UNIVERSITY OF St.Thomas

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 collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of Alabama Code § 8-38-3, 201 Code of Massachusetts Regulations §§ 17.01 et seq., Nevada Revised Statutes § 603A.210, Oregon Revised Statutes § 646A.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. Thomas owns or maintains on behalf of others, the type, nature, and scope of St. Thomas's activities involving such personal information, and the sensitivity of any customer information, while recognizing the need to protect personal information.

SECTION II. SCOPE

This WISP applies to all employees (faculty, staff, and student employees), officers, contractors, and volunteers of St. Thomas. It establishes information security requirements for all records and other information owned, held, maintained or managed by St. Thomas that contain personal information in any format and on any media, whether in electronic or paper form.

a. For purposes of this WISP, "personal information" means either a person's first and last 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,

and security event will have the same meanings as those terms in the Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314.

SECTION III. INFORMATION SECURITY COORDINATOR

St. Thomas has designated its Chief Information Security Officer to implement, coordinate, and maintain this WISP (the "Information Security Coordinator"). The Information Security Coordinator will be responsible for:

a. Initial implementation of this WISP, including:
   i. Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);
   ii. Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);
   iii. Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information (see Section 6);
   iv. Ensuring that the safeguards are implemented and maintained to protect personal information throughout St. Thomas, where applicable (see Section 6);
   v. Overseeing service providers that access or maintain personal information on behalf of St. Thomas (see Section 7);
   vi. Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);
   vii. Defining and managing incident response procedures (see Section 9); and
   viii. Establishing and managing enforcement policies and procedures for this WISP, in collaboration with St. Thomas Office of Human Resources (see Section 10).

b. Engaging qualified information security personnel, including:
   i. Providing them with security updates and training sufficient to address relevant risks; and
   ii. Verifying that they take steps to maintain current information security knowledge.

c. Training of employees and (as applicable) contractors, volunteers, vendors, and other third parties, including providing periodic training regarding this WISP, St. Thomas's safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal information, updated as necessary or indicated by St. Thomas's risk assessment activities (see Section 4);

d. Reviewing this WISP and the security measures defined herein at least annually, and when indicated by St. Thomas's risk assessment (see Section 4) or program monitoring and testing activities (see Section 8), or whenever there is a material change in St. Thomas's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information (see Section 11).

e. Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or St. Thomas's information security policies and procedures.

f. At least annually providing to St. Thomas management and its Board of Trustees (or an appropriate committee of the Board) a written report regarding the status of the information

security program and St. Thomas safeguards to protect personal information, including the program's overall status, compliance with applicable laws and regulations, material matters related to the program, such as risk assessment, risk management and control decisions, service provider arrangements, testing results, security events or policy violations and management's responses, and recommendations for program changes.

SECTION IV. RISK ASSESSMENT

St. Thomas based this WISP on a written risk assessment identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessed the sufficiency of any safeguards in place to control these risks. As a part of maintaining this WISP, St. Thomas periodically will perform additional risk assessments to reexamine these considerations.

a. As part of these periodic risk assessments, St. Thomas will:

   i. Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information and include criteria for evaluating and categorizing those identified risks;

   ii. Define assessment criteria and assess the likelihood and potential damage that could result from such risks, including the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the personal information, taking into consideration the sensitivity of the personal information; and

   iii. Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

      A. Employee, contractor, and (as applicable) stakeholder training and management;

      B. Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures;

      C. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

      D. St. Thomas's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

b. Following each risk assessment, St. Thomas will:

   i. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

   ii. Reasonably and appropriately address any identified gaps, including documenting St. Thomas's plan to remediate, mitigate, accept, or transfer identified risks, as appropriate; and

   iii. Regularly monitor the effectiveness of St. Thomas's safeguards, as specified in this WISP (see Section 8).

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. Thomas will document its administrative, technical, and physical safeguards in St. Thomas's information security policies and procedures (see Section 5).
c. St. Thomas's administrative safeguards will include, at a minimum:
    i. Designating one or more employees to coordinate the information security program (see Section 3);
    ii. Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4);
    iii. Training employees in security program practices and procedures, with management oversight (see Section 3);
    iv. Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7); and

v. Adjusting the information security program in light of business changes or new circumstances (see Section 11).

d. St. Thomas's technical safeguards will include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

i. Secure user authentication protocols, including:

(A.) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

(B.) Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and

(C.) Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

ii. Secure access control measures, including:

(A.) Restricting access to records and files containing personal information to those with a need to know to perform their duties; and

(B.) Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.

iii. Encryption of all personal information transmitted wirelessly or traveling across public networks;

iv. Encryption of all personal information stored on laptops or other portable or mobile devices;

v. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures;

vi. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information; and

vii. Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

e. St. Thomas's physical safeguards will, at a minimum, provide for:

i. Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers;

ii. Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal; and

iii. Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

f. St. Thomas's safeguards with respect to financial customer information will, at a minimum, include:

i. Implementing and periodically reviewing technical and, as appropriate, physical access controls to:

(A.) Authenticate and permit access to financial customer information only to authorized users; and

(B.) Limit authorized users' access only to financial customer information that they need to perform their duties and functions, or in the case of financial customers, to access their own information;

ii. Identifying and managing the data, personnel, devices, systems, and facilities that enable St. Thomas to achieve its business purposes according to business priorities, objectives, and St. Thomas's risk management strategy;

iii. Encrypting financial customer information that St. Thomas holds when it is at rest or in transit over external networks, unless St. Thomas determines that applying encryption is currently infeasible for its circumstances and the Information Security Coordinator reviews and approves effective alternative compensating controls under St. Thomas's exceptions process (see Section 3(e));

iv. Adopting secure development practices for in-house developed applications and procedures for evaluating, assessing, or testing the security of externally developed applications that in either case St. Thomas uses to transmit, access, or store financial customer information;

v. Implementing multi-factor authentication for individuals accessing financial customer information or systems that handle financial customer information unless the Information Security Coordinator reviews and approves in writing the use of reasonably equivalent or more secure access controls under St. Thomas's exceptions process (see Section 3(e));

vi. Developing, implementing, and maintaining procedures for securely disposing of financial customer information in any format, including:

(A.) Disposing of financial customer information no later than two years after the last date St. Thomas uses it for provisioning a product or service to the relevant financial customer unless it is necessary for business operations or other legitimate business purposes, retention is otherwise required by law or regulation, or targeted disposal is not reasonably feasible due to way St. Thomas maintains it; and

(B.) Periodically reviewing St. Thomas's data retention policies to minimize the unnecessary retention of financial customer information;

vii. Adopting change management procedures; and

viii. Implementing policies, procedures, and controls to monitor and log authorized users' activities and detect unauthorized access to, use of, or tampering with, financial customer information by them.

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 security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal information. St. Thomas will reasonably and appropriately address any identified gaps.

St. Thomas's testing and monitoring program will address the effectiveness of St. Thomas's safeguards, specifically their key controls, systems, and procedures, including those St. Thomas uses to detect attempted and actual attacks on or intrusions into its networks and systems that handle personal information.

St. Thomas will implement and maintain as appropriate for its networks and systems that handle financial customer information either:

a. Continuous monitoring or other systems to detect on an ongoing basis changes that may create vulnerabilities; or

b. A combination of the following according to St. Thomas's risk assessment (see Section 4):

   i. Annual penetration testing; and

   ii. Periodic vulnerability assessments, including systemic scans or reviews reasonably designed to identify publicly known security vulnerabilities, conducted at least every six months and whenever there are material changes to St. Thomas's operations or business arrangements, or circumstances occur that may have a material impact on St. Thomas's information security program.

SECTION IX. INCIDENT RESPONSE

St. Thomas will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures will include:

a. Documenting the response to any security incident or event that involves a breach of security.

b. Performing a post-incident review of events and actions taken.

c. Reasonably and appropriately addressing any identified gaps.

Such procedures with respect to financial customer information will include a written incident response plan:

   i. Defining:

(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.