INFORMATION SECURITY POLICY

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

1.0 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 values of the College.

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) is the coordinator of the Information Security Program at Kaskaskia College. CIO 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. CIO reports to the Vice President of Administrative Services (VPAS) of Kaskaskia College, who reports to the President of the College. The President reports to Kaskaskia College Board of Trustees. The Kaskaskia College Board of Trustees are ultimately responsible for all policies of Kaskaskia College.

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 are operating within the guidelines.

4.0 TYPES 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)

CSI can be found in many places at Kaskaskia College. Records containing this information may be referred to as "Covered Accounts". The following are some of the primary locations for CSI:

- Student records – Colleague
- Student records – ImageNow
- Student records – Paper
- Employee records – Colleague (HR, Payroll)
- Employee records – Paper (HR, Payroll)
- Student payment/billing information (credit card, bank account number)

- KC financial accounts (checking/savings accounts, investment accounts, credit/debit card accounts)
- Medical records (employees and students)

*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
- Address
- Phone Number
- 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 officially recognized activity or sport and weight, height and photos of members of athletic teams or student activities
- Photo

5.0 RESPONSIBIITIES

5.1 Employee Responsibilities

Most KC employees will come in contact with CSI at some point while performing their job duties. While some employees will work with CSI more often than others, all employees need to be aware of their responsibilities when handling CSI.

- Employees may not divulge, copy, release, review, or destroy any CSI unless properly authorized as part of their official job duties.
- Properly authorized employees must destroy CSI that is no longer needed. This includes shredding documents and having digital storage devices permanently erased.
- Employees must protect CSI regardless of its location or format (electronic or paper).
- Employees must safeguard all types of access (i.e., keys, ID cards, and passwords) to CSI.
- Employees are required to report any suspicious activity regarding CSI to their supervisor as soon as possible.
    - The supervisor will then report the activity to the CIO who will document the occurrence and with the VPAS, prepare any response action.

5.2 Administrator Responsibilities

In addition to the employee responsibilities stated above, College administrators have additional responsibilities regarding the use of CSI in their respective departments. College administrators are required to:

- Know what types of CSI are available in their department.
- Develop procedures that support safeguarding CSI in their department as outlined in this policy.
- Ensure employees are trained on departmental procedures and are following them.
- Report any suspicious activity regarding CSI to the CIO or VPAS

6.0 DILIGENCE

6.1 Diligence Concerning the Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) has two rules that impact financial institutions; the Privacy Rule and the Safeguards Rule. Colleges and universities are considered to be financial institutions under GLBA. Colleges and universities are considered to be compliant with the Privacy Rule if they are compliant with FERPA (see section 6.4). In order to be considered compliant with the Safeguards Rule, financial institutions must:

- Conduct ongoing risk assessments of all areas of operation where CSI is used.
- Design and implement a safeguards program to protect all CSI owned or entrusted to the College. This includes regular monitoring of these safeguards.
- Select appropriate service providers when those service providers work with the College’s CSI.
- Regularly evaluate and adjust the Information Security Program in light of changes in the College environment.
- Provide ongoing training to employees on the proper handling of CSI.

6.1.1 Mitigation of Risks

Kaskaskia College continuously assesses the potential risks (internal and external) to its Confidential and Sensitive Information. The College has taken the following steps to mitigate these risks:

- A network firewall has been implemented and is continuously monitored and adjusted.
- Endpoint Antivirus/Malware Protection software is running on all workstations and servers and is regularly updated. Monitoring and updates are controlled through a cloud-based service.
- Operating System updates are performed monthly on all server and workstation operating systems as well as applications installed campus-wide.
- An enterprise spam filtering software solution is in place to drastically reduce the amount of spam e-mail that enters the College’s e-mail system.
- Administrative access is restricted on workstations located in public/shared areas.
- File level access rights are controlled on all network shared drives. File shares are available as follows:
    - H: drive – user’s home directory. Only the user has access to this share.
    - S: drive – departmental and group shared folders

Note: System Administrators have access to all file shares on all servers.

- Employees are required to change their password every 90 days using Microsoft's complex password requirements.
- A self-service password reset tool located at https://password.kaskaskia.edu is used by students and employees to change their own password from on-campus or off-campus.
- Off-campus access to Kaskaskia College network resources is limited to Cisco's Virtual Private Network (VPN) software, SharePoint, and/or the myKC.kaskaskia.edu portal.

Employee Data Retention

Upon employee severance, whether through voluntary separation, retirement, or termination a digital backup of employee specific data will be retained. The backup shall contain at least the following data sources:

- Email Archive
- Network Storage – "Home Directory"
- This backup will be made in the following forms:
- Physical media storage onsite in a secure location for at least 1 year
- Server based backup (e.g. cloud based) offsite for at least 7 years.

6.2 Diligence 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 that 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 in sections 6.2.1, 6.2.2, 6.2.3:

6.2.1 Electronic Storage

KC does not store any cardholder data electronically. Cardholder data includes:

- The Primary Account Number (PAN) – 16-digit credit card number on the front of the card.
- The expiration date of the credit card.
- The service code, Card Validation Code, or value (CVC, CVC2, CVV2, etc.) – the 3-digit number found on the back of the card used for on-line transactions.
- Personal Identification Number (PIN) – the number used for ATM transactions.
- Any magnetic stripe information – which includes all of the above information.

Employees must never enter cardholder data into any electronic software system such as Colleague or any other type of database, spreadsheet or other electronic file. Credit Card data may not be stored on any laptop computer, any mobile device, any removable storage media such as a thumb drive, any office or public workstation, or any network drive.

6.2.2 Electronic Transmission

Kaskaskia College does not electronically transmit credit card information over its data network.

- All on-line credit card transactions are handled by a third-party service provider. These providers are responsible for providing a secure web site to handle the transactions as well as storing the credit card data securely.
- All "card present" transactions are handled using stand-alone terminals connected to analog phone lines or certified PCI compliant secure terminals.
- Any faxed-in applications (Continuing Education only) are received on a fax machine that is connected to an analog phone line.
- KC employees are prohibited from sending credit card information using electronic communication methods such as e-mail, chat, or instant messaging.

6.2.3 Hard Copy Storage, Transportation and Destruction

As hard copies of PCI covered are strictly limited to emergency situations, guidance on the storage, transportation, and destruction of this data is covered in the PCI Compliance policy and procedure.

6.3 Diligence Concerning 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 in order to comply with the Red Flag Rules are outlined in the Kaskaskia College's Identity Theft Pursuant to Red Flags Rule policy & procedure.

6.4 Diligence Concerning the Family Educational Rights and Privacy Act

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 the privacy of those records. 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 are covered in the Privacy of Student Records policy (FERPA policy).

6.4.1 Student Information Maintenance

The Records office has ownership and authority over the primary repository of student data at Kaskaskia College. The registrar will evaluate all requests for access to student information systems and will either approve or deny individual requests on a case-by-case basis.

Employee training requirements regarding FERPA related issues are covered in the FERPA policy. Basic outlines of major points are presented below.

6.4.2 Personally Identifiable Information

According to FERPA regulations, educational agencies or institutions are not permitted to release educational records, including personally identifiable information from those records, without prior written consent. According to FERPA, "personally identifiable information" (PIN) is

defined as information which may include but is not limited to, the following:

- Student's name
- Name of the student's parent or other family member
- Address of the student or the student's family
- A personal identifier, such as the student's Social Security Number or student ID number
- A list of personal characteristics that would make the student's identity easily traceable
- Other information that would make the student's identity easily traceable
- Refer to the FERPA policy for the official listing of PIN items as well as the proper handling of this information.

Disclosure of any student information by non-records office Services personnel to any organizations or persons, including students, is prohibited. Employees outside of the Records office should direct such requests to the Registrar.

6.4.3 Directory Information

Under FERPA, the College is allowed to disclose directory information, including that which may be personally identifiable information, without the prior consent of students. Directory Information and the student's right to suppress that information is identified in the FERPA policy.

6.4.4 Grade Posting

Employees are prohibited from posting grades or evaluative data in public areas using personally identifiable information, in whole or in part. Public areas include, but are not limited to, classrooms, computer labs, collaborative study areas, hallways, department reception areas, conference rooms, or on office doors. FERPA prohibits an instructor from posting grades by social security numbers, student ID numbers, or names because these types of information are personally identifiable or easily traceable to the students. Instructors should post grades in the current Learning Management System (LMS). The LMS provides a secure and private method for instructors to share grade information with students.

Employees are required to direct students who inquire about FERPA regulations to the Registrar. Employees outside of the Records Office are prohibited from responding to a student's questions relating to FERPA. Employees outside of the Records Office are not allowed to carry out a FERPA-based request.

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 per the institutional policy review calendar by the CIO and a working group comprised of appropriate staff members. The policy may be reviewed and updated more often if circumstances arise that require significant changes to the policy.

9.0 TRAINING AND COMMUNICATION

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

Additional training will be provided to employees whose primary job duties require them to work with CSI. Procedural training specific to a particular department regarding CSI will be the responsibility of the department head.

Approval History:

Replaces Information Security 6.13 Approved May 18, 2020