CFR) Parts 160 and 164

B. Related Policies

1. 2-350, Information Security
2. 2-352, Security Management and Evaluation