



INFORMATION SECURITY BEST PRACTICE FOR ALL PUBLIC AGENCIES
Date Effective: May 1, 2009

PURPOSE

The purpose of this best practice is to establish a set of statewide recommendations for information security. This best practice is not intended to be a statement of the current ability of public agencies. It is a statement of goals and expectations. The realization of such goals and expectations will result in more effective records management.

SCOPE

This best practice applies to all information created or received by public agencies.

STATEMENT OF AUTHORITY

Pursuant to 1 V.S.A. § 317a, 3 V.S.A. § 117, 3 V.S.A. § 218, 3 V.S.A. § 2222, and 3 V.S.A. § 2283b the Vermont State Archives and Records Administration (Office of the Secretary of State) and the Department of Information and Innovation (Agency of Administration) are authorized to establish and promulgate standards, procedures and techniques for the effective management of public records.

STATEMENT OF BENEFITS

Sound information security practices and procedures result in a number of benefits: reducing unauthorized access or disclosure to information; fulfilling legal mandates relative to confidentiality, authenticity and availability; and improving accountability and public trust.

STATEMENT OF RESPONSIBILITY

Maintaining authentic and trustworthy information over time is a shared responsibility. Establishing and sustaining effective information security practices requires a multidisciplinary approach. Public agencies should make effective use of the necessary range of expertise available throughout the State of Vermont. This includes expertise in archives, records and information management, information technology, business process management, risk management, and law.

CONTACT

Questions about this best practice may be directed to the Chief Information Officer or Vermont State Archivist.



DEFINITIONS

Authenticity: The quality or condition of being authentic, trustworthy, or genuine.

Availability: The accessibility of information in a timely manner.

Categorization: To put into categories; to classify.

Confidentiality: The nondisclosure of certain information except to another authorized person.

Information Security: A process by which a public agency protects and secures the information it acquires or produces in the course of agency business.

Record: Any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of agency business (1 V.S.A. § 317(b)).

Record Schedule: A manual, directive or policy containing descriptions of and instructions for retention, access, management and disposition of records that is approved by the State Archivist pursuant to 1 V.S.A. § 317a and 3 V.S.A. § 117.

Recordkeeping System: A system of coordinated policies and procedures that enable records to be collected, organized, and categorized to facilitate their management, including preservation, retrieval, use, and disposition. Systems may be manual or electronic.



INFORMATION SECURITY BEST PRACTICE

- 1) Information produced or acquired during the course of agency business is considered “public record” under Vermont State law.**
 - Records are defined as “any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of agency business.” (1 V.S.A. § 317(b)).
 - It is the policy of the State of Vermont to “provide for free and open inspection of records” but that all people have “the right to privacy in their personal and economic pursuits, which ought to be protected unless specific information is needed to review the action of government officer.” (1 V.S.A. § 315).

- 2) Information security requirements should be based on legal requirements governing the confidentiality, authenticity and availability of information.**
 - The confidentiality, authenticity and availability of information are statutory obligations of all public agencies pursuant to 1 V.S.A. §§ 315-320 (Subchapter 3: Access to Public Records).
 - Information security practices and procedures should be in compliance with both State and Federal laws and regulations relative to confidentiality, authenticity and availability of information.

- 3) Business processes and associated business tools, including recordkeeping systems, should support information security.**
 - Information security should be built into business processes and the work environment to ensure that confidentiality, authenticity and availability requirements are met.
 - Agencies should understand their business processes and how their operations will be impacted if information is comprised, unavailable or lost.
 - Policies and procedures for the use, labeling, and handling of information should be in place. Such policies and procedures should be consistent with the controls needed based on the format and media of the information.

- 4) Information categorization schemes should clearly articulate the interrelationships among information, legal requirements, recordkeeping, and business processes.**
 - Information security should correlate to the information life cycle: creation/receipt; management; storage; and disposition.
 - Information security categorization should be consistent with business and legal requirements set forth in agency record schedules.

- 5) Information should be categorized according to level of protection needed.**
 - Categorization schemes should define each level of protection and the conditions that need to be met.
 - Policies and procedures should be in place to ensure that information is correctly labeled or tagged into the appropriate category.



6) Information security oversight should be allocated to a coordinated group or unit within the agency comprised of business, legal, information technology, and records staff.

- Individuals with high level responsibilities for business operations, information technology, records management and legal counsel should play a role in overseeing information security.
- Individuals designated to carry out an agency or department's records management program pursuant to 3 V.S.A. § 218 must play a role in overseeing information security.
- Information security policies and procedures should be established and communicated to those for which the oversight group or unit has jurisdiction.

7) Direct ownership, liability and information control should be defined and mapped to the responsible agency division, unit, program, office or staff.

- Senior staff, such as program directors, should be identified as owners of their respective division, unit, program, office or staff's information.
- Senior staff should ensure that their respective division, unit, program, office or staff understands their responsibilities and obligations for information security.
- Agency divisions, units, programs, offices or staffs should comply with the information security policies and procedures set forth by the group or unit with oversight obligations.