Written Information Security Program

Policy number: 120
Policy owner: Chief Information Security Officer

Date of initial publication: December 19, 2022
Date of latest revision: N/A

SECTION I. PURPOSE

The objectives of this comprehensive written information security program ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards St. Thomas has selected to protect the personal information it 09 46A.622, Rhode Island General Laws § 11-49.3-2, and the Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314.

If this WISP conflicts with any contractual obligation or St. Thomas policy or procedure, then the provisions of this WISP will govern, unless the Information Security Coordinator (see Section 3) specifically reviews, approves, and documents an exception (see Section 3(e)).

The purpose of this WISP is to:

a. Ensure the security, confidentiality, integrity, and availability of personal information St. Thomas collects, creates, uses, and maintains.

b. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

c. Protect against unauthorized access to or use of St. Thomas-maintained personal information that could result in substantial harm or inconvenience to the individual to whom the personal information relates.

d. Define an information security program that is appropriate to St. Thomas's size, scope, business, and complexity, its available resources, the amount of personal information that St. [illegible] For purposes of this WISP, "personal name or first initial and last name together with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against such individual:

   i. Social Security number or tax identification number;

   ii. Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

iii. Account number, including a bank account number, or credit or debit card number, with or without any required security code, access code, personal identification number, password, or expiration date, that would permit access to, or any other information or combination of information that such individual reasonably knows or should know would permit access to, or that would permit the conduct of a transaction that will credit or debit, such individual's account;

iv. Health information, including medical identification number, information regarding such individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional;

v Health insurance identification number, health insurance policy number, subscriber identification number, or other unique identifier used by a health insurer; or

vi. Biometric data collected from such individual and used to authenticate such individual during a transaction, such as an image of a fingerprint, retina, palm, or iris.

b. User name, unique identifier, electronic mail address, or other means of identifying such individual together with any required password, security code, access code, security question and answer, or any other method necessary to authenticate the user name or means of identification, that would permit access to such individual's online account.

c. For purposes of this WISP, "personal information" also includes financial customer information. "Financial customer information" has the same meaning as "customer information" under the Gramm-Leach-Bliley Act ("GLBA"). Specifically, financial customer information means any personally identifiable financial information or list, description, or other grouping of persons (and publicly available information pertaining to them) derived from nonpublic personally identifiable financial information, where personally identifiable financial information includes any information:

i. A person (such as a St. Thomas student) provides St. Thomas to obtain a financial product or service;

ii. About a person resulting from any transaction involving a financial product or service with St. Thomas; or

iii. Information St. Thomas otherwise obtains about a person in connection with providing a financial product or service to the person.

For purposes of this WISP, "financial product or service" has the meaning under the GLBA and includes Title IV federal financial aid packaged by the St. Thomas Financial Aid Office, as well as the open-end credit account that all students establish through the St. Thomas Business Office for purposes of paying tuition, fees and other costs owed to St. Thomas.

d. Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records, other than a Social Security number.

e. For purposes of this WISP, "security incident" includes (without limitation) a security event under the GLBA (see Section 2(f)).

f. The terms authorized user, consumer, customer, encryption (with respect to customer information), financial product or service, multi-factor authentication, penetration testing,

security program and St. Thomas safeguards to protect personal information, including the

SECTION V. INFORMATION SECURITY POLICIES AND PROCEDURES

As part of this WISP, St. Thomas will develop, maintain, and distribute information security policies and procedures, in accordance with applicable laws and standards, to relevant employees, contractors, and other stakeholders. Specifically, St. Thomas will:

a. Establish policies addressing:
    i. Information classification;
    ii. Information handling practices for personal information, including the storage, access, disposal, and external transfer or transportation of personal information;
    iii. User access management, including identification and authentication (using passwords or other appropriate means);
    iv. Encryption;
    v. Computer and network security;
    vi. Physical security;
    vii. Incident reporting and response;
    viii. Employee and contractor use of technology; and
    ix. Information systems acquisition, development, operations, and maintenance.
b. Detail the implementation and maintenance of St. Thomas's administrative, technical, and physical safeguards (see Section 6).

SECTION VI. SAFEGUARDS

St. Thomas will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that St. Thomas owns or maintains on behalf of others.

a. Safeguards will be appropriate to St. Thomas's size, scope, business, complexity, and available resources; the amount of personal information St. Thomas owns or maintains on behalf of others; the type, nature, and scope of St. Thomas's activities involving such personal information; and the particular sensitivity of any personal information, while recognizing the need to protect all personal information.
b. St.

iii.

SECTION VII. SERVICE PROVIDER OVERSIGHT

St. Thomas will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

a. Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and St. Thomas's obligations.

b. Requiring the service provider by written contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and St. Thomas's obligations.

c. Monitoring and periodically assessing the service provider's performance to verify compliance with this WISP and all applicable laws and St. Thomas's obligations.

SECTION VIII. MONITORING

St. Thomas will regularly test and monitor the implementation and effectiveness of its information somad4 7hom4463s462Tw wn

(A.) The incident response plan's goals;

(B.) St. Thomas's incident response processes;

(C.) Roles, responsibilities, and levels of decision-making authority; and

(D.) Processes for internal and external communications and information sharing.

ii. Identifying remediation requirements to address any identified weaknesses in St. Thomas's systems and controls.

iii. Documenting and appropriately reporting information security events and St. Thomas's response activities.

iv. Performing post-security event reviews and updating the plan as appropriate.

SECTION X. ENFORCEMENT

Violations of this WISP will result in disciplinary action in accordance with applicable St. Thomas policies and procedures.

SECTION XI. PROGRAM REVIEW

a. St. Thomas will review this WISP and the security measures defined herein at least annually, when indicated by St. Thomas 's risk assessment (see Section 4) or program monitoring and testing activities (see Section 8), whenever there is a material change in St. Thomas's business practices, operations or arrangements that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information, or any other circumstances occur that may have a material impact on St. Thomas's information security program.

b. St. Thomas will retain documentation regarding any such program review, including any identified gaps and action plans.

SECTION XII. EFFECTIVE DATE

This WISP is effective as of the date indicated on page 1.