Securing College Data

This document is intended to provide guidelines to safeguard Protected and Confidential Data (PCD). All employees are expected to know and adhere to the policies that safeguard digital information and data in order to comply with state and federal regulations, as well as College policies.

Assignment of Information Security Liaison
Each office, department, or division that has access to Protected or Confidential Data (PCD) shall appoint an individual to serve as the Information Security Liaison. This individual is responsible for managing the access to Protected and Confidential data and ensuring that PCD within their office area is maintained in compliance with State and Federal regulation and College policy. This individual shall be responsible for determining the need for and coordinating access to PCD for individuals within their respective office. The Security Liaison will conduct an annual audit and review of their respective area for:

- Physical security. (Require a use of locked file cabinets, locked offices, etc.)
- Employee training
- Use of encryption for electronic transmission of protected or confidential data
- Annual review with employees of incident response and reporting program
- Proper disposal methods used to destroy protected or confidential information.

Employee Responsibilities
Individuals who are given rights to access or use college data are responsible for maintaining the privacy of PCD. An individual granted access to PCD agrees to abide by College policy and state or federal law and regulations governing access to, use, and protection of such data. All individuals with access to PCD shall be required to complete annual training in order to retain access to PCD, network and computer access to Knox resources. New employees shall be required to complete training within 30 days of beginning work at Knox. Failure to comply with training requirements shall result in immediate suspension of network and computer access to Knox resources.
In order to maintain security of the College's data and information the college retains the authority to:

1. restrict or revoke any user's privileges,
2. inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and
3. take any other steps deemed necessary to manage and protect its information systems and the data and information held within those systems.

This authority may be exercised with or without notice to the involved users. Knox College disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

Procedures

Inventory of Protected and Confidential Data
Offices and departments that store or process Protected or Confidential data shall document and provide an annual report of the data they have access to, individuals in their respective areas that have access, provide a risk assessment, and summary of business processes and associated security safeguards to the chairperson of the Information Systems Council on or about August 1st. The chairperson of the Information Systems Council shall deliver an annual report and inventory of Protected and Confidential Data to the Chief Information Officer annually, on or about October 1st.

File and Information Privacy
All information residing on, provided by or derived from Knox resources , on Knox servers, computing and server resources an under contractual obligation to College, desktop or laptop computers , mobile devices, electronic or optical storage media is considered College property.

Individuals accessing Knox systems and networks from any device consent to the monitoring and auditing of their activities in the course of systems maintenance or security related investigation as prescribed in the Knox College Policy for Acceptable Use of Information Technology Resources. In order to conduct the College's business and assure compliance with College policies and the law, the College may need to monitor or review digitally stored information. If such monitoring reveals possible evidence of criminal activity, the College may provide it to law enforcement.

Cloud Storage and Computing Services
The Internet is sometimes referred to as the “cloud” and “cloud computing” is the array of Internet-based services, often available to the public, for gathering, storing, processing and sharing information. Some cloud services, such as those offered by Apple or Google, may be free to end-users. For the general user who wants a convenient, Internet-based solution for storing or sharing personal information, cloud computing may provide a reasonable option. College information **must not be stored, shared, or otherwise processed** by a cloud computing service unless the service enters into a legally binding agreement with Knox College to protect and manage the data according to standards and procedures acceptable to the College. If you are unsure if a service has a relationship with Knox College contact Information Technology Services.

Should you ever need to store or share Knox information in a manner that is not currently provided by Knox, contact Information Technology Services and an attempt will be made to devise or procure a solution that will meet this need.

Data Storage Guidelines

The table below provides guidance on various classifications of digital information and permissible locations where it may be stored. Policy and Guidance for secure storage of physical documents and information is delegated to the security liaison overseeing the functional area.

	Protected Information	**Confidential Information**	**Public Information**
Knox Sponsored Cloud Services	**x**	**x**	**x**
Knox Departmental Disk and Document Storage	**x**	**x**	**x**
Knox Provided Personal Computer		**x**	**x**
Personal equipment and Mobile devices			**x**

Examples of Knox Sponsored Cloud Services are Google Drive, Slate, CSO, and other similar cloud based services to which Knox has a formal contractual arrangement for services. Knox Departmental Disk and Document Storage are servers provided by Knox College Information Technology Services that are available on the Internet or campus network. These systems include the Jenzabar CX and JX systems, the Knox Department File Server (departments.knox.edu) and the Knox Docushare Server (docushare.knox.edu). Knox provided personal computers furnished by the College to employees. These may be either desktop or laptop devices computing devices. Personal equipment and mobile devices should not be used to store Protected or Confidential information. These devices may use other services to access Protected and Confidential information. Smartphones, tablets and computers used to access College data from home are examples of this type of equipment.