KASKASKIA COLLEGE

VENDOR MANAGEMENT PROCEDURE

Policy Number: 2.4010
Subject Area: General College Policies/Administration
Adopted: 08/14/2025
Revised: 08/14/2025

I. Kaskaskia Preferences

- Vendors that have a representative assigned to the College who understands the institution's mission, challenges, and limitations of higher education.
- Long-term relationships with responsible vendors.
- Kaskaskia College will follow procurement of services, equipment, and projects in accordance with the IL Public Community College Act -- 110 ILCS 805/3-27.1 and all other applicable state and federal regulations.
- Kaskaskia will challenge prices from vendors when prices deviate significantly and consistently from past patterns.
- IT contracts are generally centralized into the IT Department for better cost control, efficiency, management, and support. A copy of all contracts will be stored in the college's Procurement Office.

II. Vendor Identification and Needs Assessment

- Departments identify the need for goods or services.
- A needs assessment is conducted to define scope, budget, and timeline.
- Procurement Office is notified to initiate the vendor sourcing process.

Roles and Responsibilities

Procurement Office: Oversees vendor selection, contract negotiation, and compliance.

Department Heads: Ensure vendors meet performance expectations.

IT and Legal Teams: Review contracts for data security and legal compliance.

III. Security Requirements

1. A Statement of Work (SOW) must clearly state the security requirements for the vendors to ensure that their work is consistent with the College's cybersecurity requirements.
2. In general, contracts for software and other services delivered from cloud vendors are reviewed by the Information Technology department leadership for security compliance, and if deemed necessary, the CISO team.
3. Statement of Work and contracts may be required to contain a documented System Security Plan, which describes all existing and planned security controls.
4. The vendor is responsible for notifying all persons whose sensitive data may have been compromised as a result of the breach, as required by law.
5. Contracts must clearly define security reporting obligations, stating that the vendor is responsible for maintaining the security of all sensitive data, regardless of ownership. In the event of a data breach, the vendor is required to immediately notify both Kaskaskia College and Information Technology Services and fully cooperate in all recovery and remediation efforts.
6. Unique customer numbers/accounts with each vendor are managed through a password-protected, access control authentication system.
7. Additionally, the contract must stipulate that the vendor is obligated to report any suspected loss or compromise of sensitive data exchanged under the agreement within 24 hours of discovery.
8. Vendors are required to comply with all the applicable Kaskaskia College Information Security Policies, unless an exception is written directly into the contract and approved by Senior Leadership.

IV. Vendor Prequalification

Vendors complete a prequalification form including:

- Company profile (W-9) to begin Onboarding Process
- BEP Certification status
- Qualifications relevant to the scope of work (i.e. SOC2, IT certification to work on equipment, data entry, etc)
- Debarment Checklist verified
- Risk assessment is conducted (e.g., data handling, legal compliance).

V. Vendor Selection

- Compliance with institutional values and diversity goals
- Data security and privacy standards
- Performance Monitoring for prior projects with the institution

- Regulatory compliance (e.g., FERPA, HIPAA, GDPR)
- Evaluation committee reviews submissions based on (cost, quality, compliance, experience, sustainability, and diversity goals)
- Shortlisted vendors may be invited for presentations or interviews.
- Vendors are required to comply with all the applicable Kaskaskia College Information Security Policies, unless an exception is written directly into the contract and approved by Senior Leadership.

VI. Onboarding Process

- Completion of vendor registration forms
- Tax documentation (e.g., W-9)
- Insurance Certificates
- Banking information for payments
- Background and sanctions screening
- Agreement to institutional policies (e.g., data use, confidentiality)
- Final approval is obtained from authorized signatories.

VII. Contract Management

Contracts that include the 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.

Contracts must include:

- Scope of work
- Payment terms
- Deliverables and timelines
- Performance metrics
- Termination clauses
- Confidentiality and data protection clauses
- Data protection and breach notification terms

Renewal and Termination:

- Contracts are reviewed before expiration.
- Renewal decisions based on performance and continued need.
- Termination procedures include:
  - Final performance review
  - Return of institutional property/data
  - Final payment and closure documentation

Termination Security Measure: Upon termination of vendor services, contracts must require the return or destruction of all Kaskaskia College data as per the Institution's Information Security Policy. Procurement Office and contract managers are to immediately ensure termination of all access to college information systems and, if applicable, facilities for housing these systems.

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

Documentation and Recordkeeping

- All vendor-related documents are stored securely.
- Retention follows institutional and legal guidelines.

VIII. Performance Monitoring

- Regular reviews based on Key Performance Indicators (e.g., delivery time, quality, support)
- Issues are documented and addressed promptly

Ensuring the 3 R's below:

1. **Responsibility**
   a. Vendors must adhere to contractual obligations, institutional policies, and legal requirements.
   b. They are expected to act ethically, ensure data protection, and deliver goods/services as agreed.
   c. Responsibility also includes social and environmental accountability, such as fair labor practices and sustainability.
2. **Responsiveness**
   a. Vendors should be prompt and effective in communication, especially when issues arise.
   b. They must respond to inquiries, service requests, and complaints in a timely manner.
   c. Responsiveness is a key indicator of a vendor's customer service quality and reliability.
3. **Reliability**
   a. Vendors must consistently deliver quality goods or services on time and within budget.
   b. Reliability includes maintaining performance standards and being dependable over the long term.
   c. Institutions often track this through performance metrics and feedback.

IX. Risk Management

- Maintain a vendor risk register
- Ensure compliance with:
  - FERPA, HIPAA, GDPR (if applicable)
  - Conflict of interest disclosures
- Classify vendors by risk level (e.g., high-risk vendors handling sensitive data)
- Evaluate vendors' prior partnerships with the institution's 3 R's performance monitoring

- Conduct periodic audits and compliance checks

X. Reporting Violations

Suspected violations of the Vendor Management Policy should be reported to:

- The Procurement Office
- The Chief Information Officer
- Or through privacy@kaskaskia.edu

XI. Policy Review and Updates

Annual review of vendor management procedures.

Incorporate feedback from departments and vendors.

Update procedures based on regulatory or institutional changes.

XII. Contact Information

For assistance with implementing these procedures, contact:

- Procurement Office: procurement@kaskaskia.edu
- IT Helpdesk: helpdesk@kaskaskia.edu
- Information Security Team: infosec@kaskaskia.edu
- Policy Questions: privacy@kaskaskia.edu