KASKASKIA COLLEGE

INFORMATION SECURITY POLICY

Board Bylaw:
Policy Number: 2.4000
Subject Area: General College Policies/Administration
Adopted: 05/18/2020
Revised: 09/24/2024

Introduction

The primary goal of Kaskaskia College's (KC) Information Security Policy is to ensure that all Confidential and Sensitive Information (CSI) maintained by the College is protected in a manner that follows all relevant legislation, industry best practices, and the College's values.

Other goals of the Information Security Policy are to:

- Define what information is considered to be confidential and sensitive.
- Define what information is considered to be public.
- Outline employee responsibilities when working with CSI.
- Provide a process for reporting security breaches or other suspicious activity related to CSI.
- Provide guidelines on how to communicate information security requirements to vendors.
- Summarize the laws and other guidelines that impact the Information Security Policy.

2.0 Information Security Program Coordinator

The Chief Information Officer (CIO), or their designee, is the coordinator of the Information Security Program at Kaskaskia College. The CIO, or designee, is responsible for working with Administrators from all areas of the College to implement information security practices in accordance with all legal requirements and industry best practices. The CIO reports to the President of the College. The President reports to the Kaskaskia College Board of Trustees. The Kaskaskia College Board of Trustees is ultimately responsible for all of Kaskaskia College's policies.

3.0 Purpose of The Information Security Policy

The purpose of the Information Security Policy is to define the guiding principles that all College employees must follow when working with Confidential and Sensitive Information. Each department that works with CSI will be required to implement department-specific procedures to ensure that they operate within the guidelines.

4.0 Classification of Information

Kaskaskia College owns or is entrusted with a vast amount of information about its students, employees, and other business partners. This information may be in electronic form, stored on network servers, PC workstations, or magnetic or optical storage media. It may also be in hard copy (paper) form stored in file cabinets.

4.1 Confidential and Sensitive Information (CSI)

The following types of information are considered by Kaskaskia College to be Confidential and Sensitive Information*:

- Social Security Number (SSN)
- Social insurance number (Medicare number)
- Date of birth
- Driver's license number
- Customer identifiers
- Debit/Credit card number (Personal account number, Expiration date, CVV code)
- Bank account numbers
- Tax ID
- Passwords
- Medical records
- Doctor names
- Insurance policy information (Insurance claim information)

* While all of these items are explicitly considered to be CSI, there may be other items which rise to the level of CSI.

4.2 Public Information

Public information, often called “Directory Information,” may be shared with the general public. Students wishing to have their Directory Information withheld from the public must submit a written request to the Registrar, and Employees must submit a written request to HR. Kaskaskia College considers the following information to be Directory Information:

- Student Name
- Enrollment Status (Full-time, Part-time)
- Major Field of Study
- Classification (freshman or sophomore)
- Dates of Attendance
- Degrees and Honors Earned and Dates
- The most previous educational agency or institution attended prior to enrollment at Kaskaskia College
- Participation in an officially recognized activity or sport and weight, height, and photos of members of athletic teams or student activities
- Photo

5.0 Responsibilities

- Classification of information/data for which person/person’s is responsible accordingly.
- Maintain “Principles of Least Privilege” to data.
- Do not divulge, copy, release, sell, loan, alter, or destroy any college information without appropriate business purpose and authorization.
- Protect the confidentiality, integrity and availability of college Information in a manner consistent with the information's classification.
- Handle information in accordance with the applicable State and Federal laws for Illinois, and Policies and Procedures for Kaskaskia College.
- Safeguard any physical key, key codes, applications, passwords, ID card, computer account, user account, or network account that allows one to access college Information.
- Discard media containing Kaskaskia College information in a manner consistent with law including hard copies, electronic, magnetic, optical, and disk storage.
- Contact the appropriate Kaskaskia College office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

6.0 DILIGENCE

6.1 Concerning Credit Card Information

Kaskaskia College accepts credit card and debit card payments for tuition, donations, and other financial transactions. Any merchant that accepts credit card payments is subject to the security requirements outlined in the Payment Card Industry Data Security Standards (PCI-DSS). All KC employees who work with credit card transactions must adhere to security requirements expressed in the KC PCI Compliance Policy. These requirements include but are not limited to the following: Electronic Storage standards, Electronic Transmission standards, Hard Copy Storage standards, and Transportation and Destruction standards.

6.2 Identity Theft

The Red Flags Rules of the Fair and Accurate Credit Transactions Act of 2003 (FACTA) require financial institutions to implement procedures to detect, prevent, and mitigate potential identity theft incidents. Procedures required to comply with the Red Flag Rules are outlined in the Kaskaskia College’s Identity Theft Pursuant to Red Flags Rule policy & procedure.

6.3 Family Educational Rights And Privacy Act (FERPA)

The Family Educational Rights and Privacy Act, more commonly known as FERPA, is a federal law that declares the rights of students to view their personal educational records while protecting their privacy. This law applies to all public and private institutions that receive funding from the U.S. Department of Education. In short, failure to comply with FERPA regulations has both legal and funding implications for the College. Specific guidance to the application of FERPA guidelines at Kaskaskia College is covered in the Privacy of Student Records policy (FERPA policy), including student information maintenance and personally identifiable information.

7.0 Vendor Agreements

When negotiating contracts with third-party vendors, Kaskaskia College employees must consider whether or not the vendor will need access to any of the College’s CSI. Any vendor that will have access to CSI will be required to abide by this Information Security Policy and any subsequent procedures. Contract language must include acceptance of the Information Security Policy. In cases where vendors will provide services directly related to Confidential and Sensitive Information, they will be required to provide proof of their compliance with all applicable laws.

Pre-existing contracts with vendors should be reviewed as they need to be renewed. The reviewer will then follow the indications above for that contract renewal. Non-acceptance of this policy language by the vendor will prompt consultation with College legal counsel for appropriate next steps.

8.0 Updating the Information Security Policy

The Information Security Policy will be reviewed by the CIO and a working group comprised of appropriate employees per the institutional policy review calendar. If circumstances arise that require significant changes to the policy, it may be reviewed and updated more often.

9.0 Training and Communication

The CIO, Information Technology, and Human Resources are responsible for managing annual information security practices training for all Kaskaskia College employees. This training will inform employees of their responsibilities when working with CSI, safe data practices at Kaskaskia College, and policy changes.

Additional training will be provided to employees whose primary job duties require them to work with CSI. The department head will be responsible for procedural training regarding CSI specific to a particular department.

5.0 Definitions

- **Authorization**: involves determining a person's access rights to information or tasks.
- **Availability**: ensures that information is accessible and usable when needed.
- **Confidentiality**: involves maintaining the privacy and secrecy of information.
- **Integrity**: ensures that information remains accurate, complete, and consistent.