# Data Management Policy

Policy number: 122
Policy owner: Chief Information Security Officer

Date of initial publication: February 24, 2023
Date of latest revision: N/A

## SECTION I. PURPOSE

St. Thomas creates, receives and uses data in the course of its daily operations. Some data are records that have ongoing value to St. Thomas as evidence of the university's organization, functions, policies, decisions, procedures, operations, transactions or other activities.

This policy establishes requirements for the management, retention and destruction of data, including data classified as records. This policy is intended to ensure the effective functioning of St. Thomas, the preservation of its history, the efficient use of resources, the appropriate protection of confidential and sensitive data, and compliance with legal requirements.

## SECTION II. SCOPE AND APPLICABILITY

This policy governs the management of all St. Thomas data in any format, including data storage, access, sharing, transmission, retention and destruction. This policy applies to all employees (faculty, staff and student workers), volunteers, contractors, student clubs and organizations, schools, colleges, divisions, departments and other units.

## SECTION III. DEFINITIONS

When used in this policy, the following terms have the following meanings:

a. ***Active*** means the data is used to support current St. Thomas operations and activities.

b. ***Archival record*** means a record that has enduring historical value to St. Thomas, including (i) the categories denoted as archival records in the record retention schedule; and (ii) any other data the university archivist or president designates as an archival record.

c. ***CISO*** means the university's chief information security officer or designee.

d. *A* ***collection*** means books, periodicals, newspapers and other materials that St. Thomas maintains as part of its library collections or special collections.

e. ***Confidential*** means the data is intended to be non-public and maintained internally on a need-to-know basis.

f. ***Data*** means all information, recorded in any format, that is collected, created, generated, held, legally filed, owned, received, shared or stored by St. Thomas, or that St. Thomas is obligated to maintain or manage in accordance with applicable law, an accreditation requirement, a membership requirement, or an agreement. Data can exist in any tangible format including but not limited to electronic and physical documents and communications, film and print graphics, and audio and video recordings. Data does not include personal papers, personal communications and private materials made or received by St. Thomas employees, volunteers or contractors outside of their St. Thomas role and responsibilities.

g. ***Data holder*** is anyone who holds data.

h. ***Data custodian*** means the person or unit responsible (typically ITS) for implementing the management, retention and destruction policies of a particular category or categories of data.

i. ***Data owner*** means each unit manager and any other St. Thomas position designated as having ultimate responsibility for the management, retention and destruction of a particular category or categories of data.

j. ***Data steward*** is any St. Thomas faculty or staff member to whom a data owner has designated day-to-day responsibility for the care and management of a particular category or set of data, whether or not, the data steward directly holds the data.

k. ***Duplicate*** means a replica of data produced for convenience, or stocks of printed or reproduced materials beyond one copy.

l. ***Electronic*** means data kept in a non-tangible electronic format, such as word processor documents, spreadsheets, databases, HTML documents, scanned or imaged documents, and any other type of file maintained in a data warehouse, on a server or computer hard drive, or on any external storage medium (such as a flash drive).

m. ***Export control laws*** are laws and regulations intended to prevent the transfer or export of certain export-controlled data, materials and technology to designated foreign countries and foreign nationals, regardless of where the foreign national is located.

n. ***Export-controlled data*** means certain kinds of technical information that are controlled by the federal government for national security or trade protection purposes.

o. ***Foreign nationals*** generally mean non-U.S. citizens, immigrants who are not lawfully admitted to the United States for permanent residence, and foreign entities.

p. ***Inactive*** means the data is not used to support current St. Thomas operations and activities.

q. ***Litigation hold*** means a requirement to preserve data for an indefinite period of time as a result of a pending or anticipated legal matter.

r. ***Personally identifiable information*** means a person's name, or another piece of information that can identify someone without more information, or a combination of information that can personally identify someone.

s. ***Physical*** means data kept on paper or in another non-electronic media.

t. ***Privacy laws*** are laws and regulations intended to prevent the inappropriate sharing of personally identifiable information. Some states and countries maintain stringent restrictions on the sharing of information about individuals who are residents of their state or country, even if the entity maintaining the information is not located or doing business in that state or country.

u. ***Record*** means any recorded information created or received in the course of conducting St. Thomas operations, that is in a category of data required to be retained for any period of time under the St. Thomas Record Retention Schedule. Records may be in any recorded format, including but not limited to electronic and physical documents and communications, film and print graphics, and audio and video recordings. Records do not include collections, duplicates, reference data or transitory communications.

v. ***Record retention schedule*** means the schedule found in Policy 106, Record Retention Schedule, which identifies the retention periods for records.

w. ***Reference data*** means data that St. Thomas obtains from a third party without any obligation of confidentiality and maintains solely for reference purposes.

x. ***Transitory communication*** means data in the form of instant messages, texts, voicemails, emails and similar communications, the content of which is limited to logistical information (such as arranging meetings or calls) or courtesies (such as making an introduction or thanking someone), and that does not contain substantive information that facilitates the university's transactions, operations, activities or decisions.

y. ***Retention period*** means the retention period for designated categories of records, as set forth in the record retention schedule.

## SECTION IV. RESPONSIBILITIES OF DATA HOLDERS, DATA OWNERS AND DATA STEWARDS

### A. General Responsibilities

Each person covered by this policy is a data holder. Some people covered by this policy also are data stewards or data owners. Data holders, data stewards and data owners are responsible for managing the data they hold in accordance with this policy. Data owners and data stewards have additional responsibilities described in Section IV.B.

Failure to comply with this policy can result in disciplinary action, up to and including dismissal from employment or service, and civil and criminal liability. If you have questions about data management, retention or destruction, contact the data owner for the set of data you hold, the CISO or the Office of General Counsel.

### B. Responsibilities of Data Owners

Each data owner has the following responsibilities, which may be delegated to data stewards but remain the ultimate responsibility of the data owner:

- Determine the appropriate definitions and format for the data under their areas of responsibility.
- Determine the appropriate utilization (the "how" and "why") of the data under their areas of responsibility.
- Ensure the availability and application of appropriate storage and access parameters for data under their areas of responsibility, in accordance with the St. Thomas Data Security Classification Policy.
- Authorize the timely destruction of inactive records under their areas of responsibility in accordance with this policy.
- Ensure that data under their areas of responsibility are appropriately identified and retained in response to any litigation hold on the data.

### C. Responsibilities of Data Stewards

Each data steward has the following responsibilities, in addition to those delegated from the above data owner's responsibilities:

- Educate functional areas to facilitate understanding of sound data management practices for the data under their area/s of responsibility.
- Be the subject matter expert for data under the area/s of responsibility.
- Ensure utilization parameters set by the Data Owner are followed by all and necessary data ethics discussions occur openly with the Data Owner.
- Maintain and create sound business processes to achieve parameters set by Data Owner.

### D. Responsibilities of Data Custodians

Each data custodian has the following responsibilities, which are executed in support of the parameters determined by Data Owners and in accordance with information technology best practices and other university policies:

- Assign, remove, and document access for others based upon the direction of the Data Owner.
- Produce data lists, reports, analysis, or derivative information for others with approval from Data Owner.
- Implement appropriate physical and technical safeguards to protect the confidentiality, security, integrity, and availability of the information asset dataset.
- Implement processes for data quality issue resolution in partnership with Data Stewards.
- Data added to data sets are consistent with the common data model.
- Versions of Master Data are maintained along with the history of changes.
- Follow university change management practices for maintenance of databases and data storage systems.
- Identify and ensure the preservation of archival records under their areas of responsibility while the records are active and authorize and ensure the transfer of archival records to the University Archives when the records become inactive.
- Audit data content and changes regularly to ensure effective controls, and integrity of data.

## SECTION V. DATA STORAGE

- **Comply with the Data Security Classification Policy.** Data must be stored with the level of security and access restrictions contained in the St. Thomas Data Security Classification Policy.
- **Securely Store Both Physical and Electronic Data.** Both physical and electronic data must be stored in accordance with applicable security and access restrictions. Locked storage should be utilized for physical data that requires restriction.
- **Use St. Thomas Systems to Store Data.** Except when shared or transported outside St. Thomas, all data must be stored in a system, file, account, device or other location that is owned and maintained by St. Thomas, or that is maintained on behalf of St. Thomas by a contracted vendor.
- **Don't Store Records in Email or Other Communication Systems.** St. Thomas communication systems (such as email, voicemail and instant messaging systems like Microsoft Teams) are not intended to be used for long-term records storage and retention. These systems are subject to automated destruction cycles that may be modified at any time in the university's discretion. If a communication contains records (whether in the body of the communication or in an attachment), timely move the records to a St. Thomas system or account that is not subject to automated destruction cycles.
- **Store Data in a Manner that Makes It Easy to Find.** Organize data in ways that make it easy to find specific data when needed.
- **Communications that Are Records Should Be Stored Based on the Content of the Record.** Communications, such as emails or text messages, that need to be retained as active

records should be saved and stored with other records of the same type. For example, communications that are student education records should be stored with other student education records you maintain, rather than in a personal correspondence file.

- **Records Attached to a Communication Should Be Stored in a Way that Permits Separate Access.** Attachments to communications should be saved in a manner that makes the attachment accessible independently from the communication.

## SECTION VI. DATA ACCESS

- **Restrict Access to Confidential Data.** In all cases, access to confidential data should be restricted to individuals with a legitimate need to know or access the information for purposes of their St. Thomas role and responsibilities. Confidential data should be stored in a manner that prevents access by those who do not have a legitimate need to know or access the information.
- **Only Access Data You Are Authorized to Access.** You must not access data unless you are authorized to access the data. If you are unsure whether you are authorized to access data, ask the data owner, data steward or CISO.
- **Use Secure Systems to Access Data Remotely.** When working remotely, access data through approved means, using either a St. Thomas device or St. Thomas secured system. Data should not be accessed through public computers or using public wi-fi. Data should not be downloaded to a device unless the device is owned by or registered with St. Thomas and subject to appropriate password protection or similar access controls.

## SECTION VII. DATA RETENTION

### A. Retain Data that Is Subject to a Litigation Hold

If St. Thomas is involved in or reasonably anticipates certain legal matters, such as litigation or a government investigation, the university is legally obligated to establish a litigation hold that preserves all data related to the matter until after the matter resolves.

Litigation holds are established and released by the Office of General Counsel. If you receive a litigation hold notice from the Office of General Counsel, you must ensure the preservation of data in accordance with the notice, until the Office of General Counsel notifies you in writing that the litigation hold has been released. You also must cooperate with all measures initiated by St. Thomas in connection with the litigation hold. These measures may include, for example, collecting or copying data in your possession, or the application of automated rules to prevent the deletion of data from St. Thomas systems and accounts.

Litigation holds generally apply to all data related to the matter, regardless of whether the data is active, inactive, a record, reference data, a transitory communication, or part of a collection. Litigation holds also apply to duplicates that have been altered from the original in any way (for example, through the addition of handwritten or typed annotations, highlighting or similar markings or alterations).

If you become aware of or reasonably anticipate a legal matter involving St. Thomas and you have not received a litigation hold notice from the Office of General Counsel, or you receive a litigation hold notice from an individual who is not a member of the Office of General Counsel, contact the Office of General Counsel promptly (generalcounsel@stthomas.edu) and preserve all data related to that matter until further notice from the Office of General Counsel.

### B. Retain Records While Active and for the Applicable Record Retention Period

Unless they are subject to a litigation hold, records should be retained as long as they are active or, if longer, for the retention period provided in the record retention schedule.

The record retention schedule is intended to be as complete as practicable, but it is not exhaustive. Its categories and retention periods are based on applicable law and the university's known operational needs and institutional interests. If you have questions about whether particular data is a record or fits into a particular records category, or you believe that data you maintain should be added to the record retention schedule, contact the CISO or Office of General Counsel.

Record retention periods may be temporarily modified from time to time for reasons other than litigation holds, such as judicial or administrative orders, audits, contractual requirements or special circumstances. Temporary modifications may be imposed by the data owner or the president, CISO, university archivist or another authorized St. Thomas representative in consultation with the Office of General Counsel. Temporary modifications generally must be communicated to affected data stewards by an authorized St. Thomas representative. Data stewards are responsible for communicating such temporary holds to data holders.

### C. Keep Other Data Only While Active

Unless they are subject to a litigation hold or other temporary hold, transitory communications should be disposed of promptly after they are read, and other data that are not records generally should be retained only while the data is active. The data owner or data steward may exercise discretion to direct or permit the retention of inactive data if either of them determines that continued retention of the data is consistent with near-term institutional needs and resources. The discretionary retention of inactive data that are not records is intended to be temporary and short-term in nature.

### D. St. Thomas May Limit Storage Space for Data that Does Not Require Retention

At its discretion, St. Thomas may choose not to allocate incremental resources (such as storage space) for the preservation of data that is not required to be retained.

## SECTION VIII. SHARING AND TRANSPORTING DATA OUTSIDE ST. THOMAS

### A. Only Share or Transport Data for a Legitimate Business Purpose

Data may be shared or transported outside St. Thomas only for legitimate business reasons and only as permitted by law and University policy.

### B. Comply with Security and Preservation Requirements

When being shared or transported, data remains subject to the security and access controls under the Data Security Classification Policy. In addition, to mitigate the risk of loss, records may not be shared or transported outside St. Thomas unless (i) a duplicate has been created and is preserved in an appropriate St. Thomas file, system or account or (ii) the record is being transported to a St. Thomas-designated off-site secure storage facility.

### C. Comply with Export Control Laws and Privacy Laws

Transporting data outside the United States, sharing personal information between countries, and sharing data with foreign nationals and foreign entities all carry heightened data security risk. In addition, these activities may be regulated by export control laws and privacy laws. St. Thomas

requires compliance with these laws. Violating these laws can result in significant costs and penalties, including civil and criminal liability.

Privacy laws may restrict the sharing of data across national borders or mandate certain procedures to be followed. Export control laws may prohibit students, faculty and staff from bringing research or other data with them when traveling to designated foreign countries. It also may prohibit them from sharing such data with foreign nationals from certain countries, regardless of whether the data is shared inside or outside the United States. Transporting export-controlled data outside the United States or sharing the data with designated foreign nationals generally requires a license from the U.S. government.

To ensure compliance with export control and privacy laws:

- **St. Thomas May Control Devices Transported Outside the United States.** St. Thomas may prohibit the transport or use of St. Thomas computers, mobile devices, portable drives and other assets outside the United States. St. Thomas may require travelers to utilize specially designated computers, mobile devices, portable drives or other assets when traveling outside the United States.
- **St. Thomas May Control Data Transported Outside the United States.** St. Thomas may require travelers whose personal devices provide access to St. Thomas data or systems to remove or encrypt the data and/or remove or lock down St. Thomas applications when traveling outside of the United States.
- **Check with the Senior International Officer Before You Transport or Transfer Confidential Data Across National Borders.** If you are planning to transport or transfer confidential data outside the United States and you are not familiar with export control laws and privacy laws, contact the senior international officer to ensure you have all the information you need to comply with applicable laws and mitigate risks.
- **Check with the Senior International Officer Before You Share Export-Controlled Data with Non-U.S. Persons.** If you hold data that may fall within a category of export-controlled data, and you plan to share that data with a foreign national or foreign entity, contact the senior international officer to ensure you have all the information you need to comply with applicable laws.

## SECTION IX. DATA DESTRUCTION

### A. When to Destroy Data

Inactive data (including records) that is not designated as an archival record should be promptly destroyed upon the *latest* of:

1. the data becomes inactive,
2. expiration of the record retention period if the data is a record, and
3. expiration of any applicable litigation hold or temporary modification that extends the applicable retention period.

St. Thomas may require the destruction of data that is not legally required to be retained, even if the data is active, if such destruction is consistent with operational needs and institutional interests.

### B. How to Destroy Data

Data should be destroyed in one of the following ways:

- Recycle non-confidential paper data.
- Securely shred confidential paper data.
- Permanently destroy non-paper physical data so that confidential information cannot practicably be read or reconstructed.
- Permanently delete or erase electronic data so that confidential information cannot practicably be read or reconstructed.

The Innovation and Technology Services division has responsibility for the permanent destruction of electronic data and microforms that are deleted from the university's electronic systems and accounts, including the regular overwriting or physical destruction of back-up tapes. Contact Innovation and Technology Services if you have questions about the permanent destruction of other electronic records.