STATE OF VERMONT
Agency of Human Services (AHS)

Audit and Accountability	REVISION HISTORY:	Chapter/Number 5.07
	EFFECTIVE DATE: 10/23/08	Attachments/Related Documents:

Authorizing Signature: Cynthia D. LaWare Date Signed: 10/23/08
Cynthia D. LaWare, Secretary, Agency of Human Services

PURPOSE:
To ensure that AHS IT systems are capable of generating usable audit records for specified events to enable traceability and investigation of security incidents and suspected incidents.

BACKGROUND and REFERENCES:
National Institute of Standards and Technology (NIST) Special Publication 800-53, *Information Security*

NIST Special Publication 800-30, *Risk Management,* (NIST Special Publications available at http://csrc.nist.gov/publications/PubsSPs.html)

DEFINITIONS:
Accountability- the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action (NIST SP 800-30, Revision A, Appendix E)
Audit- a formal (usually independent) review and examination of a project or project activity for assessing compliance with contractual obligations (NIST SP 800-30, Revision A, Appendix E)

Audit Records- logs or electronic record showing who or what has accessed a system and what actions have been performed during a given period of time

Legacy Systems- applications that have exceeded a normal lifecycle and are usually supported by dated technologies.

SCOPE:

This document applies to all Agency Departments, Division and Offices hereafter referred to jointly as "department". This document also applies to contractors, business associates, and other users of departmental information systems.

STANDARDS:
All AHS IT systems, as they are implemented, shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable laws, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically and updated as necessary.

The AHS Office of the CIO and departmental IT Managers shall collaboratively create audit and accountability templates and procedures that reflect levels of data protection and access requirements. Based on the results of this work, the IT Managers and office of the CIO shall submit a plan to meet audit and accountability requirements for their existing information systems. All new systems shall include audit and accountability requirements, templates, and procedures as part of their creation, installation, implementation, or operation (if purchased).

As a result of this policy, procedures shall be documented to establish and maintain the following capabilities:

- Capture specified information in audit records.
- Generate an audit record for specified events to support investigation of security incidents.
- Generate management alerts in the event of an audit that enable timely corrective action.
- Enable review of audit information and the generation of audit reports.
- Regular review and analysis to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity.
- Retain audit records to support investigation of security incidents and meet regulatory and/or AHS requirements.

COMPLIANCE:

It is the responsibility of the individual department's IT Managers to ensure dissemination and review of this policy to all employees within their organizations and other associates as appropriate.

AHS departments with legacy systems or other extenuating circumstances must apply in writing to the AHS CIO for exceptions to this policy and include for each information system a plan and schedule to meet standards.

ENFORCEMENT:

The Office of the Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.