ST. LOUIS COLLEGE of PHARMACY

Information Technology
Data Protection Standards - Data Management Guide

Applies to: (examples; Faculty,Staff, Students, etc)

Faculty , Staff , Students , Contractors_Vendors

Policy Overview:

Issued: 11-30-2018

Next Review Date: 03-02-2022

Frequency of Review: Annually

Information maintained by the College is a vital asset that must be available to all employees who have a legitimate business need for it. However, the use of College data for anything other than approved College business is prohibited by College policy and, in many instances, by state and federal law.

Applies to all active members of the College community, including faculty, students, staff, and affiliates, and to authorized visitors, guests, and others for whom College technology resources and network access are made available by the College. This policy also applies to campus visitors who avail themselves of the College's temporary visitor wireless network access, and to those who register their computers and other devices through Conference and Event Services programs or through other offices, for use of the campus network.

Details:

This document is a companion to the Data Classification Policy and defines the roles and responsibilities associated with the distribution and security of College data. As described below, individuals may not access, use or store some kinds of sensitive data without authorization from the appropriate Data Trustee. Individuals who are authorized by a Data Trustee to access, use or store sensitive information must follow any restrictions imposed by the Data Trustee.

Procedures:

Access Request Appeals
If the Data Trustee denies a requests for access to College data, the requestor may appeal the decision to the executive or department head of the unit or department that owns the data (or a designee).

Data and Data Trustees
If you need assistance identifying a Data Trustee, please contact your Departmental Security Administrators (DSAs) as defined below or STLCOP Information Security.

Generally, contact these offices with questions about these data types:
(** These data fields are jointly owned and approval must be granted by all trustees.*)

See Data Trustee List document retained in IT for specific lists of data trustees.

Responsibilities:

Position/Office/Department	**Responsibility**
Data Trustee	The executive or head of each department included in the list of Data and Data Trustees below will designate at least two, but not more than four, Data Trustees. Data Trustees are those persons at the College with responsibility for the accuracy, integrity, and privacy of College data. They grant or deny access to College data, monitor the integrity of the data repositories, and perform regular audits to ensure all approved accesses still valid and appropriate. Data Trustees must make decisions regarding the handling of data in accordance with the College's Information Security Policy and the Data Protection Standards, and in compliance with all federal, state, and local laws and regulations. Data Trustees

	are responsible for reviewing requests for access to sensitive data under their care regardless of whether the data is stored in the original data source, the authoritative repository or with any downstream users of the data. **Data Trustee responsibilities include:** 1. Responding to requests for access to College data within three business days with one of the following decisions: “Accepted”, “On Hold” (requesting more information), or “Denied”. Before permitting access, the Data Trustee must confirm that the requestor has a legitimate business reason for access to the data. 2. Approving the *minimum* access or authorization necessary for the requestor’s needs. 3. Support the implementation of required security measures as outlined in the College Data Protection Requirements. Trustee may consult with IT Department and STLCOP Information Security to determine appropriate controls. 4. Working with other Data Trustee’s and the DSA of the department to identify the department’s need to store or access Confidential and Restricted Use data. 5. Assisting with the data classification process and coordinate with the STLCOP Information Security Team. 6. Assisting with security awareness for the unit or departments. 7. Requesting that access be removed when no longer required due to termination or job reclassification on campus. When an individual becomes a Data Trustee, the executive or department head should ensure that he or she receives a written description of his or her duties as Trustee and receives the appropriate training. (The Trustee duties list, manual and training are maintained and provided by STLCOP Information Security.) The Data Trustee must acknowledge the responsibilities by signing and returning a copy to the executive or department head and to STLCOP Information Security. In the event a Data Trustee is unavailable to fulfill the responsibilities above, the executive or department head must designate an alternate until the Data Trustee is again available.
Departmental Security Administrators (DSA)	Each unit or department’s executive or department head will be designated as the DSA. DSAs will act as liaisons to the STLCOP Information Security Team. DSAs oversee data security responsibilities at the department level. DSA responsibilities include: · Identifying where sensitive information is stored and communicating that to the STLCOP Information Security Team. · Conducting regular reviews with their department (not less than one time per year) of access lists and requesting removal of access when no longer needed. · Communicating to the Security Incident Response Team in the event of any unauthorized disclosure, modification, or loss of Confidential or Restricted Use data. · Assisting with security awareness for the unit or departments DSA’s should uphold data security in their respective departments by ensuring that employees are storing and access data by secure STLCOP approved means. DSA’s will work with STLCOP Information Security Team members as needed to communicate security data storage needs and report on where sensitive data is being stored.
STLCOP Information Security	Members of the STLCOP Information Security Team support enterprise data management by providing certain functions and processes centrally.

	Information Security responsibilities include: · Coordinating with General Counsel to communicate changes in applicable law that impact the responsibilities of the Data Trustees, Data Security Administrators and Data Custodians. · Maintaining and publishing data management and protection standards, with appropriate input and approval. · Providing training to Data Trustees on tools and processes to conduct reviews of the access to data for which Trustees are responsible. · Maintaining the list of DSA responsibilities and processes; maintaining the DSA manual. · Providing training for DSAs. Training should be refreshed on an annual basis. · Receiving and processing access requests from DSAs for designated systems. · Define and provide secure methods for clients to access Confidential and Restricted Use data. Where an appropriate method does not exist, provide consulting on the development of new solutions or compensating controls.
Data Custodian	Data Custodians are those persons primarily responsible for maintaining security and integrity of College systems on which College data resides. The Data Custodian's "clients" are people or systems that access or use the data or systems which the Data Custodian maintains. Data Custodian responsibilities include: 1. Providing data or access to data only as approved by the Data Trustee. 2. Assisting clients or project teams with the submission of requests for access to College data. If a Data Trustee has previously approved access to the data using one format or method, the Data Custodian need not get a new approval for a different format or method. For example, if access via spreadsheet or database is approved and the client would like it in a text file instead, this change does not require re-approval by the Trustee. Similarly, as long as the data is being transported using a mechanism approved by STLCOP Information Security, changing from one to the other does not require re-approval. For example, switching from SFTP to FTP-S as the secure transport mechanism. 3. Removing of access when requested by the DSA. 4. Conducting regular reviews (not less than one time per year) of access lists and removing access when no longer needed. 5. Work with clients regarding new software request, integrations points, maintenance, and asset storage methods. (i.e. on premise vs cloud) A new Data Custodian's manager should ensure that the new Custodian receives a written description of his or her duties as Custodian and receives the appropriate training. The Custodian must acknowledge the responsibilities by signing and returning a copy to his or her manager.

Resources:

Data Protection Standards policies

Digital Millennium Copyright Act Policy

Data Trustee List maintained by IT

Policy Contacts:

Name	Contact Information
Lewis, Zachary, Director IT	Zachary.Lewis@stlcop.edu, 314-446-8402
Knoll, Eric, Vice President Operations	Eric.Knoll@stlcop.edu, 314-446-8375