Vermont State Archives and Records Administration
Office of the Secretary of State
1078 US RTE 2, Middlesex • Montpelier, VT 05633-7701 • Tel: (802) 828-3700

INFORMATION SECURITY

Effective: May 1, 2009; Last Revised: October 2025

Introduction

The purpose of this statewide records and information management standard is to establish best practices and governance frameworks for information security. This standard 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 and information management.

Scope

This standard applies to all information created or received by Vermont public agencies.

Statement of Authority

Pursuant to 1 V.S.A. § 317a, 3 V.S.A. § 117, and 3 V.S.A. § 218, the Vermont State Archives and Records Administration (VSARA) is authorized to issue record schedules, statewide records and information management standards, and information governance frameworks for the effective management of public records by Vermont public agencies.

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 standard may be directed to the Vermont Chief Records Officer and State Archivist or the Vermont State Archives and Records Administration.

VSARA RIM Standard No. 3

VSARA RIM STANDARD NO. 3 REVISION HISTORY

2025-10	Rebranded as State of Vermont Records and Information Management Standard No. 3 (VSARA RIM Standard No. 3) for clarity when citing in agency records management policies and procedures and for use in the State of Vermont's Self-Assessment of Internal Controls (SAIC) in 2026. Under 4), replaced "classification scheme" with "public access/security codes" to reflect current label/terminology in record schedules. Added 8) for information governance frameworks issued by the Vermont State Archives and Administration under 3 V.S.A. § 117(c)(2-3) and all frameworks related to this standard are now included.
2020-04	Per request from Chief Information Officer and Secretary of the Agency of Digital Services, replaced header and, in Statement of Authority and Contact sections, removed references to the former Department of Information and Innovation; Chief Information Officer; and Agency of Administration statutes. Minor revisions in all sections to align with current legal definitions. "Confidentiality" changed to "protection" and "authenticity" changed to "integrity" to align with Generally Accepted Recordkeeping Principles.
2010-03	Corrected the word "compromise" under Best Practice number 3 (typographical error).
2009-05	Standard jointly issued by the Department of Information and Innovation (DII) and Vermont State Archives and Records Administration (VSARA) following drafting, review, and recommendation by the Information Strategies Taskforce on Archives, Records and Technology (*i*Start).

Definitions

Availability: Ensuring timely and reliable access to and use of information. (NIST Glossary)

Categorization: To put into categories; to classify.

Confidentiality: The designation by law as confidential or by a similar term and the nondisclosure of certain information by law only to specifically designated persons. (1 V.S.A. § 317(c)(1-2))

Information Governance Framework: A framework issued by the Vermont State Archives and Records Administration that establishes governance controls, practices and processes for information acquired or produced in the course of agency business. (3 V.S.A. § 117)

Information Security: A process by which a public agency protects and secures the information it acquires or produces in the course of agency business from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (NIST Glossary)

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

Public Agency: Any agency, board, department, commission, committee, branch, instrumentality, or authority of the State or any agency, board, committee, department, branch, instrumentality, commission, or authority of any political subdivision of the State. (1 V.S.A. § 317(a)(2))

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 policy issued by the Vermont State Archives and Records Administration and approved by the State Archivist governing the life cycle management, retention, and disposition of public records. (1 V.S.A. § 317a; and 3 V.S.A. § 117).

Recordkeeping System: A system of coordinated controls, policies, 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 STANDARD

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 examination of records" but that all people have "a 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 integrity, availability, and protection of records and information.**

    - The integrity, availability and protection of records and information are statutory obligations of all public agencies pursuant to the Vermont Public Records Act (1 V.S.A. §§ 315-320).

    - Information security practices and procedures should comply with Federal and State laws, rules and regulations relating to integrity, availability and protection of records and 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 integrity, availability and protection requirements are met.

    - Agencies should understand their business processes and how their operations will be impacted if records and information are compromised, unavailable or lost.

    - Policies and procedures for the use, labeling, and handling of records and information should be in place. Such policies and procedures should be consistent with the controls needed based on the format and media of the written or recorded information.

4) **Information categorization should clearly articulate interrelationships among information, recordkeeping and legal requirements, and business processes and transactions.**

    - Information security should be implemented at all stages of the record and information lifecycle: creation; receipt; maintenance; use; and disposition.

- Information security categorization should be consistent with business and legal requirements as well as the public access/security codes set forth in record schedules approved by the State Archivist.

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 adopted and implemented to ensure records and information are correctly labeled or tagged into the appropriate category.

6) **Oversight of information security 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 as records officers 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, and staff should comply with the information security policies and procedures set forth by the group or unit with oversight obligations.

8) **For statewide uniformity and consistency, recordkeeping and all other information systems should apply, to the extent possible, the information governance frameworks issued in this standard.**

   - All enterprise and statewide systems shall be managed and operated in a manner that supports public agency compliance with this standard, the Vermont Public Records Act, and where applicable, 3 V.S.A. § 218. (3 V.S.A. § 117(c)(2))

GOVERNANCE FRAMEWORKS FOR INFORMATION SECURITY

The following information governance frameworks for information security are grounded in the *Vermont Public Records Act (1 V.S.A. §§ 315-320)*, *ISO/IEC 27002:2022, NIST Special Publication 800-60 Rev. 2,* and *GAO-24-107026.*

- ✓ Vermont Public Records Act *(1 V.S.A. §§ 315-320)* is a legal compliance requirement for all written and recorded information produced or acquired in the course of public agency business, regardless of format.

- ✓ *ISO/IEC 27002:2022* and NIST Special Publication 800-60 provide frameworks for classifying written and recorded information following an assessment of the impact that a loss of confidentiality, integrity or availability would have on an individual or agency. These assessments are generally mapped to scale ranging from HIGH (greatest impact) to LOW (least impact).

- ✓ *GAO-24-107026 (Federal Information System Controls Audit Manual)* has become the foundation for evaluating the effectiveness of controls over government information systems and provides auditors with a methodology and framework for assessing the design, implementation, and operating effectiveness of these controls in accordance with the Generally Accepted Government Auditing Standards (GAGAS), also known as the Yellow Book.

Public agencies, as part of their records and information management programs, are encouraged to adopt and incorporate the following Information Governance Frameworks into their records and information management policies and procedures.

- VSARA RIM Framework 3.1: Information Security Controls
- VSARA RIM Framework 3.2: Public Access and Security Compliance and Control Matrix
- VSARA RIM Framework 3.3: Public Access and Security Management Controls
- VSARA RIM Framework 3.4: Public Access and Security Management Sub-Controls

General Guidance for Agency Records and Information (RIM) Management Programs

- ✓ Record schedules issued by the Vermont State Archives and Records Administration pursuant to 1 V.S.A. § 317a and 3 V.S.A. § 117 include these frameworks.

- ✓ The absence of a record schedule does not impede the adoption and incorporation of this governance framework. All public agencies must comply with the Vermont Public Records Act (PRA) and manage their records and information according to the PRA, including statutory requirements relating to the confidentiality and availability of information.

- ✓ The term “public access/security code” may be used in agency records management programs for statewide uniformity and consistency among public agencies and in recordkeeping and information systems, especially enterprise and statewide systems.

VSARA RIM Framework 3.1: Information Security Controls

Security	Control Definition
High	Stringent security controls are needed; **breach would have severe impact**. Any unauthorized or accidental modification or destruction of information is **anticipated to cause major damage or injury** to individuals, the agency, and/or the State of Vermont. Safeguards to address unique risks associated with protected personally identifiable information are also needed.
Moderate	Enhanced security controls are needed; **breach could have serious impact**. Any unauthorized or accidental modification or destruction of information is **anticipated to cause significant damage or injury** to individuals, the agency, and/or the State of Vermont.
Low	Essential security controls are needed; **breach could have limited impact**. Any unauthorized or accidental modification or destruction of information **would cause minor damage or injury** to individuals, the agency, and/or the State of Vermont.

VSARA RIM Framework 3.2: Public Access and Security Compliance and Control Matrix

Security	Term	Definition
High	Exempt	Records shall not be provided for free and open examination pursuant to 1 V.S.A. §§ 315-320.
	Redact	Record contains specific information that shall not be provided for free and open examination pursuant to 1 V.S.A. §§ 315-320.
Moderate	General	Record shall be provided for free and open examination pursuant to 1 V.S.A. §§ 315-320.
Low	Publish	Record shall be provided for free and open examination pursuant to 1 V.S.A. §§ 315-320 and are published specifically for public inspection and copying.

VSARA RIM Framework 3.3: Public Access and Security Management Controls

Public agencies responsible for managing and operating enterprise and statewide systems are required to support public agency compliance with the Vermont Public Records Act and, where applicable, 3 V.S.A. 218. (3 V.S.A. § 117(c)(2)).

Term	Definition	Usage
Exempt	Record shall not be provided for free and open examination pursuant to 1 V.S.A. §§ 315-320.	Assign to records that are wholly exempt from public inspection and copying pursuant to 1 V.S.A. § 317.
General	Record shall be provided for free and open examination pursuant to pursuant to 1 V.S.A. §§ 315-320.	Assign to records that are not exempt from public inspection and copying pursuant to 1 V.S.A. § 317.
Publish	Record shall be provided for free and open examination pursuant to pursuant to 1 V.S.A. §§ 315-320 and are published specifically for public inspection and copying.	Assign to records that are not exempt from public inspection and copying pursuant to 1 V.S.A. § 317 and are specifically published for public inspection or copying.
Redact	Record contains specific information that shall not be provided for free and open examination pursuant to pursuant to 1 V.S.A. §§ 315-320.	Assign to records that contain specific information that is exempt from public inspection and copying pursuant to 1 V.S.A. § 317 and must be redacted for public inspection or copying.
Review	Record shall be reviewed internally for consideration of an exemption from public inspection and copying pursuant to 1 V.S.A. § 317.	Assign to records that require internal review for an exemption from public inspection and copying pursuant to 1 V.S.A. § 317.

VSARA RIM Framework 3.4: Public Access and Security Management Sub-Controls

Public access and security management sub-controls allow public agencies to narrow the scope of exemptions to specific categories or types of records as necessary for auditability and information security purposes. Some information systems have preconfigured or configurable categorization schemes for confidentiality and availability based on Federal laws or the Federal Code of Regulations (CFR) that are applicable to all state and local governments.

For records and information categorized as Exempt or Redact, there are nine (9) common categories that can be used as sub-controls for statewide uniformity and consistency. *VSARA RIM Framework 3.4* shall be used with the lists of State of Vermont exemptions in Vermont Statutes Annotated (V.S.A.) compiled and published by the Office of Legislative Counsel in consultation with the Office of the Attorney General (1 V.S.A. § 317(d)).[1]

[1] Executive branch public agencies are encouraged to adopt and implement this framework and the lists compiled by the Office of Legislative Counsel to facilitate consistent and accurate reporting in the Executive Branch Agency Public Records Request System as required under 1 V.S.A. § 318a.

Sub-1: Attorney-Client, Common Law, or Executive Privilege Information	
Applicability/Usage	***Source Definition***
Use for information that would cause the custodian to violate duly adopted standards of ethics or conduct for any profession regulated by the State; or to violate any statutory or common law privilege other than the common law deliberative process privilege as it applies to the General Assembly and the Executive Branch agencies of the State of Vermont.	1 V.S.A. § 317(c)(3); 1 V.S.A. § 317(c)(4)

Sub-2: Criminal Justice Information (CJI)	
Applicability/Usage	***Source Definition***
Use for information dealing with the detection and investigation of crime; and/or criminal justice information (CJI) submitted to, or received from, Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems or services.	1 V.S.A. § 317(c)(5); Criminal Justice Information Services (CJIS) Security Policy

Sub-3: Critical Infrastructure Information	
Applicability/Usage	***Source Definition***
Use for information related to systems and assets, whether physical or virtual, so vital to the State of Vermont and/or the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	1 V.S.A. § 317(c)(25); 1 V.S.A. § 317(c)(32); 6 CFR Part 29

Sub-4: Employment Eligibility or Personnel Information	
Applicability/Usage	***Source Definition***
Use for information related to the determination of employment eligibility for potential employees and information related to the verification and personnel actions of current employees and separated employees.	1 V.S.A. § 317(c)(7)

Sub-5: Juvenile or Education Information	
Applicability/Usage	***Source Definition***
Use for information related to an individual who is or has been a child in need of care or supervision or the subject of a juvenile proceeding; and/or information directly related to an individual who is or has been in attendance at an educational agency or institution and regarding whom the agency or institution maintains education records.	1 V.S.A. § 317(c)(11); Specific state statutes; 34 CFR Part 99

Sub-6: Medical or Individually Identifiable Health Information	
Applicability/Usage	***Source Definition***
Use for medical or psychological information pertaining to any individual; and/or individually identifiable health information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.	1 V.S.A. § 317(c)(7); 1 V.S.A. § 317(c)(37); 1 V.S.A. § 317(c)(38); 1 V.S.A. § 317(c)(39); 45 CFR Part 160; 45 CFR Part 162; 45 CFR Part 164; HIPAA Administrative Simplification Rules

Sub-7: Other Confidential Information	
Applicability/Usage	***Source Definition***
Use for other information designated by law as confidential or by a similar term; or by law may only be disclosed to specifically designated persons.	1 V.S.A. § 317(c)(1); 1 V.S.A. § 317(c)(2)

Sub-8: Protected Personally Identifiable Information (PII)	
Applicability/Usage	***Source Definition***
Use for information that refers to an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, and educational transcripts. Does not include PII that is required by law to be disclosed.	Individual data elements, that if disclosed could result in harm to the individual as defined in 1 V.S.A. § 317(c); Title 9, Chapter 62; Specific state statutes; Federal Privacy Act of 1975

Sub-9: Tax or Federal Tax Information (FTI)	
Applicability/Usage	***Source Definition***
Use for tax returns and related documents that include the same type of information as in the tax return itself; and/or tax return or return information received directly from the Internal Revenue Service (IRS) or an authorized secondary source.	1 V.S.A. § 317(c)(6); IRS Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies.

References

Alberta (Canada), Government of (2011). *Data and Information security classification*. Government of Alberta: Alberta, Canada. Last retrieved October 2025 from https://manuals.alberta.ca/imt-policy-instruments-portal/standards/content-management/data-and-information-security-classification/

International Organization for Standardization (2016). *ISO 15489-1:2016: Information and Documentation – Records Management – Part 1: Concepts and Principles*. International Organization for Standardization: Geneva, Switzerland.

Ibid. (2022). ISO/IEC 27002:2022: *Information security, cybersecurity and privacy protection — Information security controls.* International Organization for Standardization: Geneva, Switzerland.

National Institute of Standards and Technology (2008). *NIST SP 800-60 Vol. 1, Rev. 1: Guide for mapping types of information and information systems to security categories*. National Institute for Standards and Technology: Gaithersburg, MD. Last retrieved 2025 from https://csrc.nist.gov/pubs/sp/800/60/v1/r1/final

Ibid. (2024). *NIST SP 800-60 Vol. 1, Rev. 2 (Initial Working Draft): Guide for mapping types of information and information systems to security categories*. National Institute for Standards and Technology: Gaithersburg, MD. Last retrieved 2025 from https://csrc.nist.gov/pubs/sp/800/60/r2/iwd

Ibid. (2008). *NIST SP 800-60 Vol. 2, Rev. 1: Guide for mapping types of information and information systems to security categories: Appendices*. National Institute for Standards and Technology: Gaithersburg, MD. Last retrieved October 2025 from https://csrc.nist.gov/pubs/sp/800/60/v2/r1/final

United States Government Accountability Office (2024). *GAO-24-107026: Federal information system controls audit manual (FISCAM)*. United States Government Accountability Office: Washington, DC. Last retrieved October 2025 from https://www.gao.gov/products/gao-24-107026