ST. LOUIS COLLEGE of PHARMACY

Information Technology
Data Protection Standards - Minimum Security Standards

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

Faculty , Staff , Students , Contractors_Vendors

Policy Overview:

Issued: 11-30-2018

Next Review Date: 03-03-2022

Frequency of Review: Annually

Protecting College Data is a shared effort. Individuals with access to College Data are responsible for accessing, storing, and processing data on systems that have appropriate security controls in place for the class of data. Individuals should consult with the IT Department to determine the best way to access, store, and use their data, particularly for more sensitive data.

This document defines the minimum security standards required for any Electronic Device (defined below) or cloud service that may be used to access, store or process (input, output, transmit, receive, display, calculate, etc.) Sensitive Information (defined below) owned or used by the College. More specific security standards may be established unde other College policies and applicable laws and regulations.

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.

Definitions:

Term	Definition
College Data	Information generated by or for, owned by, or otherwise in the possession of STLCOP that is related to the College's activities. College Data may exist in electronic or paper form and includes, but is not limited to, all academic, administrative, and research data, as well as the computing infrastructure and program code that support the College.
Sensitive Information	College Data that is classified as Internal, Confidential, or Restricted Use. See the Data Classification Policy for definitions and examples of each of these classifications.
Cloud Services	Any free or paid application, tool, or infrastructure made available by third parties wherein computing or storage resources are accessed via the Internet.
Electronic Device	Any device that is used to access, store or process data electronically. For example: a computer of any type (including a smart phone or iPad), a data storage device (including a USB device), a network device, a printer or copier that contains a storage device or that may be connected to a network.
Encryption	The process of converting human readable data (plain text) into data that cannot be read (cipher text) without knowledge of a specific secret (a key). There are two types of encryption referenced in this document: encryption in transit and encryption at rest. Encryption in transit refers to ensuring that all data sent over a network is encrypted, where encryption at rest refers to ensuring that all data written to disk or other permanent storage is encrypted. While the encryption process and outcome may be the same, the tools and methods for achieving each type of encryption are different.

Details:

The data handling protections outlined in this document apply to all Electronic Devices and Cloud Services (defined below) used to access, store, or process Sensitive Information whether owned by the College or by a College employee or consultant and used to do College business. The use of an Electronic Device you own (referred to herein as a “Personal Electronic Device”; for example, a home computer, smart phone, or tablet) to access, store or process Sensitive Information, is prohibited. If you choose to use a cloud service that you have set up yourself (referred to as a “personal cloud service”; i.e., a service that has not been provisioned by the College), use of the service to access, store or process Sensitive Information belonging to STLCOP is prohibited. (Examples of such services: Dropbox, Google Drive, Box, GMail)

The Payment Card Industry Data Security Standards (PCI-DSS) includes more stringent requirements for systems handling credit card data than described herein. If you are handling credit card data in any way, please contact the IT Department to ensure that your systems meet the PCI-DSS requirements.

Please refer to the Identity Theft Prevention Program Policy for information about procedures pertaining to identity theft and the Red Flag rules.

Systems that handle Protected Health Information (as defined under the Health Insurance Portability and Accountability Act (HIPAA)) are subject to HIPAA and must comply. Please consult with the Information Security Team if you have questions about the use of HIPAA data in our environment.

Procedures:

Roles

Enterprise Services
The IT Department is responsible for ensuring compliance of IT Department supported devices and services with this policy. The IT Department will provide guidance about the approved data classifications for each service.

Schools, Department, and Offices
The IT Department is responsible for ensuring that the devices and services they provide to the College meet these minimum security standards, including specifying whether services are appropriate for each class of data.

Personal Responsibility
All STLCOP faculty and staff are expected to be familiar with the Data Management Guide, Data Protection Requirements and Minimum Security Standards to ensure understanding of how to handle Confidential or Restricted Use information properly.

If you use a personal Electronic Device or a personal cloud service, you are responsible for ensuring that your Electronic Device and/or personal cloud service meet the requirements below and is not used to handle or store sensitive STLCOP data.

If you have questions, ask your supervisor, Departmental Security Administrator, or IT Department.

Restricted Use Data Registry

All services that collect, store, or provide Restricted or Confidential use data by design must be approved by the Information Security Team. All new services that collect, store, or provide Restricted or Confidential Use data must be approved by Information Security Committee.

Business Standards

Risk Based Controls

- Kiosks and terminals intended for unauthenticated public use should not store any Sensitive Information.
- Restricted Use or Confidential data should only be stored on devices that are owned by the College or approved for such use the IT Department.
- Systems storing Confidential or Restricted Use data should be managed by a designated, qualified Data Custodian who is capable of properly meeting the configuration requirements or deploying and confirming appropriate compensating controls.

Systems Management

- Procedures should be in place for coordinating downtime with stakeholders on short notice to deploy critical security patches, particularly for server systems.

Cloud Services

Cloud Services include any free or paid application, tool, or infrastructure made available by third parties wherein computing or storage resources are accessed via the Internet. The use of Cloud Services with College Data is governed by the Conditions of Use Policy, the Minimum Security Standards (this document) and other relevant College policies and procedures.

The following standards apply to the use of Cloud Services provided by or arranged for by, the College:

1. Services that will access, store or process Confidential or Restricted Use data should be evaluated by a Data Custodian and the appropriate Data Trustee before use.

2. Cloud Services must provide an exit strategy that enables the College to retain its data and to remove all data from the cloud service.
3. The cloud provider must not mine, search, or index College Data for purposes other than those approved by the College.
4. Cloud providers that will store Confidential or Restricted Use data must document and contractually agree to implement strong physical access controls for their infrastructure.
5. Cloud service providers that will store Confidential or Restricted Use data must verify security with a SOC2 Type 2 report.
6. The unit procuring the cloud services must understand where and how cloud services store data, including specific countries that data is, or could be, stored, replicated to, or routed through. Other countries may have requirements concerning access to data stored in or crossing their borders.
7. Cloud Services must implement access controls to ensure that data is not accessed by unauthorized users. For some Cloud Services this may include removing public/global read/view access.
8. The cloud provider must log all authentication attempts to provided services and be able to export the data if requested.
9. Restricted Use data must be encrypted at rest; other data should be encrypted where reasonable to do so.

Personal Cloud Services used for College Data

"Personal Cloud Service" is a subset of "Cloud Service" where the service is arranged for by an individual rather than the College for storing College Data, including the use of free services. Examples: Google Docs, Box, Dropbox

1. Restricted Use or Confidential data should not be stored in Personal Cloud Services unless the service has been approved by the Information Security Team and the appropriate Data Trustee.
2. You must read and understand the terms of use, including whether the provider has access to your data and what it can do with the data. For example, the regular consumer version of Gmail scans your emails looking for keywords to better target advertising toward you, while STLCOP's O365 email does not.
3. Understand how your data is protected, where (geographically) it is stored and how you might be able to get it back and erase the cloud copy in the event that you stop using the service.
4. Do not use your STLCOP password for Personal Cloud Services or any personal use services. (Bank Accounts, Amazon, personal email)

Endpoint Devices

An endpoint device is a system that is intended for direct human interaction. By comparison, a server is intended to offer an application, storage, or other service and while it may be used directly by a human such use is not the norm. In some cases, both sets of standards may apply, and the more stringent standard should be used.

Note: If you are using an Electronic Device that you cannot configure or for which you cannot confirm is securely configured (such as a public kiosk computer or a computer in a hotel, for example), that device should not be used to conduct STLCOP business. Only devices managed by the IT Department should access Restricted Use, Confidential or Internal data.

Endpoint devices must meet the following requirements:

1. Use an operating system that is supported by a company who updates the operating system when security vulnerabilities are discovered. For mobile devices such as smart phones and tablets this includes not using devices for which security controls have been intentionally subverted by the end user, such as a "jail broken" or "rooted" operating system. Please refer to the Conditions of Use Policy for information on hacking devices.
2. Setup to received updates from STLCOP managed update servers.
3. For mobile devices, use the native app store to download and install operating system and application updates automatically.
4. Unless mobile device updates are being managed by the IT Department, configure devices to be updated within 2-3 days of a patch being released.
5. Where business requirements prevent running fully updated software it may be necessary to deploy compensating controls. Consult with the IT Department for these cases.
6. Strong password will be enforced from the IT Department.
7. Use biometric authentication (thumbprint, facial recognition, etc.) or set a strong PIN (alphanumeric), passcode, password or pattern on mobile devices. Many protections and security features of your phone (for example, the native encryption capability of the iPhone) are not activated unless you have turned on this security feature.
8. Lock screens will be enforced by the IT Department.
9. Antivirus must be installed by the IT Department.
10. Information that is critical to the business of the college should only be installed on STLCOP managed devices.
11. If connecting from an off-campus location, establish a VPN or encrypted connection before accessing any Confidential or Restricted Use data via the network. This must only be done from your issued STLCOP computer.
12. Electronic Devices that support it, will have the capabilities to be remotely wiped in the event they are lost or stolen.
13. All wireless connections must use strong encryption-WPA2 or equivalent or better- such as is offered by STLCOP EuTecNet wireless network or by using a VPN over a wireless network.

Non-Endpoint Devices

This section contains detailed security requirements for all devices and services run or arranged for by the College, including but not limited to by the IT Department.

1. Vendor supported operating systems and applications should be used to store or process data, and must be used for storing or processing Confidential or Restricted Use data. Non-supported operating systems should not be used. For already deployed systems that cannot be upgraded, compensating controls must be in place and approved through the Risk Acceptance Process.
2. A patch management program, security-related patches and updates must be applied to servers within 30 days.
3. Any default or vendor-supplied password must be changed to a non-default value.
4. System/Device based firewalls should be used where it is reasonable to do so, are recommended for systems with Confidential data, and required for systems with Restricted Use data.
5. Data that is important to the operations of the College should be backed up to protect against loss of use.
6. Sensitive Information should be encrypted in transit where it is reasonable to do so using VPN, SSL, or similar technologies. Encryption in transit is strongly recommended for Confidential data and required for Restricted Use.
7. All authentication attempts to operating systems and applications, both successful and failed, must be locally logged.
8. On multiuser devices, file system access controls should be implemented to ensure that data is not accessed by unauthorized users. Systems used to process or store Confidential or Restricted Use information should not host any unauthenticated service that allows access to browse the file system, such as anonymous ftp or directory indexing via a web server.
9. Servers storing significant quantities of Confidential data or any Restricted Use data should be kept in secure rooms with strong physical access controls. Two factor physical access controls and video surveillance of these areas should be considered.
10. Restricted Use data must be encrypted at rest; other data should be encrypted where reasonable to do so, preferably using technologies like whole disk encryption that is native to the operating system.
11. Reusable media (disk drives) should be securely erased when removed from service. When Restricted Use data is involved, failed media that is not encrypted (even if under warranty) cannot be returned to the manufacturer if it cannot be wiped. These drives must be destroyed.
12. Systems should be routinely scanned for vulnerabilities and discovered vulnerabilities should be remediated swiftly.
13. Network-accessible systems that contain Restricted Use information from multiple individuals should require two-factor identification where technically practicable, including access by individuals to their own data.
14. Anti-virus software should be installed and tied to enterprise management and reporting utilities.
15. Network services that do not have an associated business need should be disabled.

Exceptions

Information Security is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and the implementation of appropriate compensating controls.

In addition, Information Security may publish directives aimed at clarifying the intent of a standard to aid in the interpretation of this policy.

Important

Failure to comply with the Data Protection Standards may result in harm to individuals, organizations or the College. The unauthorized or unacceptable use of College Data, including the failure to comply with these standards, constitutes a violation of College policy and may subject the User to revocation of the privilege to use College Data or Information Technology or disciplinary action, up to and including termination of employment.

Responsibilities:

Position/Office/Department	Responsibility
All computer and infrastructure users	Abide by Minimum Security Standards

Resources:

Digital Millennium Copyright Act Policy

Payment Card Industry Data Security Standards (PCI-DSS)

Identity Theft Prevention Program Policy

Health Insurance Portability and Accountability Act (HIPAA)

Data Protection Standards policies

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