Knox College Information Security Policy

Policy Coordinator: Steven S. Hall
Vice President for Information Technology Services and Chief Information Officer

Purpose of Policy
Information and information systems are critical college resources and assets. Knox College has adopted these information and computing policies to safeguard the College's constituents, investments, to preserve the confidence and goodwill of the Knox Community and to comply with state and federal law.

Policy
The protected data and information maintained by the College must be handled and managed in accordance with state and federal law and College policy. All employees are expected to know and adhere to this policy and other policies and procedures incorporated by reference. Violations may lead to revocation of system access privileges and/or disciplinary action including termination of employment.

The use of any Knox College data or information, in any format, for any purpose other than conducting College business is strictly forbidden. Unacceptable uses include sharing the data with groups, organizations, or activities that are not College sponsored or approved, use of data for personal gain, use of data to satisfy personal curiosity, removing data or reports from the campus except in the required performance of College duties, or use by individuals outside of their normal job responsibilities.

Procedures
Knox College utilizes access controls, audit records, and other physical and technical security measures to protect the confidentiality, integrity, and availability of the College's information. Information can be stored and transmitted in a variety of ways, including but not limited to email, portable electronic storage devices, paper files, audio or video files, fax, telephone, and interpersonal communications. The College owns all data, produced, stored, or processed by information systems owned or operated by or on behalf of the college. While the College maintains ownership of data, individual operating units or departments may have stewardship responsibilities for particular portions of that data or data sets.

Employees who access or create data and information must follow guidelines and procedures for Securing College Data. Whenever possible, paper files should not contain protected or confidential data. When it is absolutely necessary, paper files must be attended or kept in a secured, locked area and disposed of properly (shredded) when no longer required. Protected or confidential data should not be taken off campus without permission of the assigned area's information security liaison. When taken off campus it should be never be left unattended. If absolutely necessary to leave in a vehicle, it must be secured in the trunk or locked compartment inside the vehicle.

Notifications for Data Breach of Personal Information:
Illinois Personal Protection Act **(815 ILCS 530)** requires that *"Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system."*

The law defines "personal information" as:
"an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements is not encrypted:

1. Social Security number;
2. driver's license number or state identification card number; or
3. account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
4. Medical Information.
5. Health Insurance Information.

OR

6. A username or e-mail address, when in combination with a password or security question and answer would permit access to an online account…"

If an employee of Knox College has reason to believe personal information *or any other type of protected or confidential data* may have been been improperly disclosed, the steps in this Data Incident Response Plan should be followed immediately.

Types of Protected or Confidential Data:
Knox College classifies data into three categories:

Protected:
The unintended disclosure of Protected Information may cause the College to become subject to litigation, fines, substantial financial harm, the inability to participate in some federal and state sponsored programs, and severe or irreparable harm to the reputation of the institution. Protected data is defined, its appropriate use, and standards for protection are delineated by state and federal regulations such as FERPA, HIPAA, GLBA, Illinois Personal Protection Act and others. Data elements in this group include, but are not limited to, Personal Information, social security numbers, student ID numbers, credit card numbers, medical information, bank account numbers, grades, date and/or location of birth, drivers license information, ACH (automated clearing house) numbers, tax return information, credit rating, income history, loan payment history, passport information, and coursework.

Confidential:
The unintended disclosure of Confidential data may result in harm or embarrassment to an individual, group of individuals or the College. This data is not protected under state or federal regulations. However, Knox College has determined that this information be private and be accessed only by those with authorized access and a business reason to access it. This data may include employee evaluation data, salary information, employee ID numbers, review files, or statistical studies of Knox College constituents that has not been sufficiently disaggregated so as to prevent the discovery of the identity of those in the study sample.

Public Data:
This data that is created and maintained by the College that may be disclosed to the public.

Other Related Knox College Policies, Procedures, Federal Regulation for Protected or Confidential Data:

Securing Campus Data
Office Responsible: Information Technology Services
Program Coordinator: Mike Cokel, Systems Administrator
Summary: Knox guidance for protecting electronic information and account access

Gramm-Leach-Bliley Act (GLBA)
Office Responsible: Finance and Administrative Services
Program Coordinator: Bobby Jo Mauer, Controller
Summary: To protect consumer information from threats in security and data integrity.

Family Educational Rights and Privacy Act (FERPA)
Office Responsible: Registrar's Office
Program Coordinator: Chuck Schulz, Registrar
Summary: Educational Institutions must grant and protect certain rights relating to educational records.

Health Insurance Portability and Accountability Act (HIPAA)
Office Responsible: Human Resources
Program Coordinator: Crystal Bohm, Associate Vice-President for Human Resources
Summary: To protect the privacy of personal health information

Payment Card Industry Data Security Standards (PCI DSS)
Office Responsible: Finance and Administrative Services
Program Coordinator: Vicki Trant, Information Coordinator
Summary: Anyone who processes credit card payments must follow laws set by credit card companies.

Fair and Accurate Credit Transactions Act (FACTA)/Red Flag Rules
Office Responsible: Finance and Administrative Services
Program Coordinator: Bobby Jo Mauer, Controller
Summary: We must be able to detect red flags for identity theft in instances where we issue credit.

Copyright Laws
Office Responsible: Dean of College
Program Coordinator: Laura Behling, Vice President for Academic Affairs and Dean of the College
Summary: All employees of the College are expected to follow laws that protect copyrights.