KASKASKIA COLLEGE

INFORMATION SECURITY PROCEDURE

Policy Number: 2.4000
Subject Area: General College Policies/Administration
Adopted: 07/17/2025
Revised: 07/17/2025

I. INTRODUCTION

The primary goal of Kaskaskia College's (KC) Information Security Procedure 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 Procedure are to:

Categorize information as public versus confidential and sensitive to implement appropriate access controls

Train employees and maintain controls to assist them in performing their duties while working with CSI, should be in accordance with all policies, procedures, laws, and good practice guidelines.

Provide and train a process for reporting security breaches or other suspicious activity related to CSI.

Provide guidelines and controls on how to communicate information security requirements to vendors.

Summarize the controls and other guidelines that protect the Information Security Policy.

II. PURPOSE OF THE INFORMATION SECURITY PROCEDURE

The Information Security Procedure defines the controls implemented and processes 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. This procedure establishes guidelines and protocols for safeguarding sensitive information and ensuring the confidentiality, integrity, and availability of data within Kaskaskia College.

III. SCOPE

This procedure applies to all faculty, staff, students, and third-party contractors who have access to the institution's information systems and data.

IV. 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.

Classification	Description	Examples	Access & Handling
Level 1: Public	Information intended for public release. No risk if disclosed.	Course catalogs, press releases, job postings, institutional statistics	No restrictions. May be shared freely.
Level 2: Internal Use	Routine business data not intended for public but not harmful if disclosed.	Staff directories, internal emails, budget memos, procedural documentation	Accessible by faculty/staff; not for public or media release. Avoid posting online.

Level 3: Confidential	Information protected by policy or law. Unauthorized disclosure could cause harm or legal liability.	Student grades (FERPA), employee records (PII), procurement contracts	Must be secured (password-protected systems). Shared only with authorized users. Encrypted if transmitted/stored off-site.
Level 4: Restricted	Highly sensitive or regulated data. Unauthorized disclosure could result in financial, legal, or reputational damage.	Social Security Numbers, financial aid data (GLBA), credit card data (PCI-DSS), medical records (HIPAA)	Encryption required in transit and at rest. Access must be role-based. Strict logging, monitoring, and approval required for access.

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)

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 officially recognized activity or sport and weight, height and photos of members of athletic teams or student activities

Photo

V. RESPONSIBILITIES

Classification of information/data for which person/persons are 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 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.

Employee Responsibilities

Chief Information Officer (CIO) - The Chief Information Officer 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. CIO reports to the President of the College. The President reports to Kaskaskia College's Board of Trustees. The Kaskaskia College Board of Trustees are ultimately responsible for all policies of Kaskaskia College. Responsible for developing and maintaining the institution's information security policies, procedures, and guidelines. - Conducts regular risk assessments and ensures compliance with relevant regulations and standards.

Faculty and Staff and Third-Party Contractors

Ensure that sensitive information is accessed and used only for legitimate purposes.

Report any security incidents or breaches to the Information Security Officer (ISO) or designated IT security personnel.

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 must 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.

***Most KC employees will encounter 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.

Students - Must adhere to the institution's acceptable use policy regarding information systems and data.

Report any suspected security issues or concerns to the IT helpdesk or ISO.

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 in departmental procedures and follow them.

Report any suspicious activity regarding CSI to the CIO or VPAS

VI. Diligence

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.

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.

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

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, with MFA built into the tool. If phone number associated with the account is incorrect, the information can only be changed for students in Admissions and employees in Human Resources.

Off-campus access to Kaskaskia College network resources is limited to Cisco's Virtual Private Network (VPN) software, SharePoint, Microsoft Portal, 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 Backup – "Home Directory"

Physical media storage onsite in a secure location for approved time

Server based backup for approved time

VII. 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: Electronic Storage standards, Electronic Transmission standards, Hard Copy Storage standards, and Transportation and Destruction standards.

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 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.

Electronic Transmission

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

All online credit card transactions are handled by a third-party service provider. These providers provide a secure web site to handle the transactions and store 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.

VIII. 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.

IX. 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 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 is covered in the Privacy of Student Records policy (FERPA policy), including student information maintenance and personally identifiable information.

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.

Students will retain access to their institutional email account for two years following the completion of their last credit-bearing course. Continuing education, non-credit, or community education courses do not count toward this timeline and will not reset the retention period.

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 that 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.

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.

X. INFORMATION SECURITY CONTROLS

Access Control - Implement role-based access control (RBAC) to ensure that users have access only to the information necessary for their job responsibilities. - Use strong authentication methods (e.g., multi-factor authentication) for accessing sensitive systems and data.

Data Protection - Encrypt sensitive data both at rest and in transit using approved encryption algorithms and methods. - Regularly back up critical data and store backups securely offsite.

Security Awareness and Training - Provide regular training sessions and awareness programs to educate faculty, staff, and students about information security best practices and policies. - Conduct phishing simulations to help users recognize and respond to phishing attempts.

Incident Response - Establish an incident response team (IRT) and develop an incident response plan (IRP) outlining procedures for detecting, responding to, and recovering from security incidents. - Test the IRP through simulated exercises to ensure effectiveness and readiness.

Physical Security - Secure physical access to servers, data centers, and other critical IT infrastructure. - Implement surveillance and monitoring systems to detect unauthorized access or suspicious activities.

Change of Management

Objective

Ensure that access to institutional systems, software, and data is promptly adjusted when an employee's role changes —protecting sensitive systems while supporting smooth role transitions.

Scenarios Covered

- Promotions, transfers, or lateral moves
- Departures (voluntary or involuntary)
- Temporary access (e.g., covering a leave)
- Adjunct onboarding/offboarding
- Student worker assignments

1. Trigger Event: HR or Supervisor Identifies Change

- Any role change, new hire, or separation is reported through an HR status change form or email notification to IT.
- Supervisor or HR must initiate or approve access request changes.

2. Ticket Created in IT System

Ticket should include:

- Employee name and department
- Role/title before and after change
- Effective date of change
- List of required access additions/removals
- List of equipment needs
- Supervisor or HR contact for approval
- Whether it's a termination, transfer, or new role onboarding

3. Approval Workflow

- Direct Supervisor or HR must approve the ticket before IT acts.
- Approval must be logged in the ticket for auditing purposes.
- For access to sensitive systems (e.g., student records, finance, Self-Service, Active Directory groups), IT requires dual approval: HR + Supervisor.

4. IT Actions – Access Adjustments

Upon approval, IT:

- Grants/removes system access per the ticket (email, LMS, Colleague, Shares, licenses, etc.)
- Adjusts group memberships and file shares
- Deactivates VPN, MFA, and SSO credentials if applicable
- Initiates account disablement for separations
- Logs all changes in the ticket with timestamps
  "Termination tickets" must be resolved on or before the employee's final day. Auto-removal scripts or calendar alerts are used for a portion of the process.

5. Confirmation & Closure

IT updates the ticket with the completed actions.

Supervisor and/or HR are notified of completion.

The ticket is closed only when:

All access is verified

Offboarding checklists are complete

Any returned equipment is recorded

Access Control Best Practices

Use Role-Based Access Control (RBAC): Access granted based on job function, not individual discretion.

Implement Review Alerts: Periodic reviews (bi-annually) of user access lists.

Automate Where Possible: Leverage workflows in your ITSM tool for onboarding/offboarding. IT does utilize automations and workflows.

Logs include: All approvals, changes, and actions must be recorded in the ticket.

XI. COMPLIANCE AND MONITORING

Regularly audit and review the effectiveness of information security controls and procedures.

Ensure compliance with relevant laws, regulations, and industry standards (e.g., GDPR, HIPAA, FERPA).

Conduct periodic vulnerability assessments and penetration testing to identify and mitigate potential security risks.

XII. INCIDENT REPORTING

Establish a procedure for reporting security incidents, including contact information for reporting incidents to the ISO or designated IT security personnel.

Document and investigate all reported incidents to determine root causes and implement corrective actions.

XIII. DOCUMENTATION AND REVIEW

Maintain documentation of information security policies, procedures, and guidelines.

Review and update security controls and procedures regularly to address emerging threats and technological advancements.

XIV. VENDOR AGREEMENTS

When negotiating contracts with third-party vendors, Kaskaskia College employees must consider whether the vendor will need access to any of the College's CSI. Any vendor that has access to CSI will be required to abide by Kaskaskia College policies and procedures. Contract language must include acceptance of the institution policies. 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.

Security Requirements

A Statement of Work (SOW) must clearly state the security requirements for the vendors to ensure that their work is consistent with College cybersecurity requirements.

In general, contracts for software and other services delivered from cloud vendors are reviewed by the CIO for security compliance.

Security Documentation Deliverables

Statements of Works and contracts may be required to contain a documented System Security Plan which describes all existing and planned security controls.

Contract Language

Contracts that include exchange of sensitive data must require state confidentiality agreements to be executed by the vendor, must identify applicable state policies and procedures to which the vendor is subjected, and must identify security incident reporting requirements.

Reporting Requirements

Contracts must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of sensitive data, regardless of ownership. In the event of a breach of the security of the sensitive data, the vendor is responsible for immediately notifying Kaskaskia College and Information Technology Services and working with both regarding recovery and remediation. Security reporting requirements in the contract must also require the vendor to report all suspected loss or compromise of sensitive data exchanged pursuant to the contract within 24 hours of the suspected loss or compromise.

Breach Notification

The vendor is responsible for notifying all persons whose sensitive data may have been compromised due to the breach as required by law.

Policy Compliance

Vendors are required to comply with all the applicable Kaskaskia College Information Security Policies.

Contract Maintenance

Departments that have implemented contracts shall ensure all contracts being renewed are updated with provisions supporting this policy's requirements.

Termination of Service

Upon termination of vendor services, contracts must require the return or destruction of all Kaskaskia College data in accordance with Access Control Policy. Procurement and contract managers are to immediately ensure termination of all access to college information systems and, if applicable, facilities housing these systems.

XV. UPDATING THE INFORMATION SECURITY PROCEDURE

The Information Security Procedure 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.

XVI. TRAINING AND COMMUNICATION

The CIO, Director of Information Technology, and Human Resources are responsible for managing 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.

Access to Professional Development and Training Resources

All IT department employees are provided access to a variety of third-party technology training platforms to support continuous professional development and ensure readiness for evolving institutional needs. This includes on-demand training accounts with Crestron, Extron, and Ellucian, as well as access to relevant technology conferences and specialized training opportunities as new systems and tools are implemented. These resources are made available to empower staff to stay current with industry standards, enhance operational efficiency, and proactively support the College's strategic technology initiatives.

XVII. 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.