Data Retention Policy Sample

Purpose

The purpose of this Data Retention Policy is to establish guidelines for the retention and disposal of data within [Agency]. This policy ensures that data is retained for appropriate periods to comply with legal, regulatory, and operational requirements specifically with the Virginia Public Records Act (VPRA), Code of Virginia § 42.1-76–§ 42.1-91, which governs the creation, maintenance, and disposition of public records. For detailed information, visit the Library of Virginia's website at Library of Virginia Records Management

Scope

This policy applies to all employees, contractors, and third-party agents who handle, manage, or use data owned by or entrusted to [Agency].

Definitions

Term	Definition
Data	Any information that is stored electronically or in physical form.
Retention Period	The length of time that data must be kept before it can be destroyed.
Data Owner	The person or entity responsible for the overall data governance of a dataset, typically a senior leader within the organization.
Data Steward	An individual responsible for managing a dataset and ensuring its quality and metadata accuracy.
Data User	Any individual who interacts with data for analysis, reporting, or operational purposes.
Data Custodian	IT personnel responsible for the technical environment and security where data is stored, processed, and transmitted.
Records Officer	An individual who oversees the agency's records management program in accordance with the Virginia Public Records Act (VPRA) § 42.1-85. The designated records officer(s) will serve as a liaison(s) to the Library of Virginia for the purposes of implementing and overseeing a records management program, and coordinating legal disposition, including destruction of obsolete records.
ISO	Information Security Officer is responsible for developing and managing the agency's information security program.

Roles and Responsibilities

Role	Responsibility
Data Owner	• Determine appropriate retention periods for data based on legal, regulatory, and operational requirements. • Ensure compliance with this policy within their respective areas. • Approve data destruction requests.
Data User	• Adhere to data retention guidelines and policies. • Report any discrepancies or issues related to data retention to data owners or custodians.
Data Custodians	• Implement and maintain technical safeguards to ensure data is retained according to policy. • Manage data backup and recovery procedures. • Execute data destruction processes as authorized by data owners.
Records Officer	• Developing procedures to implement the agency's records management program in coordination with the Library of Virginia • Providing training in records management procedures and practices, including the use of appropriate forms • Implementing systems to meet program requirements for completeness, legibility, reproducibility, retrievability, distribution, control, security, storage, and disposition of records, regardless of format or media type • Advising staff members on where to access and how to use Library of Virginia–approved retention schedules • Coordinating and/or assisting staff in the surveying of records • Ensuring that essential, archival, and permanent records are identified, properly maintained, protected, and accessible for the length of time cited in an applicable retention schedule • Maintaining contact and connections with AGENCY records coordinators
ISO	• Ensure data retention practices comply with relevant laws, regulations, and standards. • Monitor compliance with the data retention policy and report findings to senior management. • Provide guidance and support for data retention and destruction processes.

Policy

Under Code of Virginia § 42.1-85, the Library of Virginia (LVA) has the authority to issue regulations governing the retention and disposition of state and local public records. In keeping with the Code's mandate, LVA has developed records retention and disposition schedules outlining the disposition of public records.

Under this policy, the LVA issues two types of schedules. General schedules apply to the records of common functions performed by or for all localities and state agencies. Specific schedules apply to records that are unique to an individual state agency.

Before a state agency or locality can destroy public records:

- A records officer for your organization must be designated in writing by completing and filing a Records Officer Designation and Responsibilities (RM-25 Form) with the Library of Virginia.
- Records to be destroyed must be covered by a Library of Virginia-approved general or specific records retention and disposition schedule and the retention period for the records must have expired.
- All investigations, litigation, required audits, and Virginia Freedom of Information Act requests must be completed or fulfilled.
- The organization's designated records officer and an approving official must authorize destruction by completing a Certificate of Records Destruction (RM-3 Form) prior to the records being destroyed.

Data Retention Schedule

The retention schedule is established based on the type of data and applicable legal, regulatory, and operational requirements. Below are examples of common data types and their retention periods:

Type of Record	Description	Retention Period
Administrative Records	Includes internal memos, policies, and procedures.	LVARetentionState (virginia.gov)
Fiscal Records	Includes budgets, invoices, and audit reports.	LVARetentionState (virginia.gov)
Personnel Records	Includes employment contracts, performance reviews, and payroll records.	GS-103.pdf (virginia.gov)
Legal Records	Includes contracts, litigation documents, and compliance records.	Permanent or as determined by legal counsel
General Services Records	Includes maintenance, property, security, and insurance records.	GS-106.PDF (virginia.gov)
Information Technology	Includes network diagrams, project files, system access records.	GS-106.PDF (virginia.gov)

Data Destruction

Data that has reached the end of its retention period must be securely destroyed to prevent unauthorized access or disclosure. The destruction process must comply with applicable laws and regulations.

Data Destruction Procedures:
- Data Custodians are responsible for securely destroying electronic and physical data.
- Methods of destruction may include shredding, degaussing, or using certified data destruction services.
- Data destruction must be documented through the submission of the Library of Virginia Certificate of Records Destruction (RM-3 Form), and records of destruction must be maintained.
- Destruction must be done in a timely manner, construed by the Library of Virginia to be one (1) year from retention expiration.

Authorization for Destruction:
- Data Owners must approve the destruction of data within their purview.
- Data Custodians must ensure that all approvals are obtained before proceeding with destruction.

Compliance

- The Records Officer must conduct regular audits to ensure compliance with the data retention policy.
- The Records Officer must monitor data access and usage to ensure that data is retained and disposed of according to policy.
- The Records Officer, Data Owner, Data Custodian, or Data User must report any non-compliance or data breaches to the Information Security Officer for further action.

Training and Awareness

- The Records Officer must provide training for all employees on data retention policies and procedures.
- The Records Officer must promote awareness of the importance of data retention and secure destruction practices.

Policy Review

This Policy will be reviewed and updated annually from the approval date, or more frequently if appropriate. Any staff members who wish to make any comments about the Policy may forward their suggestions to [AGENCY Contact].

Related Policies

[AGENCY] Policies, Standards and Procedures
Data Governance Policy
Data Quality Policy
Metadata Management Policy
Data Stewardship Policy
Data Security Policy
Data Privacy Policy

The [Agency] adheres to all Commonwealth Information Technology Resource Management (ITRM) policies and standards for security and architecture Policies, Standards & Guidelines | Virginia IT Agency.

VITA Related Policies
IT Information Security Policy - SEC519
Information Security Standard - SEC530
IT Risk Management Standard - SEC520

Version History

Version Number	Revision Date	Description of Change	Author
V1	6/13/2024	Initial Draft	Chris Burroughs