# Data Security Classification Policy

Policy number: 114
Policy owner: Information Technology Services

Date of initial publication: June 6, 2017
Date of latest revision: March 2, 2023

## SECTION I. PURPOSE

The purpose of this policy is to provide a structured and consistent process for defining the university's data security levels, which will establish the foundation for appropriate access control policies and procedures used across the university. St. Thomas takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty and staff, as well as to protect the confidentiality of information important to the university's mission.

## SECTION II. SCOPE AND APPLICABILITY

This policy applies to:

- Employees (faculty, staff, student workers)
- Student clubs and organizations
- Contractors
- Volunteers

This policy does not apply to materials and information that are the personal property of individuals covered by the policy, such as personal notes.

## SECTION III. DEFINITIONS

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

- ***Data*** **-** All information generated or owned by the University of St. Thomas (including, but not limited to, information generated or developed by the university's employees in the course of their job duties and responsibilities, unless the university has waived its ownership rights to the Data) and information not generated or owned by the university, but which the university has the duty to manage. This information can exist in any form including, but not limited to, print, electronic and digital.
- ***Data Owner*** – The designated person at the university assigned as the owner and decision maker on the respective set of Data. The Data Owner sets the appropriate data classification and determines the impact the Data has for continuity and disaster recovery purposes.
- ***Data Steward*** – Faculty or staff member who has been assigned as the person directly responsible for the care and management of a certain type of Data. Data Stewards are responsible for approving access to the Data they manage. For example, the Registrar is responsible for approving access to Student Data.
- ***Data Custodian*** – Person or unit responsible (typically ITS) for implementing the management, retention and destruction policies of a particular category or categories of data.

- ***FERPA-Protected Student Data*** – Includes all information related to a student's academic record not defined by the university as directory information. See: http://www.stthomas.edu/registrar/student/ferpa/annualnotice
- ***Least Privilege Required*** **-** Security concept that users should only be granted the minimum level of access required to complete their job duties.
- ***Personally Identifiable Information (PII)*** – 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.
- ***PCI-DSS – Payment Card Industry*** - Data Security Standard established by the major credit card companies which are required to be followed by all organizations taking credit card payments.
- ***Protected Health Information (PHI)*** – Personal health and health-related Information protected by HIPAA or other laws or regulations that require extra levels of security to ensure the information is kept confidentially.

## SECTION IV. DATA CLASSIFICATION

St. Thomas has classified its information assets into the categories of I-Green, II-Yellow, III-Orange, IV-Red for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access.

The university classifies its data and provides access to data on a "need to know" basis as it relates to specific job duties. Wherever practicable, the university assigns access under a "least privilege required" model whereby employees are only granted the permissions needed to perform their jobs and no more. Data security measures must be implemented commensurate with the sensitivity of the Data and the risk to the university if the Data is compromised.

It is the responsibility of the applicable university Data Owner to evaluate and classify Data according to the classification system adopted by the university and described below. If Data of more than one level of sensitivity exists in the same System or Endpoint, such Data shall be classified at the highest level of sensitivity.

The university has adopted the following four security classifications of Data:

| **Category IV. Red**<br><br>Data that includes any information that St. Thomas has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the University to notify the affected individual and state or federal authorities.<br><br>Access to Category IV-Red data will be subject to the highest level of security controls as defined by the Minimum Security Standards. | Examples include, but not limited to:<br><br>• Payment Card Information (PCI-DSS), such as:<br>  ○ Credit or debit card number<br>  ○ Credit card security code (CVV) number<br>  ○ Card magnetic stripe data<br><br>• Protected Health Information (PHI), including any health information about an individual, in combination with Personally Identifiable Information<br><br>• Personally Identifiable Information (PII) that is legally protected against unauthorized disclosure under federal, state or other applicable law, including: |
|---|---|

| | |
|---|---|
| | ○ First name or initial, plus last name, when combined with any of the following:<br>• Social security number<br>• Driver's license number<br>• Other government-issued personal identification number<br>• Bank account number<br>• Date of birth<br>• Passwords<br><br>• Personally Identifiable Information combined with sensitive data, as defined by federal and international law such as the European General Data Protection Regulation (GDPR), including:<br>○ Race and ethnicity<br>○ Religious affiliation<br>○ Trade union status<br><br>• Individually Identifiable Human Subject Research Data, as defined by the University Institutional Review Board<br><br>• Customer Information as defined by the Gramm-Leach-Bliley Act and related regulations<br><br>• Controlled Unclassified Information (CUI) required to be compliant with NIST 800.171 according to Federal government agencies.<br><br>• Unpublished institutional information about patentable inventions, including specifications, schematics, descriptions, lab notebooks, and unfiled patent applications<br><br>• Authentication data used to access university systems or data, including:<br>○ Passwords<br>○ PIN#<br>○ Biometric data |

| | |
|---|---|
| **Category III. Orange**<br><br>Data that, if made available to unauthorized parties, may adversely affect individuals or the business of the University of St. Thomas. This classification also includes data that the University is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor.<br><br>Access to Category III-Orange data will be subject to a high level of security controls as defined by the Minimum Security Standards. | Examples include, but not limited to:<br><br>• FERPA Protected Student Information not covered under Category IV, and not considered "directory information," such as:<br>  ○ Student ID Number<br>  ○ Grades<br>  ○ Test scores<br>  ○ Other education records, such as submitted academic work or correspondence with university employees about a student's educational matters<br><br>• St. Thomas ID numbers for employees and alumni when combined with any other nonpublic personal information.<br><br>• Individual donor information, including:<br>  ○ Gift instruments and other donation-related agreements<br>  ○ Giving history when combined with the donor's name<br>  ○ Anonymous donor information<br>  ○ Alumni donor information when combined with the donor's name or student ID number<br><br>• Employee records not covered in Category IV<br><br>• University contracts<br><br>• Information provided to the university pursuant to a legal contract |
| **Category II. Yellow**<br><br>Data that is proprietary or produced only for use by members of the university community or service providers who have a legitimate purpose to access such data, and that is not subject to legal or contractual data security requirements.<br><br>Data the disclosure of which is unlikely to cause material harm, but which the university has chosen to keep confidential. | Examples include, but not limited to:<br><br>• Data about employees that is not classified as employee records covered in Category IV or III<br><br>• Internal operating procedures and manuals<br><br>• Technical documents such as system configurations and floor plans<br><br>• Unpublished research that does not relate to patentable inventions<br><br>• Internal memoranda, reports, business emails and other documents not containing Red or Orange data and that do not fall into another category |

| | |
|---|---|
| **Category I. Green**<br><br>Public information. Any information that may or must be made available to the general public, with no legal restrictions on its access or use. | Examples include, but not limited to:<br><br>• General information and marketing materials about the university such as press releases, campus maps, athletic results, information about academic program offerings<br><br>• St. Thomas e-mail addresses<br><br>• University reports filed with federal or state governments and generally available to the public<br><br>• Copyrighted materials that are publicly available<br><br>• Student information covered as "Directory information" under FERPA if not restricted by individual student action |

## SECTION V. SECURITY CONTROLS AND APPROPRIATE SYSTEM USE

The Minimum Security Standards will include the required security controls and allowed university systems for each data security classification. These appendices will be updated by ITS regularly to accommodate changes in technology or university processes. Significant changes to these controls will be reviewed by the University Technology Advisory Committee and its security related sub-committee.

ITS will implement technical controls to verify and enforce that university data are being handled in accordance with this policy.

This policy serves to define the classifications for university data. Separate, but related, policies will define data ownership, governance and access to university data.

UNIVERSITY OF St.Thomas

# Appendix A to Data Security Classification Policy

# Data Categorization and Examples

Date of initial publication: June 6, 2017
Date of latest revision: March 2, 2023

| **Faculty / Staff Information** | **Category Level** |
|---|---|
| St. Thomas Email Address | Category I - Green |
| Work Address | Category I - Green |
| St. Thomas Phone Number | Category I - Green |
| Performance Review Information | Category II - Yellow |
| Salary Information | Category II - Yellow |
| St. Thomas ID Number | Category –III - Orange |
| Individual Benefits Elections | Category II - Yellow |
| St. Thomas Account Password | Category IV - Red |
| Social Security Number | Category IV - Red |
| | |
| **Student Information** | **Category** |
| St. Thomas ID Number | Category III - Orange |
| Education Records (excluding Directory Information) | Category –III - Orange |
| Financial Aid and Grant Application Information | Category –III - Orange |
| St. Thomas Account Password | Category IV - Red |
| Social Security Number | Category IV - Red |
| | |
| **Research Information** | **Category** |
| Sponsored Project Contracts or Grants | Category II - Yellow |

| | |
|---|---|
| Published Research Data | Category II - Yellow |
| Unpublished Research Data Unrelated to a Patentable Invention | Category II - Yellow |
| Unpublished Information about Patentable Inventions | Category IV - Red |
| Intellectual Property owned by the university that it has chosen not to patent | Category II - Yellow |
| Individually Identifiable Human Subject Research Data | Category IV - Red |
| | |
| **General Business Information** | **Category** |
| Annual Reports | Category I - Green |
| Organization Charts | Category I - Green |
| Public Websites | Category I - Green |
| Public Relations and Marketing Brochures and Materials | Category I - Green |
| Internal Intranet Websites | Category II - Yellow |
| Email Correspondence | Category II - Yellow |
| University Financial Account Numbers (Org and Index Codes) | Category II - Yellow |
| Travel Reimbursement Forms | Category II - Yellow |
| Credit Card Numbers | Category IV - Red |
| | |
| **Library Records** | **Category** |
| Library Catalog Information | Category I - Green |
| Library Subscription Database Content | Category II - Yellow |
| Interlibrary Loan Records | Category II - Yellow |
| Circulation Records | Category II - Yellow |
| Library Database Usage Data | Category II - Yellow |