Data Security Policy Compendium

Policy number: 800-IT-6
Policy owner: Chief Information Security Officer

Date of initial publication: March 2, 2023
Date of latest revision: N/A

SECTION I. PURPOSE

This policy compendium is intended to collect and reference all St. Thomas data security requirements in a single document for easy reference. It includes all policies that:

- help St. Thomas and its community members comply with legal, contractual and institutional requirements to protect data;
- help safeguard the university's information technology resources from accidental or intentional damage;
- help safeguard data from alteration or theft; and
- designate the appropriate level of security requirements for securing data and information technology resources.

Some of these data security requirements are contained directly in this policy compendium, while others are linked from this policy.

SECTION II. SCOPE AND APPLICABILITY

This policy governs all data. This policy applies to all St. Thomas employees (faculty, staff and student workers), student clubs and organizations, contractors and volunteers.

SECTION III. DEFINITIONS

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

a. ***CDO*** means the university's chief data officer or designee.

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

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

d. ***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.

e. ***Data security incident*** means an incident involving the known or suspected: loss, theft or destruction of IT resources; malware on IT resources; unintentional disclosure, destruction, loss or disclosure of confidential data; or unauthorized access, use, disclosure, transfer or destruction of data or IT resources.

f. ***IT resources*** means the university's information technology resources, including software, systems and computers, servers, other hardware and other devices used to create, generate, hold, share or store data.

g. ***ITS*** means the university's Innovation and Technology Services unit.

h. ***WISP*** means the comprehensive written information security program maintained by St. Thomas and linked from this policy.

SECTION IV. GENERAL DATA SECURITY REQUIREMENTS TRAINING

In order to access data and IT resources, all employees are required to complete regularly provided data security awareness training. Employees, volunteers and contractors may be required to undergo additional training specific to applicable regulations, systems and internal compliance expectations relevant to the individual's St. Thomas role and responsibilities and level of system access. The CISO and CDO are jointly responsible for determining minimum training requirements for data and systems access.

A. Report Data Security Incidents

Employees, volunteers and contractors must report data security incidents to the ITS Information Security unit as soon as the individual becomes aware of the incident.

B. Comply with Applicable Policies

All persons covered by this policy are expected to comply with this policy (including all polices linked from this policy). Violations of this policy may result in suspension or loss of the violator's data access and use of IT resources. Additional administrative sanctions may apply up to and including termination of employment or volunteer or contractor status with the University.

If you have questions about this policy, contact the CISO.

SECTION V. MINIMUM SECURITY STANDARDS

If this policy (including any of the policies linked from this policy) does not directly address a particular category of data, the Minimum Security Standards should be used as the baseline for determining the security controls needed.

SECTION VI. WRITTEN INFORMATION SECURITY PROGRAM

In order to comply with various state and federal data security and privacy regulations, St. Thomas has adopted a WISP that summarizes the steps and controls St. Thomas follows to protect constituent data. Many of the steps and controls addressed in the WISP also appear in the policies referenced in this compendium. In cases where there is a conflict between the WISP and an individual policy, the WISP will take precedence.

SECTION VII. DATA SECURITY POLICIES

In addition to the expectations contained in this policy compendium, the following policies regarding specific aspects of data security also apply.

A. Technology Use Related Policies

1. **Responsible Use of Computing Resources Policy**
2. **Personal Device and Remote Work Technology Policy**
3. **Remote Access Policy**
4. **Mass E-mail Policy**

B. Data Related Policies

1. **Written Information Security Program Policy**
2. **Online Privacy Policy**
3. **Data Management Policy**
4. **Records Management and Retention Policy & Schedules**
5. **Data Security Classification Policy**

C. Technology Management Policies and Standards

1. **Minimum Security Standards**
2. **Workstation Administrator Policy**
3. **IT Change Management Policy**

SECTION VI. AUTHORITY AND ADMINISTRATION

A. Emergencies

In emergency cases, actions may be taken by the Incident Response Team in accordance with the procedures in the ITS Incident Response plan. These actions may include rendering systems inaccessible.

B. Exceptions

This policy represents a baseline of information security requirements for the University.

In certain situations, compliance with this policy or the Minimum Security Standards may not be immediately possible. In such cases, the CISO is authorized to make exceptions. Requests for exceptions should be submitted here.

C. Review

This policy, and all policies, standards, handbooks and supporting materials contained within, will be reviewed by ITS Information Seecuirty and Risk Management on an annual basis.